

Verifiable Credential and Decentralized Identifiers

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

@ AXIES2021, 2021/12/16



本日のお題

- Decentralized ID (DID), Verifiable Credentials について
- DIDの標準化状況
- VCのこれから
- 課題と関連トピック
 - ワクチン接種証明書 / SMART Health Cards

Decentralized Identifier (DID) and Verifiable Credentials at W3C



自己主権型で実装可能な分散型ID (Decentralized Identifier) とデジタル証明書 (Verifiable Credential)

- 自己主権型デジタルアイデンティティ
 - 誰にも依存せずに自身で制御可能なデジタルアイデンティティ
- Decentralized Identifier (DID) / W3C Candidate Recommendation
 - 属性情報と紐付けられていない「限り無く無色の」アイデンティティ
 - 分散システム指向であり、自己主権型で実装可能
- Verifiable Credential / W3C Recommendation
 - 属性情報を第三者に証明してもらうための【デジタル証明書】仕様
 - ゼロ知識証明などの技術の組み合わせにより個人情報の「選択的最小開示」を実現できる
- 詳細については「大学教育におけるDXシンポジウム」のスライドを参照 [1]

DID標準化への経緯 [1]

- 2014 - W3C WebPayment Groupでの議論が発端 [2]
- 2015 - [XDI.org](https://xdi.org/) での議論継続 [3],
 - 第一回 Rebooting Web Of Trust (RWOT1) [4] でのホワイトペーパー "Decentralized Public Key Infrastructure" [5]
- 2016 - RWOT2でのホワイトペーパー: "Requirements for DIDs" [6]
- 2017 - RWOT3でのホワイトペーパー:
 - "DID (Decentralized Identifier) Data Model and Generic Syntax 1.0 Implementer's Draft 01" [7]
 - W3C Credentials Community Group [8] の作業に統合
- 2019 - W3C Decentralized Identifiers Working Group による標準化開始 [9]
- 2021 - Decentralized Identifiers (DIDs) v1.0 が Proposed recommendation に [10]

[1] Decentralized Identifiers (DIDs) v1.0, Appendix D. Acknowledgements (Editor's Working Draft), <https://w3c.github.io/did-core/#acknowledgements>

[2] Web Payments Community Group Telecon Minutes 2014-05-07, <https://web-payments.org/minutes/2014-05-07/#topic-1>

[3] XDI.org Registry Working Group Charter, <https://docs.google.com/document/d/1EP-KhH60y-nl4xkEzoeSf3DjmjLomfboF4p2umF51FA/edit>

[4] Rebooting Web of Trust, <https://www.weboftrust.info>

[5] Decentralized Public Key Infrastructure, <https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf>

[6] Requirements for DIDs, <https://github.com/WebOfTrustInfo/rwot2-id2020/blob/master/final-documents/requirements-for-dids.pdf>

[7] DID (Decentralized Identifier) Data Model and Generic Syntax 1.0 Implementer's Draft 01, <https://github.com/WebOfTrustInfo/rwot3-sf/blob/master/final-documents/did-implementer-draft-10.pdf>

[8] W3C Credentials Community Group, <https://www.w3.org/community/credentials/>

[9] W3C Decentralized Identifiers Working Group, <https://www.w3.org/2019/did-wg/>

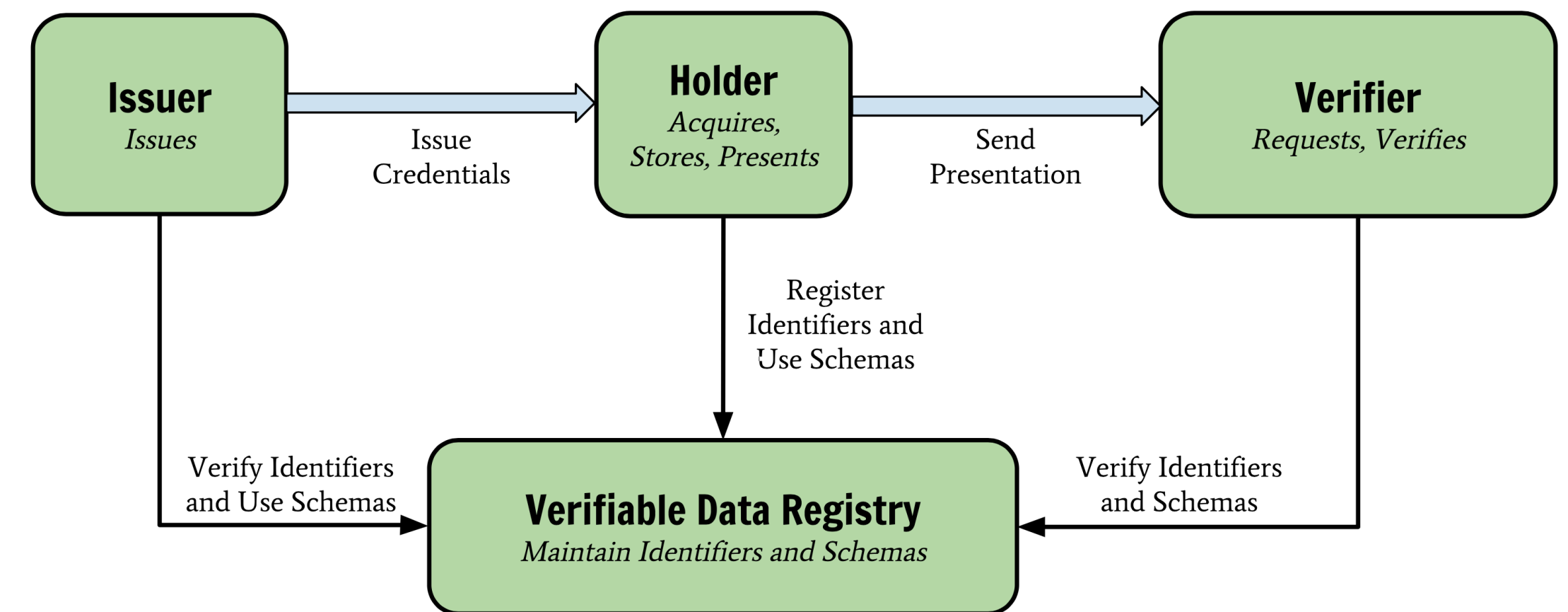
[10] Decentralized Identifiers (DIDs) v1.0, W3C Proposed Recommendation 03 August 2021, <https://www.w3.org/TR/2021/PR-did-core-20210803/>

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



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

Proposed Recommendation

Decentralized Identifiers (DIDs) v1.0

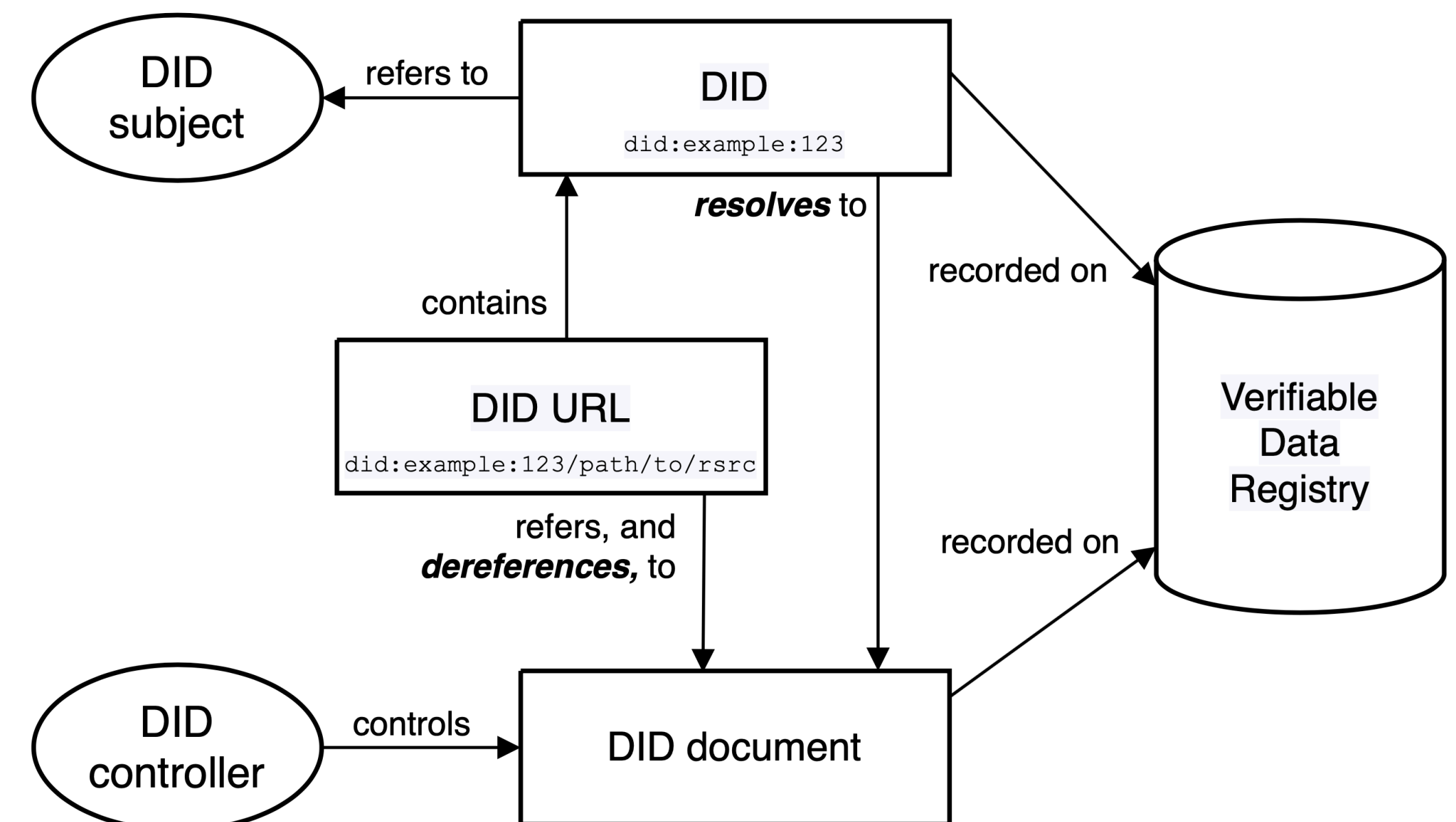
Core architecture, data model, and representations

W3C Proposed Recommendation 03 August 2021

This version:
<https://www.w3.org/TR/2021/PR-did-core-20210803/>

ReSpec
W3C

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/>



DID document

- DID document は DIDで示される主体を表現するのに必要なデータやメカニズムが記載されている。データとしては、公開鍵、特定のブロックチェーン中の位置を示す情報などが例としてあげられる

```
{
  "@context": "https://w3id.org/did/v0.11",
  "id": "did:web:did.actor:alice",
  "publicKey": [
    {
      "id": "did:web:did.actor:alice#z6MkrmNwty5ajKtFqc1U48oL2MMLjWjartwc5sf2AihZwXDN",
      "controller": "did:web:did.actor:alice",
      "type": "Ed25519VerificationKey2018",
      "publicKeyBase58": "DK7uJiq9PnPnj7AmNZqVBFoLuwTjT1hFPrk6LSjZ2JRz"
    }
  ],
  "authentication": [
    "did:web:did.actor:alice#z6MkrmNwty5ajKtFqc1U48oL2MMLjWjartwc5sf2AihZwXDN"
  ],
  "assertionMethod": [
    "did:web:did.actor:alice#z6MkrmNwty5ajKtFqc1U48oL2MMLjWjartwc5sf2AihZwXDN"
  ],
  "capabilityDelegation": [
    "did:web:did.actor:alice#z6MkrmNwty5ajKtFqc1U48oL2MMLjWjartwc5sf2AihZwXDN"
  ],
  "capabilityInvocation": [
    "did:web:did.actor:alice#z6MkrmNwty5ajKtFqc1U48oL2MMLjWjartwc5sf2AihZwXDN"
  ],
  "keyAgreement": [
    {
      "id": "did:web:did.actor:alice#zC8GybikEfyNaausDA4mkT4egP7SNLx2T1d1kujLQbcP6h",
      "type": "X25519KeyAgreementKey2019",
      "controller": "did:web:did.actor:alice",
      "publicKeyBase58": "CaSHXEvLKS6SfN9aBfkVGBpp15jSnaHazqHgLHp8KZ3Y"
    }
  ]
}
```

<https://did.actor> の <https://did.actor/alice/> から

DID URL

- DIDを起点としたリソースロケータ
- DIDを含み、URLのようにパス、クエリ、フラグメント等の要素をもち、DIDで示される対象（リソース）に含まれるであろう要素を示す
- DID documentの中では、フラグメントを用い、DID document中の公開鍵を相対的に指定するために使われる (#key-1)

EXAMPLE 4: A unique verification method in a DID Document

```
did:example:123#public-key-0
```

EXAMPLE 5: A unique service in a DID Document

```
did:example:123#agent
```

EXAMPLE 6: A resource external to a DID Document

```
did:example:123?service=agent&relativeRef=/credentials#degree
```

EXAMPLE 7: A DID URL with a 'versionTime' DID parameter

```
did:example:123?versionTime=2021-05-10T17:00:00Z
```

EXAMPLE 8: A DID URL with a 'service' and a 'relativeRef' DID parameter

```
did:example:123?service=files&relativeRef=/resume.pdf
```

EXAMPLE 9: An example of a relative DID URL

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "did:example:123456789abcdefghi",
  "verificationMethod": [{
    "id": "did:example:123456789abcdefghi#key-1",
    "type": "Ed25519VerificationKey2020", // external (property value)
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMnam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }, ...],
  "authentication": [
    // a relative DID URL used to reference a verification method above
    "#key-1"
  ]
}
```


プライバシー重視の仕様策定

- DID は単一のユーザが多数用い、自由に使い分けができるようになっている
 - DID は、DID を伝える対象、組み合わせるVC等に応じて、対象ごとに都度作成 (pair-wise) で使われることが前提となっている
- DID および DID document に含まれる情報に、個人識別情報(PII)を含めるだけでなく、個人識別に繋がる可能性のある情報が含まれないように、注意深く検討、仕様化（必要に応じた注意書き）などが行われている
- DID Core仕様書の §9. Security Considerations、§10. Privacy Considerations は、デザイン上の思想が表現されている

DID/VC Ecosystem

- DID
 - DID itself
 - method implementation <-> Verifiable Data Registry
 - resolver implementation
- VC
 - VC itself
 - Issuer implementation <-> Verifiable Data Registry
 - Holder implementation (= wallet)
 - Verifier implementation
- Transport between entities / Negotiation Protocols
- ... Operation ... Interoperability ... etc.




Formal Objections on DID Core v1.0 Proposed Recommendation



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)

 DiD 1.0 Comments 21 September 2021  

Attendees		Contents
Present	Tantek Çelik, Chris Wilson, Philippe Le Hégaret, 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	

Meeting minutes

plh: sent agenda in advance
... want to see if we can find common ground without forcing common ground on broader community

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



DID Working Group

1. DID Formal Objection FAQ

This document is an informative document that has been reviewed, published, and is maintained by the [W3C Decentralized Identifier Working Group](#). The document IS NOT a reflection of the views of the objectors (Apple, Google, and Mozilla) to the publication of the DID Core specification. Comments regarding this FAQ are welcome and should be sent to the [W3C Advisory Committee Forum](#), a Member-only W3C mailing list. Any member of the public is also welcome to join the discussion in the [W3C Credentials Community Group](#), where updates on the status of the DID Core Formal Objections are provided on a regular basis.

1. [What is going on?](#)
2. [What are the points of contention?](#)
3. [Why does the W3C hate decentralization?](#)
4. [What happens if the objections are upheld?](#)
5. [Why the concern over Google, Apple, and Mozilla objecting?](#)
6. [Did the DID Working Group follow its charter?](#)
7. [Did the DID Core specification get wide review?](#)

[1] <https://www.w3.org/2019/did-wg/faqs/2021-formal-objections/>



Verifiable Credentials 2.0 and New WG Charter



VC WG 新 Charter [1]

- 何をVC 2.0標準に取り込むのか、議論中
 - 決定済:
 - 検証可能な証明書データモデルの旧バージョンで見つかった誤りに対処
 - クレデンシャル、プレゼンテーション、および証明のデータモデル
 - データモデルのレジストリ
 - 既存の暗号プリミティブを利用した証明の表現と検証のためのアルゴリズム
 - 加えて
 - 多言語化 (鈴木により提案中[2]。取り組むことになる見込み)
- 承認されてから2年間の作業

[1] Verifiable Credentials' WG new charter

<https://w3c.github.io/vc-wg-charter/>

[2] Standardization of Multilingual Support

<https://github.com/w3c/vc-wg-charter/issues/19>



| 応用事例: SMART Health Cards



日本でのワクチン接種証明のデジタル化

- 厚生労働省「海外渡航用の新型コロナワクチン接種証明書について」[1]
- 2021/12/20から、スマホ向けで発行。マイナンバーカードで本人確認
- 日本国内用は Smart Health Card [2] で、Verifiable Credentialベース
- 海外用+国内用は VDS-NC(ICA0)標準 (VCでは無い)+Smart Health Card

【国内用、海外用の接種証明書(紙)の様式】

日本国内用 接種証明書						海外用及び日本国内用 接種証明書					
<p>新型コロナウイルス感染症 予防接種証明書 Vaccination Certificate of COVID-19</p> <p>姓 名 [Surname Given name] 接種 証明 [SESSYU SYOUMEI] 生年月日 [Date of Birth] (YYYY-MM-DD) 1991-02-05 国籍・地域 [Nationality/Region] JAPAN</p> <p>① 国内用 [Domestic Use] SMART Health Cards</p> 						<p>新型コロナウイルス感染症 予防接種証明書 Vaccination Certificate of COVID-19</p> <p>姓 名 [Surname Given name] 接種 証明 [SESSYU SYOUMEI] 生年月日 [Date of Birth] (YYYY-MM-DD) 1991-02-05 国籍・地域 [Nationality/Region] JAPAN 旅券番号 [Passport Number] TR0000000</p> <p>② 国内用・海外用 [Domestic Use / International Travel] SMART Health Cards</p>  <p>③ 海外用 [International Travel] ICA0 VDS-NC</p> 					
接種年月日 [Vaccination Date] (YYYY-MM-DD)	ワクチンの種類 [Vaccine Type]	メーカー [Manufacturer]	製品名 [Product Name]	製造番号 [Lot Number]	接種国 [Country of Vaccination]	接種年月日 [Vaccination Date] (YYYY-MM-DD)	ワクチンの種類 [Vaccine Type]	メーカー [Manufacturer]	製品名 [Product Name]	製造番号 [Lot Number]	接種国 [Country of Vaccination]
2021-04-02	COVID-19 mRNA	ファイザー	コミナティ	ABC123	日本 [JAPAN]	2021-04-02	COVID-19 mRNA	ファイザー	コミナティ	ABC123	日本 [JAPAN]
2021-04-23	COVID-19 mRNA	ファイザー	コミナティ	DEF456	日本 [JAPAN]	2021-04-23	COVID-19 mRNA	ファイザー	コミナティ	DEF456	日本 [JAPAN]
2021-12-23	COVID-19 mRNA	ファイザー	コミナティ	GHI789	日本 [JAPAN]	2021-12-23	COVID-19 mRNA	ファイザー	コミナティ	GHI789	日本 [JAPAN]

【国内用、海外用の接種証明書(紙)の規格・記載項目の違い】

	日本国内用 接種証明書	海外用及び日本国内用 接種証明書
二次元コード 規格	1つ ・SMART Health Cards(①)	2つ ・SMART Health Cards(②) ・VDS-NC (ICA0)(③)
人定事項	<ul style="list-style-type: none"> ・ 姓名(漢字ありローマ字なし) ・ 生年月日 	<ul style="list-style-type: none"> ・ 姓名(漢字ありローマ字あり) ・ 生年月日 ・ 国籍・地域 ・ 旅券番号
接種記録	<ul style="list-style-type: none"> ・ 接種年月日 ・ ワクチンの種類 ・ メーカー 	<ul style="list-style-type: none"> ・ 製品名 ・ 製造番号 ・ 接種国
証明主体 その他事項	<ul style="list-style-type: none"> ・ 証明書発行者 ・ 日本国厚生労働大臣 	<ul style="list-style-type: none"> ・ 証明書ID ・ 証明書発行年月日

※SMART Health Cards規格：民間IT企業の共同プロジェクト「VCI」が策定した健康証明書用の規格。
 ※VDS-NC規格：国連専門機関の一つ国際民間航空機関(ICA0)が策定した健康証明書用の規格。

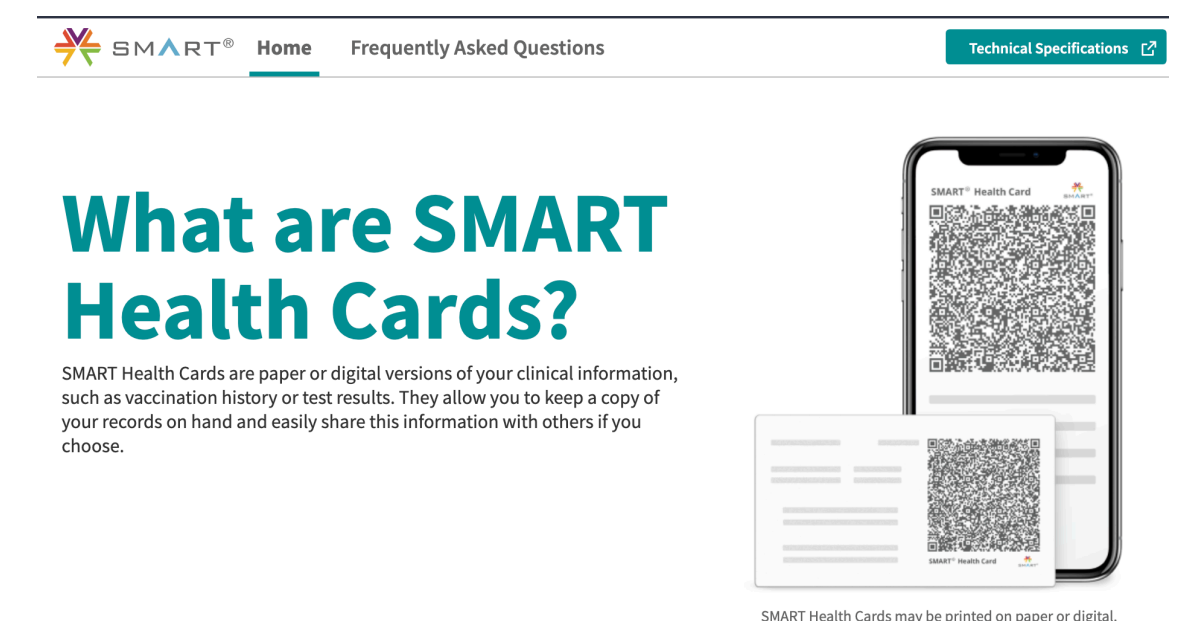
[1] https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/vaccine_certificate.html
 [2] <https://smarthealth.cards>

確認済みの情報としての健康情報の交換 (Apple, iOS15)

- WWDC'2021 "Explore Verifiable Health Records" セッション [1]
- ポイント
 - 仕様としては SMART Health Cards [2] 標準を用いている
 - 健康情報を集中的に保持するHealthKitのデータとして保持
 - 健康情報サービス提供者(アメリカ、イギリス、カナダのみ) から、あるいは直接のQRコードでの読み込みで取り込める
 - アプリから、取り込まれた情報の存在を問い合わせ取得できる
 - アプリからの操作は毎回必ずアプリに情報を渡すか否かをユーザに確認
 - アイデンティティウォレットとしての機能提供ではない

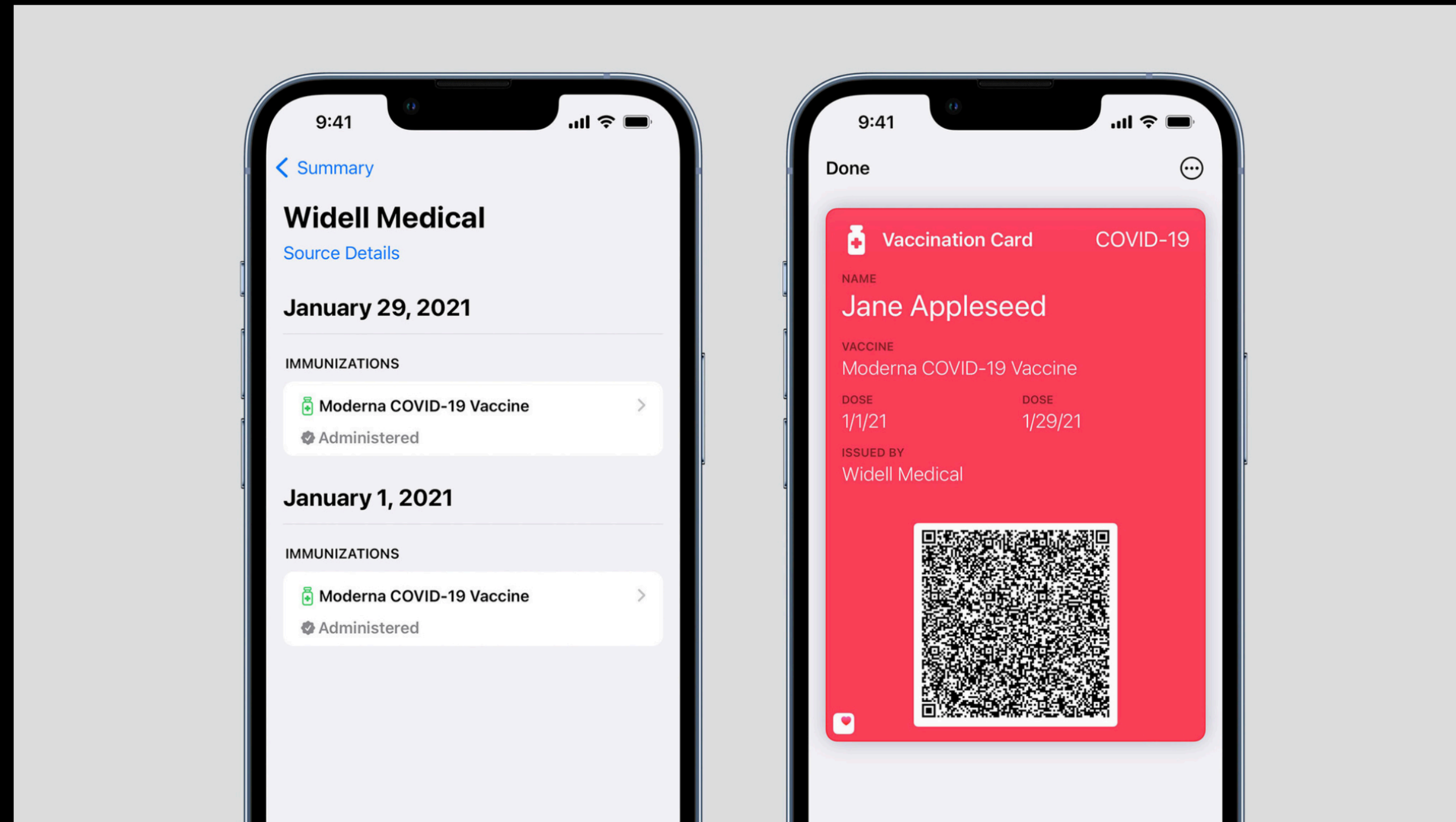
[1] Explore Verifiable Health Records <https://developer.apple.com/videos/play/wwdc2021/10089/>

[2] <https://smarthealth.cards>



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

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**

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>

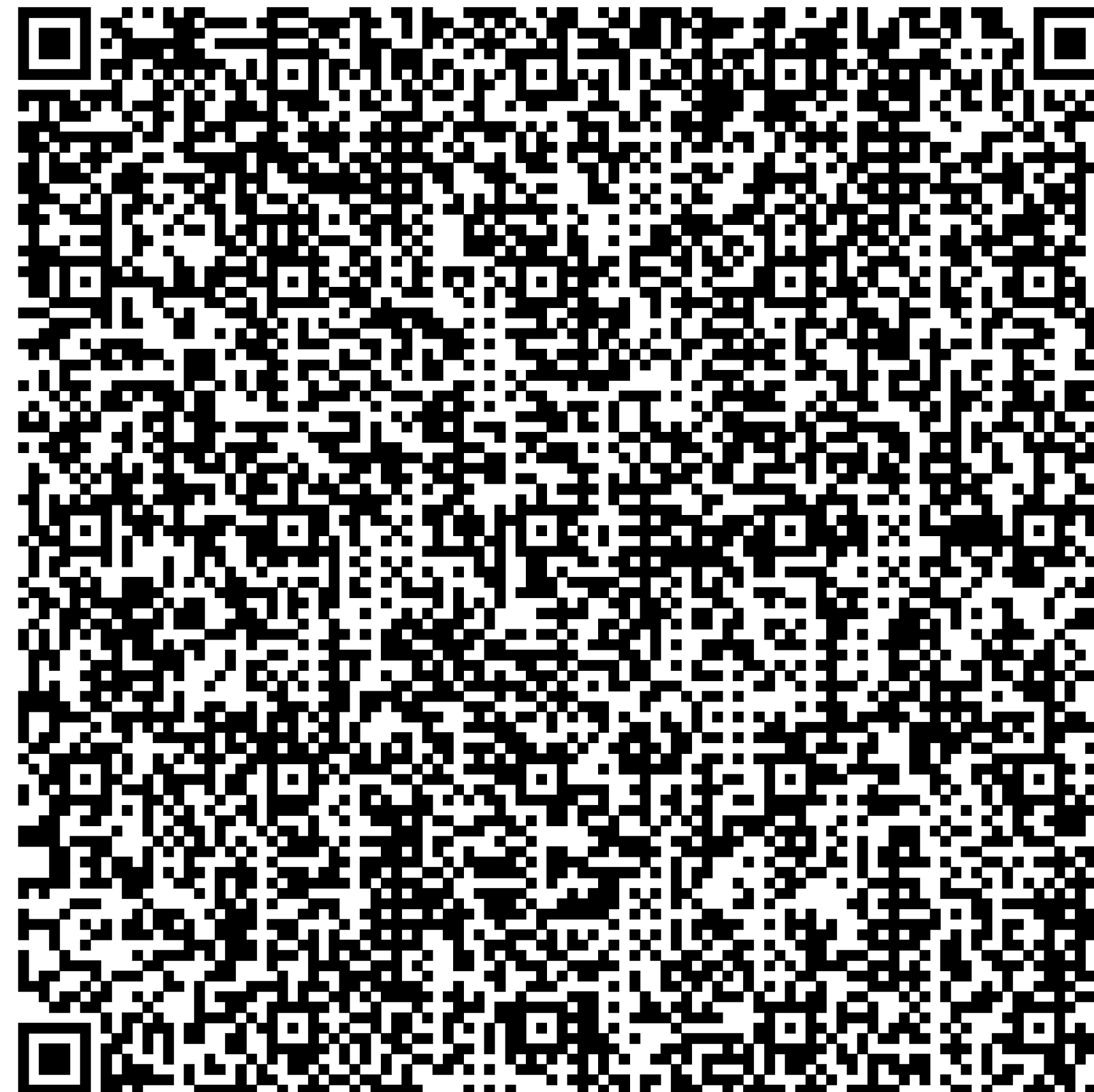
[3] Verifiable Credentials Data Model 1.0 <https://www.w3.org/TR/2019/REC-vc-data-model-20191119/>

[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>

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

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
```

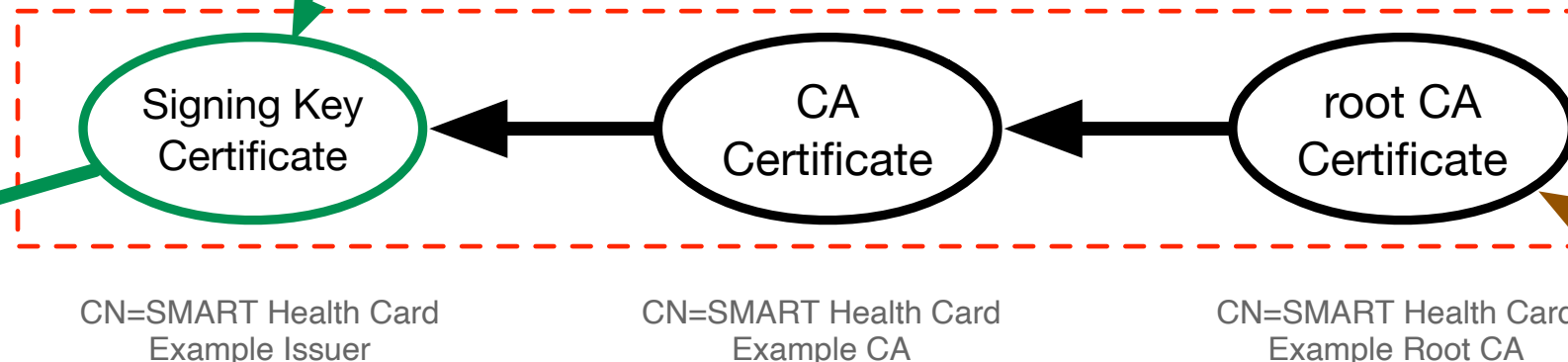
Web Server: https://smarthealth.cards/

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

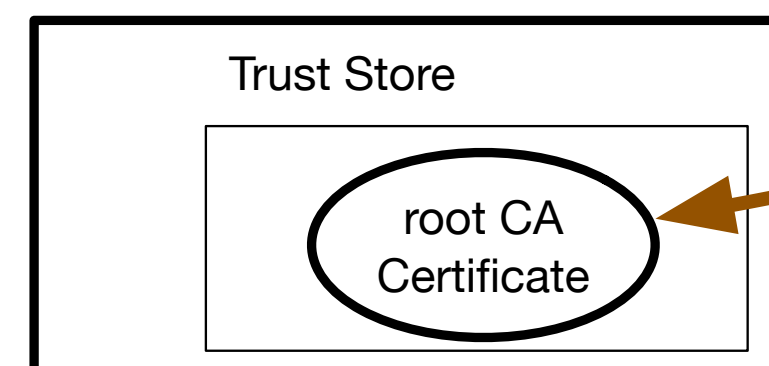
```
{
  "warning": "You should be using spec.smarthealth.cards. <snip>",
  "keys": [
    {
      "kty": "EC",
      "kid": "3Kfdg-XwP-7gXyywtUfUADwBumDOPKMqx-iELL11W9s",
      "use": "sig",
      "alg": "ES256",
      "crv": "P-256",
      "x": "11XvRWylI2S0EyJlyf_bWfw_TQ5CJJNLw78bHXNxcgw",
      "y": "eZXwxv01hvCY0KucrPfKo7yAyMT6Ajc3N7OkAB6VYy8"
    },
    {
      "kty": "EC",
      "kid": "OBztBGRexV0me4ycPTBp-lAMWQmU1_OY1q8m4awW_34",
      "use": "sig",
      "alg": "ES256",
      "x5c": [
        "MIICBjCCAYygAwIBAgIUgGxqplmagmOhhHUnRDUnQhTKaZUwCgYIKoZIz<snip>",
        "MIICBjCCAWigAwIBAgIUWgu3m7SToFGJKDerCOQcMK5AlbUwCgYIKoZIz<snip>",
        "MIICMTCCAZoAwIBAgIUbn1LvaIdt13U3xO2i7miRk1thEQwCgYIKoZIz<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

■ DID/VC応用における課題



DID/VCの課題 (1)

- 対象領域（～業界）毎の国際的に合意されたスキーマの作成は困難
- 玉虫色の仕様 → 複数の実装が存在するシステムの宿命
 - データモデル仕様 / Representation と Abstract Data Model
 - JSON vs JSON-LD & @context / MIME type (ふたつの `+`)
 - 署名方式 (JSON Web Tokens^[1] vs LD-Proofs^[2])
- Dereferencerの仕様が心配（複雑・挙動が十分に仕様化されていない）

[1] Linked Data Proofs 1.0 <https://w3c-ccg.github.io/ld-proofs/>

[2] The Security Vocabulary <https://w3c-ccg.github.io/security-vocab/>

DID/VCの課題 (2)

- 既存トラストフレームワーク/ミドルウェアとの連携あるいは構築
- DIDあるいはVCのインターオペラビリティ
 - DIDの置き換え、method レベルでの置き換え
 - VC提示・交換の Protokol
 - クレデンシャルウォレット / アイデンティティウォレット
- セキュリティ
 - (古典的な公開鍵暗号運用の問題)
 - (ライブラリ、ツールチェーンなどのトレーサビリティ問題)

ラップアップ

- Decentralized ID (DID), Verifiable Credentials について
- DIDの標準化状況
- VCのこれから
- 課題と関連トピック
 - ワクチン接種証明書 / SMART Health Cards