OpenID for Verifiable Credentials

Verifiable Credentials がもたらす信頼モデルの変化

2022 年 6 月 23 日
バージョン：非公式ドラフト 第二版
編集責任者：Kristina Yasuda, Torsten Lodderstedt, David Chadwick, Kenichi Nakamura, Jo Vercammen

内容

内容

エグゼクティブ・サマリー

OpenID Connect は、アイデンティティ連携を大規模に展開できるようにするプロトコルであり、ユーザ中心主義を念頭に置いて開発された。このプロトコルは、エンドユーザから直接同意を得た後、アイデンティティプロバイダがエンドユーザに関する Claim を RP に提供するように設計されている。これにより、アイデンティティプロバイダは自分が情報提供することに関して、RP のプライバシー情報を求めておりそれに応えることに[1]にユーザが『同意』していることを法的な根拠にすることができる。また、このプロトコルは、2 種類のアイデンティティプロバイダの存在を可能にする。一つはエンドユーザがコントロールするアイデンティティプロバイダ[2]で、もう一つはサードパーティが提供するアイデンティティプロバイダ[3]である。

現在、ユーザ中心主義は、ユーザが自身のアイデンティティ情報をよりコントロール、秘匿、および持ち運びできるように進化している。「OpenID for Verifiable Credentials」を使うことで、エンドユーザはアイデンティティ情報を直接 RP に提示できるようになった。これによってエンドユーザは、いつ、どのような情報を共有するかという重要な決定を、よりコントロールできるようになる。さらに、アイデンティティプロバイダは、エンドユーザがどの RP でどのようなアクティビティを実行しているかを知ることがなくなるため、エンドユーザのプライバシーは保護される。また、エンドユーザは、資格情報発行者とフェデレーション関係を結んでいない RP に自分のアイデンティティ情報を提示できるため、自身のアイデンティティ情報の可搬性も得られる。

本稿の目的は、「OpenID for Verifiable Credentials」（OpenID4VC）仕様書群の内容について読者に情報を提供し教育することである。ここでは、自己主権アイデンティティ（SSI）、非集中型アイデンティティ、ユーザ中心主義アイデンティティと呼ばれるユースケースに対応している。この取り組みは OpenID Foundation （国際標準化団体）内で、Decentralized Identity Foundation（DIF）および国際標準化機構（ISO）の ISO/IEC JTC 1/SC 17 [4]ワーキンググループ（Cards and security devices for personal identification）と連携して行われている。これにより、ISO 準拠の携帯運転免許証と W3C Verifiable Credentials データモデルとの協調に向けた取り組みが可能になり、エコシステムにとって特に関心のある分野の 1 つとなった。

本稿の対象読者は、エンドユーザが発行者から直接、資格情報を受け取り、Verifiable Credentials を使用して検証者に直接資格情報を提示するという概念、ユースケース、および設計に関心がある民間および公共部門の意思決定者、システム設計者、実装者である。重要なのは、Verifiable Credentials は、W3C Verifiable Credentials データモデルによって示されている資格情報ばかりでなく、他のデータモデルを用いて示されるものも含むことに注意が必要であることである。

最初に、Verifiable Credentials の基本的なコンセプトを、それがもたらす信頼モデルの変化、その利点、そして一般的に誤解されている概念の明確化に焦点を当てて説明する。

次に、コスト、時間、およびセキュリティの面で、物理的資格情報をデジタル化する利点とビジネス推進要因について詳細に説明する。続いて、Verifiable Credentials が現在実現していることについてのユースケースの項目を設け、その価値、柔軟性、および幅広いシナリオと資格情報形式への適用性に焦点をあてる。

---

[1] 訳注：RP が求めている属性情報の表示画面のこと

[2] 訳注：ユーザが自身のデバイス（スマートフォンなど）やウェブサイト上で、自分自身のアイデンティティ情報を管理する仕組みのこと。デジタルウォレットなどがこの例

[3] 訳注：Google、Facebook、政府機関、金融機関といったサードパーティの企業や組織が提供するアイデンティティプロバイダのこと

[4] https://www.iso.org/committee/45144.html

そして、OpenID4VC の技術的な詳細を示すとともに、なぜ OpenID Connect、OAuth 2.0 が Verifiable Credentials の提示および発行プロトコルの基盤として適しているかなど、決断に至った理由について説明する。

最後に、本稿では、グローバルに相互運用可能な Verifiable Credentials エコシステムを実現するためには、特定のユースケースを満たす標準を選択することが重要であることを繰り返し述べている。

Verifiable Credentials の大規模な採用の実現は「革命ではなく、進化による」ものである。アイデンティティ・コミュニティは、OpenID4VC のような既存および新興の標準の収束と相互運用性を促進する標準を採用することで、アイデンティティ・インフラとポリシーを開発する人々や政府機関をより迅速に支援することができる。

私たちは、この初回の実装者向けドラフトに対するフィードバックを歓迎する。[5]また、ワーキンググループに参加し、標準化を進展させ、他の標準化団体と連携に協力してくれることを歓迎する。最後に、私たちは実装者が「GAIN Proof of Concept Community Group（概念実証の達成コミュニティ）」に参加し、実装のテストを検討することも歓迎する。これらの機会については、本稿の ″結論 ″のセクションを参照されたい。

用語解説

本仕様書では以下の用語を定義する。

OpenID Connect Core ですでに定義されている用語はそのまま使用し、必要に応じて修正する。

- **識別子：**特定のコンテキストにおいてエンティティを一意的に指し示す値
- **アイデンティティ：**定義されたコンテキストの中で個人を一意に識別する一連の属性のセット。[6]
- **Verifiable Credential (VC)[7]：** Verifiable Credential とは、「誰が発行したか」を暗号技術によって検証可能で改ざんを検知できる資格情報である。この定義は、W3C Verifiable Credentials データモデル仕様から借用したが、ISO/IEC 18013-5 mDL [8]などの他のデータモデルを含め、より広範囲に使用されている。
- **エンティティ：** 独立した別個の存在であり、コンテキストの中で識別できるもの。エンドユーザはエンティティの一例である。
- **エンドユーザ：** 人間の参加者
- **ウォレット：** エンドユーザの資格情報と鍵情報を受信、保存し、提示、管理するエンティティ。ウォレットの単一のデプロイメントモデルはない。資格情報とキーは両方とも、エンドユーザによってローカルに保存/管理されるか、遠隔のセルフホストサー

[5] （訳注）2025 年 7 月 10 日現在、OpenID for Verifiable Presentations 1.0 は最終化されている。また、拡張子用の OpenID for Verifiable Credential Issuance (OID4VCI)、OpenID4VC High Assurance Interoperability Profile (HAIP)は検討が進められている。最新状況は https://openid.net/wg/digital-credentials-protocols/specifications/

[6] https://icma.com/physical-credentials-still-necessary-in-the-age-of-digital-transformation/

[7] これは、「資格情報」という言葉が、従来 ID 業界において、パスワードや生体認証など、「Identity や他のリソースを使用する権利があることの証拠として提示されるデータ」という意味で使われてきた定義とは違うことに注意すること。(OpenID Connect Core 1.0)

[8] https://www.iso.org/standard/69084.html

ビス、または遠隔のサードパーティサービスによって保存/管理される。

- **検証者**： 資格情報を検証し、エンドユーザにサービスを提供するかどうかの決定をするエンティティ。RP またはクライアントとも呼ばれる。
- **資格情報発行者**： Verifiable Credentials を発行するエンティティ
- **アイデンティティプロバイダ（IdP）/OpenID プロバイダ（OP）**：エンドユーザを認証し、エンドユーザの同意があれば、認証イベントとエンドユーザに関する Claim を RP に提供できる OAuth 2.0 認可サーバー。アイデンティティプロバイダは、政府エンティティ、アイデンティティ・サービス・プロバイダ、デジタル・プラットフォーム、モバイル・ネットワーク、デジタル・ウォレット・プロバイダ、金融機関のほか、ユーザがアイデンティティ Claim の保存と提示を信頼するあらゆるエンティティである。
- **Self-Issued OpenID Provider（SIOP）**： 暗号的に検証可能な識別子に対するコントロールを証明するためにエンドユーザが使用する OpenID プロバイダ（OP）。
- **Relying Party（RP）**： OAuth2.0 クライアントアプリケーションで、OpenID プロバイダからのエンドユーザ認証と Claim を必要とする。
- **クライアント**： エンドユーザに代わって、その認可のもとに、保護されたリソースのリクエストを行うアプリケーション。「クライアント」という用語は、特定の実装特性（例えば、アプリケーションがサーバー、デスクトップ、または他のデバイス上で実行されるかどうか）を意味するものではない。
- **ウォレットプロバイダ**： ウォレット実装の構築、デプロイ、実行を担当するエンティティ。

ユーザ、ウォレット、検証者、資格情報発行者のなどの役割は、同じ登場人物だとしても、ユースケースとビジネストランザクション次第で異なる。例えば、同じ登場人物でも、プレゼンテーションプロトコルでは、あるウォレットに対して検証者として動作し、発行フローでは別のウォレットに対して資格情報発行者として動作することがある。

クライアント、RP、OpenID プロバイダ、および SIOP は、プロトコル内のエンティティが引き受ける役割である。例えば、プレゼンテーションプロトコルでは、ウォレットは SIOP の役割を担い、発行プロトコルではクライアントの役割を担う。

要点

- 物理的な資格情報をデジタルに変換することは、コスト、時間、セキュリティ、デジタルサービスでのエンドユーザエクスペリエンスという観点から、非常に有益である。Verifiable Credentials は、エンドユーザが自身の ID 情報を管理、秘匿、持ち運びできないという問題を解決し、組織間のクロスドメイントラストの確立を促進する。エンドユーザは、一市民であろうと、従業員または顧客であろうと、Verifiable Credentials を使用して以下の事が可能である。
  - ✧ どの資格情報をどの検証者にいつ開示するかの主導権を維持

- どの資格情報発行者からどの資格情報を取得するかの主導権を維持
- 資格情報発行者に知られることなく、資格情報を検証者に提示し、エンドユーザのプライバシー保護を強化
- 資格情報発行者と連携関係にない RP に資格情報を提示
- さまざまの資格情報発行者によって発行された複数の資格情報をまとめて提示
- サードパーティのアイデンティティプロバイダの決定または寿命とは無関係に、検証者との関係をコントロール

- Verifiable Credentials は、エンドユーザまたは検証者が直接発行者と交流することのなく、エンドユーザが検証者に対し提示する資格情報（運転免許証またはパスポート）のような、物理的資格情報の様式と類似している。このアプローチは、プライバシー法（GDPR、CCPA[9]）やオープンバンキング/オープンデータの動き[10]に見られるような、ユーザの同意に基づくポリシーやアーキテクチャを可能にする世界的な傾向とも一致する。
- OpenID4VC 仕様群を使用することで、資格情報エコシステムを、安全で相互運用性があり信頼できる方法で実装することができる。この仕様は、実装者が Verifiable Credentials の技術スタックの他の構成要素（エンティティ識別子タイプ（DID メソッドを含む）、資格情報形式、失効スキーム、暗号スイート、信頼メカニズムなど）を独自に選択できるようにすることで、さまざまなユースケースに対応できる柔軟性を備えている。
- OpenID4VC は、OpenID Core 仕様に基づいて開発されているため、既存のインフラストラクチャの一部を再利用することができ、コードとライブラリを広く利用することができる。

Verifiable Credentials： パラダイムシフト

物理的資格情報をデジタル化するメリット

物理的資格情報をデジタル版に変換することは、後ほど「物理的資格情報をデジタル化するビジネス推進要因」のセクションで説明するが、現在の紙ベースまたはセミオンラインのプロセスよりも、アイデンティティ検証をより安価、迅速、かつ安全にする機会を提供する。

デジタルの世界で物理的資格情報をそのまま使用すると、パスポートの PDF を電子メールに添付して送信するような、弱点や脆弱性の影響を受けやすいプロセスになってしまう。運転免許証、監査済み納税申告書、出生証明書、結婚証明書、卒業証明書などの物理的証明書をデジタルで Verifiable Credentials に変換し、信頼でき、安全で、プライバシーを保持し、相互運用性のある方法でインターネット上で提示できる世界に向け、今まさに変革の岐路に立っている。

Verifiable Credentials は、この変革の旅において有望なツールである。

---

[9] 2025 年 7 月現在は CRPA（カリフォルニア州プライバシー権法：California Privacy Rights Act）

[10] 「オープンバンキング、オープンデータ、金融グレード API」　編集責任者　Dave Tonge
OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16_jp_v2.pdf

Verifiable Credentials がもたらすトラストモデルのシフト

Verifiable Credentials [11]アーキテクチャは、検証者と資格情報発行者の間のやり取りの中心にエンドユーザを置くパラダイムシフトを作り出す。このアーキテクチャは、エンドユーザが以下を行うことを可能にすることで、エンドユーザに対してより大きな秘匿性、可搬性およびコントロールを提供する：

- 検証者が資格情報発行者に直接連絡することなく、資格情報を検証者に提示する
- 特定のサードパーティアイデンティティプロバイダの名前空間にないエンドユーザ識別子を使用する
- サードパーティのアイデンティティプロバイダの決定または、プロバイダが提供するサービスの利用可能期間から独立して、検証者との関係をコントロールする

これは、アイデンティティ・エコシステム内の登場人物、すなわち資格情報を所有するエンドユーザ、資格情報を検証する検証者、および資格情報を発行する資格情報発行者間の信頼関係における大きな変化である。

現在広く採用されているフェデレーションモデルでは、ユーザが RP にアクセスしたいときは IdP にアクセスし、その場で必要な資格情報（OpenID Connect の場合は ID トークン）の発行を要求する必要がある。その後、これらの資格情報は、何らかのユーザエージェント（通常はウェブブラウザ）によって RP に提示される。検証者は、アイデンティティプロバイダとの関係と、その IdP が使用する Claim 検証手続きに関する知識に基づいて、これらの Claim を利用する（または利用しない）ことを選択する。提供された Claim がその目的に適したものであるかどうかを判断するのは RP である。

このフローでは、ユーザが過去にどの RP とやりとりしたかを IdP が知ることでメリットが得られる従来のシナリオの多くが可能になる。このような従来のシナリオは、トランザクションが組織間のフェデレーションの条件の境界内で発生する場合や、アクセス先の RP のアイデンティティに応じてビジネスロジックを実行する必要がある場合に必ず発生する。しかし、ユーザがどの RP からいつリソースにアクセスしたいかを IdP が知る正当な理由がないシナリオもある。ユーザがいつ、どの RP とやりとりするかを IdP に隠すことは不可能なため「従来の」フローではこうしたシナリオを実現できない。

Verifiable Credentials を使用することは、これらの新しいシナリオを可能にするが、従来のシナリオを無効にするものではないことに注意することが重要である。

Verifiable Credentials では、検証者はエンドユーザのコントロール下にあるウォレットから直接資格情報を受信する。検証者は、1）検証者に信頼された発行者から資格情報が発行されていること、2）エンドユーザが資格情報を提示するために使用したウォレットが、資格情報が発行されたのと同じウォレットであることを暗号的に検証できるため、それらの資格情報を受け入れる決定を下すことができる。最も注目すべき特徴は、検証者が発行者と直接やりとりすることなく、提示された資格情報を受信し検証できることである。発行時と提示時の両方でウォレット

[11] さまざまな用語が存在し、類似または関連する概念は、自己主権型アイデンティティ、自己管理型イデンティティ、直接提示モデル、分散型イデンティティ、ユーザ中心主義アイデンティティなどと呼ばれることもある。

をコントロールするのが同じエンドユーザであることを証明するには、追加で強力な認証メカニズムが必要であることに注意すること。

Verifiable Credentials を利用するパワーと利点を引き出すには、Verifiable Credentials が発行者と検証者の間をエンドユーザを介して流れる新しいエコシステム自体の信頼をいかに効果的に確立するかという課題が残ることに留意することが重要である。検証者が Verifiable Credentials を受け入れ、エンドユーザにそのサービスへのアクセスを許可するためには、資格情報上の資格情報発行者の署名を検証できれば十分なのか。エンドユーザは、Verifiable Credentials を管理するために任意のウォレットを使用できるか。Verifiable Credentials を含むこの新しいモデルは、新しいトラストフレームワークの出現をもたらしている。

Verifiable Credentials のさらなる利点

さらなる利点として、エンドユーザはさまざまな資格情報発行者から発行された複数の資格情報、例えば COVID パス、およびカンファレンスへのアクセスチケットなどを 1 回の提示ですませることが出来るため、より円滑なエンドユーザエクスペリエンスが可能になる。

Verifiable Credentials を使用する場合でも、RP がアイデンティティプロバイダを信頼する必要があるフェデレーテッドアイデンティティモデルのように、検証者はそれぞれの資格情報発行者を信頼する必要があることに注意することが重要である。このような信頼を実現するには、技術的相互運用性に加えて、規制または契約関係が必要となる。

Verifiable Credentials を使用することで、特に数百の資格情報発行者、多数のウォレット、数百万の検証者がエンドユーザを認証し、サービスへのアクセスを許可するユースケースにおいて、技術的な実装がより簡単かつシンプルになる。検証者、ウォレットプロバイダ、資格情報発行者は、一度関係を確立すれば、すべての資格情報発行者のエンドポイントに連絡する必要はない。

このため、多くのエンティティ間の共同作業を必要とする以下のようなユースケースが本番環境で実装されることになった：

- 新人研修（従業員、顧客、サプライヤー、パートナーなどを対象に、サービスの新規導入するにあたり、サービスを利用できるようにする初期サポート）
- エンタイトルメント管理（従業員のアプリケーション、パートナー組織のアプリケーション、インターネット上のサードパーティアプリケーション、物理的な建物などへのアクセス管理など）
- 政府発行機関によるデジタルアイデンティティ資格情報の発行
- サプライチェーンプロセス、または複数のエンティティが国境を越えて取り扱う商品のトレーサビリティが法的要件である場合

これらについては、本稿の「ユースケース」のセクションで詳述する。

Verifiable Credentials に関する誤った通説を解明する

数ある誤った通説の中で、解明すべき重要なものが 4 つある。

第一に、Verifiable Credentials は、自己表現型 Claim または自己署名付き Claim と同等では

ない。Verifiable Credentials で使用されるプロトコルは、確かに、ユーザによる自己表現型 Claim または自己署名付き Claim の検証者への提示を可能にする。しかし、これには、今日オンラインでトラストサービスを提供しているサードパーティエンティティや、物理的アイデンティティ資格情報を発行している政府エンティティによって発行された Verifiable Credentials も含めることができる。要するに、Verifiable Credentials はより広範であり、両方のタイプの資格情報のスーパーセットである。

Verifiable Credentials は、エンドユーザの自主性と発行者および検証者からの自由を意味する場合、自己主権と等価ではない。これは、特に規制対象のユースケースのように、現実のユースケースでは達成が困難である。検証者がエンドユーザから直接資格情報を取得した場合でも、その資格情報を受け入れてエンドユーザにサービスを提供するか（または提供しないか）を決定するのは検証者である。エンドユーザがどこで資格情報を使用する予定であるかにかかわらず、そもそもエンドユーザに資格情報を発行するかどうかを決定するのは依然として発行者である。発行後であっても、ほとんどの場合、発行者は資格情報を取り消し無効にする権利を保持する。

第 2 に、Verifiable Credentials は分散型台帳技術（DLT）やブロックチェーンの使用と同等のものではない。エンドユーザが発行者から直接資格情報を受信し、それを直接検証者に提示するためには、検証者が発行者のコントロールする公開鍵をどのように入手するかのメカニズムが重要になる。DLT またはブロックチェーンを活用する非集中型識別子（DID）は、そのための有用なメカニズムの 1 つである。しかし、すべての DID が DLT やブロックチェーンに依存しているわけではなく、PKI（公開鍵インフラ）や、そのエンティティ[12] が管理するドメイン名でアクセス可能なウェブページを介して公開鍵を取得するなどのメカニズムもある。他の分散化技術には果たすべき役割があるが、Verifiable Credentials エコシステムを実現するために必要でも十分でもない。

第 3 に、Verifiable Credentials は、W3C Verifiable Credentials データモデルの使用と同等のものではない。他のデータモデル、たとえば ISO 準拠の mDL モデルを使用することもできる。

第 4 に、Verifiable Credentials は、参加に関してさまざまなオープン性を持つことができる。政府によって管理されるエコシステムのように、ウォレットアプリケーションプロバイダ、資格情報発行者、および検証者がそのエコシステムに参加するために特定の許可または認証を必要とするものもあれば、誰でも参加できる完全にオープンなものもある。これは、さまざまなガバナンスと参加モデルを可能にするフェデレーテッド・アイデンティティ管理システムと同じである。

「非集中化」のさまざまな範囲

Verifiable Credentials エコシステムの利点を論じるとき、「**非集中化**」が賞賛されることが多い。本稿の目的上、「**非集中化**」のスコープを定義することは非常に重要である。

非集中化のスコープの一つは、場所の観点からの分散であり、1 つの中央コンピューターシステムに依存しないこと、つまり分散システムであることを意味する。これはピアツーピアであったり、クライアントサーバ型の分散システムであったりするが、どちらも何十年も運用されてきた

[12] e.g. /.well-known/ locations

ものである。OpenID Connect エコシステムは、数千の OpenID Connect サーバー（IdP）と数百万のクライアント（RP）を抱え、この観点から非集中型システムとみなすことができる。しかし、このエコシステムにおける個々の OP および検証者は、それ自体が通常特定の当事者のコントロール下にある。ただし、SIOP（自己署名付き OP）は例外で、OP はエンドユーザのコントロール下にある。

非集中型のもう 1 つの範囲は、サードパーティの ID プロバイダから割り当てられる識別子の代わりに、エンドユーザ自身の識別子を資格情報発行者や検証者に提供できることである。W3C 非集中型識別子（DID）は、この識別子提示の分散化の文脈で最も言及されている。

また、検証者が資格情報発行者に直接連絡することなく、エンドユーザが検証者に資格情報を提示できる分散化の範囲もある。W3C Verifiable Credentials （VC）は、この資格情報提示の分散化の文脈で言及されている。

最後に、エコシステムへのアクセスをコントロールする単一の組織に依存しないことを意味するコントロールの観点からの分散化がある。「NASCAR 問題」とウォレットの呼び出しは、通常この文脈で言及される。必要な資格情報のユースケースと保証レベル、そしてどのエンティティにもエコシステムへアクセスを許可するのか、それとも認定されたエンティティだけがエコシステムにアクセスできるのかによって異なる。OpenID Connect Core は既存の技術でこの範囲のアクセスコントロールを可能にしているが、多くの RP はユーザが完全に自由に OP を選択することを可能にしていない。完全にオープンで非集中型のエコシステムを実現するには、ブラウザやモバイル OS など特定のソフトウェアコンポーネントに技術的な変更が必要になるかもしれない。

本稿では主に、上記のような非集中化の 3 つ目の範囲に焦点を当てるが、他の 3 つの範囲についても触れる。

物理的資格情報をデジタル化するビジネス促進要因

このセクションでは、物理的資格情報をデジタル資格情報に変換することの利点とビジネス推進要因について詳しく説明する。

物理的資格情報には、それが紙ベースであれプラスチック・カード・ベースであれ、多くの問題がある。第 1 に、これらの証明書は、特に透かし、エンボス、ホログラム、埋め込みチップなどのセキュリティ機能と組み合わされる場合、製造コストがかかる[13]。プラスチック・カードは低額から簡単に運用できるが、よりセキュアな証明書は、カード 1 枚あたり€ 150（生産コスト[14] ）にもなる。第二に、紛失や盗難に遭いやすく、所有者は数時間、数日、あるいは数週間、紛失に気づかない可能性がある。第三に、セキュリティ機能があるにもかかわらず、偽造が比較的容易である。ほとんどの職業・教育資格証明書はインターネット[15]で公然と購入することができ、偽造 ID、パスポート、COVID-19 証明書[16]は闇市場で購入することができる。第 4 に、これら

[13] 例えば、イギリスのある大学は学生証 1 枚につき 1.40 ポンド以上を支払い、年間 2 万枚近くを発行している。イギリス政府が 2011 年にイギリスのパスポート 1 枚を作成するのに要した費用は 10.79 ポンドだった。（https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118636/17949-breakdown-costs-passport.pdf ）

[14] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education(1).pdf

[15] 偽の学位証明書は、https://www.buydiydiploma.com/ からオンラインで公然と購入できる。

[16] https://www.dailymail.co.uk/news/article-8871923/Passengers-use-fake-negative-Covid-test-certificates.html

の証明書は、資格情報発行者に連絡してその真偽を確認しない限り、確実に検証することはほとんど不可能である。

形は無いがより大きな推進要因のひとつは、市民と発行者の双方が、デジタルの Verifiable Credentials を「不可避の進化」であり、物理的ウォレット内の他の資格情報をデジタル化することの延長だと考えていることである。今日、クレジットカードやデビットカード、交通カード、ポイントカード、航空会社の搭乗券、ビルへの入館資格情報、「現金」、暗号通貨は、一般的に消費者がスマートフォンのアプリケーションに保存できるようになっている。事実、物理的資格情報のデジタル版の開始を発表したり、その開始の意向を示している政府の発行機関もある。例えば、米国では国土安全保障省の運輸保安局と提携してモバイル運転免許証の発行を開始し、EU ではデジタルウォレット（eIDAS 2.0）の提案要請を行っている。

こうした理由から、多くの資格情報発行者は、ある種の電子資格情報発行システム（認証情報を管理提供するシステム）に移行している。最も単純なケースでは、これは既存の物理的資格情報の検証のためだけかもしれないが、電子的に発行および検証することで、物理的資格情報を電子的資格情報で補完するケースもある。電子クレデンシャリングシステムは、前述の物理的資格情報の問題を解決できる。このシステムでは発行コストが非常に安価で、発行システムの初期インストール後の限界コストはほぼゼロからと低額である（必要なセキュリティ・レベルおよびその他の考慮事項に依存する）。また、紛失、偽造、または無視される可能性のあるさまざまな物理的保護メカニズムに頼るのではなく、暗号的に検証できるため、資格情報発行者の信頼と評価が高まる。デジタル資格情報は、ほぼ瞬時に検証できるため、検証者と資格情報発行者の両方のコストを削減すると同時に、不正行為の発生を事実上排除することができる[17]。

イギリスの大学が発行する紙ベースの学位証明書の検証を例に見てみよう。オマーンの英国文化振興会は、学位証明書の検証サービスを 52 米ドル[18]で提供している。

プロセスは以下の通りである：

1. 学歴証明書原本と身分証明書を持参の上、来所する
2. 検証依頼書式に記入し同意書を提出する。その後、同意書のコピーを書類のコピーとともにイギリスの授与機関に E メールで送付し検証を依頼する
3. 資格の真正性の確認が取れ次第、連絡がくる
4. その後、書類を持参して来所し、スタンプを押してもらう

検証プロセスには費用も時間もかかる。それだけでなく、スタンプのある学位証明書は、スタンプのない学位証明書と同様に簡単に複製することができるため、物理的な文書にスタンプを追加しても、追加のセキュリティとはならない。

---

[17] 不正な電子 COVID-19 証明書が販売されているが、これは不正な従業員が本物の研究所から暗号的に真正な証明書を発行したものである。例えば、https://www.bbc.co.uk/news/world-europe-54839434

[18] https://www.britishcouncil.om/en/study-uk/verification-uk-education-services

HEDD（高等教育機関が授与する学位・資格データチェック）と呼ばれるサービスは、同意した個人について、大学学位を確認したいイギリス企業に、セミオンライン・サービスを提供している[19]。プロセスは以下の通りである：

1. ビジネス検証者は、HEDD にアカウントを作成する。ビジネス検証者の名前、組織名、組織の住所、エンドユーザの E メールアドレスを記入する
2. その後、これら内容の手動検証が行われ、提供された E メールアドレスに確認 E メールと秘密の URL を送信することで E メールアドレスが検証される。本稿の執筆者が試みたところ、エンドユーザの詳細情報の手動検証に 3 時間かかっている
3. 企業は、学位検証についての同意書を作成し、学位の詳細な検証をしたい個人から署名をもらう
4. ビジネス検証者は、HEDD ウェブサイトの申請書に記入し、卒業生の詳細（生年月日を含む）と学位（分類など）を入力し、署名入りの同意書の写しをアップロードし、所定の手数料を支払う。費用は大学によって異なるが、検証 1 件につき 12〜37 ポンド（+20%の付加価値税）で、ほとんどの大学は 12 ポンドである
5. 手数料を支払い同意書提出後、ビジネス検証者は E メールでの通知を待つように連絡がある。本稿の執筆者が試みたところ、これに 16 日を要した

繰り返しになるが、このようなセミオンラインプロセスがビジネス検証者にとっていかに高価で時間のかかるものであるかがわかるだろう。

次に、これをデジタル式の資格情報発行および検証システムと比較対照してみよう。OpenID Connect で W3C Verifiable Credentials を使用して、このようなシステムを導入する方法の技術的な詳細は「OpenID Connect と OpenID4VC の技術説明 101」のセクションで説明する。

前提条件として、大学はデジタル学位証明書を発行する必要があり、エンドユーザはそれをスマートフォン上のデジタルウォレット（大学の公式アプリまたは汎用ウォレットアプリが使用可能）に保存することができる。発行大学は、その資格情報の主体だけがその個人が所有するデバイスにデジタル資格情報を受信することができるプロセスを確立する責任を負う。

デジタル学位証明書を利用するために、どのビジネス検証者もエンドユーザから提示された証明書を暗号的に検証し、学位を発行した大学名、卒業時の卒業生の名前、学位の主体、分類、授与日などの情報を取得することができる。

検証者が資格情報の暗号化を検証するための公開鍵または証明書を取得するために支払うべきコストは、場合によっては無料であることもあるが、上記の物理的/セミオンライン検証サービスに支払う価格よりもはるかに安い。このため、デジタル資格情報は非常に費用対効果の高い代替案または補完となる。さらに、検証はほぼ瞬時に行われるため、検証者は膨大な時間と労力を節約できる。

[19] https://hedd.ac.uk/

Verifiable Credentials によって、検証者がウォレットまたはマーケットプレイスを介して資格情報発行者に報酬を支払うなど、斬新なビジネスモデルが可能になる可能性があることは注目に値する。

物理的資格情報をデジタル化することの重要性は COVID-19 が発生したときに明らかになった。各国は、乗客が COVID-19 の予防接種を受けたこと、最近 COVID-19 検査で陰性であったこと、または最近 COVID-19 から回復したことの証明を確実に提出できない限り、海外旅行を安全に再開できないと考えた。当初は紙の資格情報が導入されたが、各国はこれらの証明書の正しい資格情報発行者が誰なのか、どの証明書が有効でどれが無効なのかを把握することが困難であった。それだけでなく、偽造された紙の証明書はすぐに闇市場で購入できるようになった。電子証明書のビジネス上の必要性は明らかだった。

ユースケース

本セクションでは、OpenID4VC 仕様群を使用してさまざまな形式の資格情報が発行され提示されるユースケースを探ることにより、Verifiable Credentials の価値を紹介する。

企業（企業から従業員）、政府、消費者（企業から顧客）のユースケースは提供価値が異なるため、区別することが重要である。

Verifiable Credentials のための OpenID 仕様群がサポートする資格情報形式には、W3C Verifiable Credentials データモデル[20]、ISO/IEC 18013-5 mobile Driving License (mDL)[21]、ISO/IEC 23220-2 electronic Identification (eID)[22]、Anonymous Credentials[23]、SMART Health Cards Framework[24] で使用される FHIR (Fast Healthcare Interoperability Resources) データモデル[25]などがある。

VC データモデル： 従業員新人研修（企業ユースケース）

これまで述べてきたように、Verifiable Credentials は、エンドユーザが資格情報発行者を介さずに、1 回の提示で、さまざまな資格情報発行者が発行した複数の資格情報を提示するよう求められるユースケースで非常に有利になる。

そのようなユースケースのひとつが、従業員の新人研修である。

クイーンズランド州政府、eftpos[26]が提供する ConnectID[27]の ID サービスおよび Meeco[28]は、新入社員受け入れの効率化の改善を目的として、本番環境での試験運用を実施した。その目的は、従業員がスキルセットと経験を証明するためにアイデンティティ、資格認定書、資格情報を提示す

[20] https://www.w3.org/TR/vc-data-model/

[21] https://www.iso.org/standard/69084.html

[22] https://www.iso.org/standard/79124.html

[23] https://www.hyperledger.org/use/hyperledger-indy

[24] https://ecqi.healthit.gov/fhir

[25] https://spec.smarthealth.cards/

[26] （訳注）オーストラリア等で使用されている決済システム

[27] （訳注）オーストラリア政府の TDIF の下で認定された初の非政府デジタル ID サービスプロバイダ

[28] （訳注）2012 年にオーストラリアで設立され、分散型 ID 管理と認証サービスを提供するグローバルプロバイダ

るビジネスフローを自動化し編成することだった。

通常、これらの資格情報は手作業で提供される。従業員は紙の書類をスキャンまたは写真に撮ったコピーを電子メールに添付して、ライセンスや証明書などを提出するよう求められる。

SIOP v2 仕様群と W3C Verifiable Credentials を活用して Verifiable Credentials ソリューションを開発することで、PoC は大幅な効率向上を実証した[29]：

- 必要な資格情報を提出する時間が **48 時間から 30 分に短縮された**
- アイデンティティと資格情報の検証にかかる時間が **3 日から 30 分に短縮された**

OpenID4VC は、この PoC におけるテクノロジー・ドライバであった。OIDC4VP を使用することで、すでに OpenID Connect インフラを持つ既存の検証者は、既存のインフラへの影響を最小限に抑えながら、Verifiable Credentials の検証者となった。これらの資格情報は恒久的に更新が必要なため、資格情報の有効性を保証するプロセスも確立された。従業員は、特定のスキルセットについて、変化し続ける実践や知識にあわせ最新に保つ必要がある。

また、従業員がさまざまなアイデンティティプロバイダから必要な資格情報を取得し、それらを雇用主に提示するためのオーケストレーション・プロセスを作成するのも非常に容易だった。

W3C Verifiable Credentials データモデルは、職場資格情報を含むあらゆるタイプの資格情報を表現するために使用できる柔軟で一般的なデータモデルを定義している。

VC データモデル： 職場の資格情報によるエンタイトルメント管理（企業ユースケース）

従業員新人研修のユースケースは、職場の資格情報を伴うエンタイトルメント管理のユースケースに一般化することができる。資格情報は職場組織によって発行され、エンドユーザは従業員、学生、スタッフ、請負業者、またはベンダーである。新人研修に加えて、以下のエンドユーザの一連の行動や思考プロセスをサポートする：

- 職場のアプリケーションへのアクセス – 例： 認証済み従業員が職場の電子メールにアクセスする
- パートナーによる職場アプリケーションへのアクセス – 例えば、ウッドグローブ社の認証済み従業員がファブリカム社で共同作業を行っている
- インターネット上のアプリケーションへのアクセス – 例えば、ウッドグローブ社で認証済みの社員が、航空会社の旅行割引を利用できる状態にする
- 物理的な建物へのアクセス – 例えば、認証済み従業員は、全国どこにいても会社の敷地内にアクセスできる

マイクロソフト社が注目している、職場資格情報を使ったエンタイトルメント管理の基本シナリオのひとつは以下のようなものだ：

[29] https://www.meeco.me/resources/case-study-digital-identity-verifiable-credentials

1. ウッドグローブ社は、マーケティング・キャンペーンのためにファブリカム社と契約した。ウッドグローブ社は、ウッドグローブ社または下請け企業の従業員のみがリソースにアクセスできるポリシーを設定している。ウッドグローブ社はデジタルウォレットを通じてエンタイトルメント資格情報を受け付ける
2. ファブリカム社は従業員に電子メールを送り、雇用主が事前に選択したウォレットに従業員資格情報を発行することを提案する
3. ファブリカム社の従業員アリスがウッドグローブ社のリソースにアクセスしようとすると、雇用主に対して証明するための資格情報の提示を求められる。アリスはファブリカム社のウェブサイトに表示された QR コードをスキャンし、プロンプトが表示されたら、ウッドグローブ社に資格情報の提示を確認する。ウッドグローブ社は受信した資格情報を確認し、アリスを契約者がアクセスできるリソースにアクセスできるようにする

ISO/IEC 18013-5 データモデル： モバイル運転免許証（政府ユースケース）

Verifiable Credentials は、政府発行の資格情報にも有用である。注目すべきユースケースの一例としてモバイル運転免許証がある。

物理的な運転免許証は、それぞれの国・地域の主体である運転許可のデータセットであり、国内でのみ有効である。歴史的にみると、のちに国際運転免許証として使用できるようになる国内運転免許証を設計する作業の主な場所は、国際標準化機構（ISO）であった。

最近、北米、南米、欧州、アジア太平洋を含むさまざまな地域で、mDL として知られるモバイル運転免許証の導入が検討されており、多くの概念実証や大規模な導入が行われている。mDL は、運転許可証のデジタル版であり、運転者のアイデンティティ情報と運転資格を含む。

国・地域は、運転免許証情報を使用して、所持者のアイデンティティおよびその運転資格を検証することができる。検証を成功させるには、以下の条件を満たす必要がある：

- 所持証明（Proof of possession ： PoP） ： 運転免許証の情報は、免許証の所持者だけが使用できるように、一意性のある暗号鍵に結び付けられている。
- ユーザの同意： 運転免許情報は、所持者が明示的に要求した後にのみ提示されるべきである。

身分証明書は「目的の用途」と「二次利用」の両方に使用できることに注意すべきである。運転免許証の「目的の用途」の範囲は、発行認可機関によって定義され、多くの場合（国・地域の）運転資格を確認するためである。個人識別のための携帯運転免許証の使用は二次利用であり、発行当局はそのような使用について責任を負わず、免許証所持者は自己リスクで使用しているとみなされる。OpenID4VC は、ISO/IEC 18013- 5 で定義されたデータモデルで表現された mDL の発行および提示、特に「二次利用」に適している。

自己署名付き OP は、以下の 2 つの ISO 技術仕様で言及されている：

- ISO/IEC TS 23220-4 個人識別のためのカードおよびセキュリティデバイス - モバイル

デバイス経由のアイデンティティ管理のための構成要素 – 第 4 部：運用段階のプロトコルおよびサービス

- ISO/IEC TS 18013-7 個人識別- ISO 準拠運転免許証 – 第 7 部：携帯運転免許証（mDL）アドオン機能

mDL のユースケースは、国民識別番号、出生証明書、結婚証明書などの政府発行の ID 文書に拡大できることに留意されたい。

FHIR データモデル： SMART ヘルスカード（消費者ユースケース）

もう一つのユースケースは医療データである。医療業界で広く使われているデータモデルのひとつに FHIR 規格（Fast Healthcare Interoperability Resources）がある。

SMART ヘルスカードはエンドユーザの臨床情報を紙またはデジタル化したもので、主にワクチン接種の資格情報を表現することで知られている。これは、「医療セマンティクス」（どこで、誰によって、どのようなワクチンを接種したか、接種者の属性は何か）を表現する FHIR データモデルと、「アサーション・セマンティクス」（誰が何を言ったか、いつ言ったか、どうやって知ったか）を表現する W3C Verifiable Credentials データモデルの両方を活用した基準値を示す好例である。

SMART ヘルスカードはまた、職場用 VC や mDL の前の例とは対照的に、それを所有するエンドユーザの識別子に暗号的にバインドされない資格情報の例でもある。その代わり、SMART ヘルスカードには、Claim ベースのバインディング[30]を可能にするエンドユーザ・アイデンティティ Claim が含まれている。検証者は、SMART ヘルスカードと同時に、同じアイデンティティ Claim（例：本人に直接、またはオンラインの ID 検証サービスを使い、運転免許証または他の ID カードからの名前、住所、生年月日）を含む既存の物理的またはデジタル ID 形式の提示を要求することで、資格情報のバインディングが正しいかを確認しなければならない。

SMART Health Card は、OpenID4VC のプレゼンテーション仕様を使用する必要はないが、FHIR コミュニティはすでに OAuth 2.0 を使用して資格情報を発行しているため、OpenID for Verifiable Credential Issuance 仕様から大きな恩恵を受けることができる。

OpenID Connect と OpenID4VC 技術説明 101[31]

OpenID Connect に対する誤解

既存の俗説とは対照的に、OpenID Connect は中央集中型の大手アイデンティティプロバイダ（IdP）のためだけに開発されているわけではない。中央集中型の IdP だけでなく、IdP の大規

[30] （訳注）資格情報に含まれる Claims（属性情報）を基に、エンドユーザとその認証情報の関連性を確認する仕組み

[31] 101 とは、基本的な入門編や概要のこと

模ネットワーク（大学、モバイル事業者、金融機関など）、エンドユーザが自身の Web サイトで運営する IdP、エンドユーザのモバイルデバイスで実行する IdP など、幅広いアーキテクチャをサポートしている。後者のモデルは、SIOP （自己署名付き OP）という形で、OpenID Connect Core 仕様で専用にサポートされている。

OpenID Connect は、始めからユーザ中心主義を念頭に開発された。アイデンティティデータは、個々のエンドユーザの Claim の粒度で要求および提供できるため、データ最小化原則が適用される。プロトコルフローは、IdP がエンドユーザと直接対話し、エンドユーザ Claim を検証者に公開する前にエンドユーザの同意を取得する機能を提供するようにも設計されている。IdP は要求されたデータおよび最終的なデータ受領者をエンドユーザに提示し、これによりエンドユーザは、情報に基づいた決定を行い、要求された Claim の共有を承認または拒否することができる。

このエンドユーザとの直接対話機能によって、OpenID Connect の実装は WebAuthn のような最新のオリジンベースの認証メカニズムを利用することもできる。

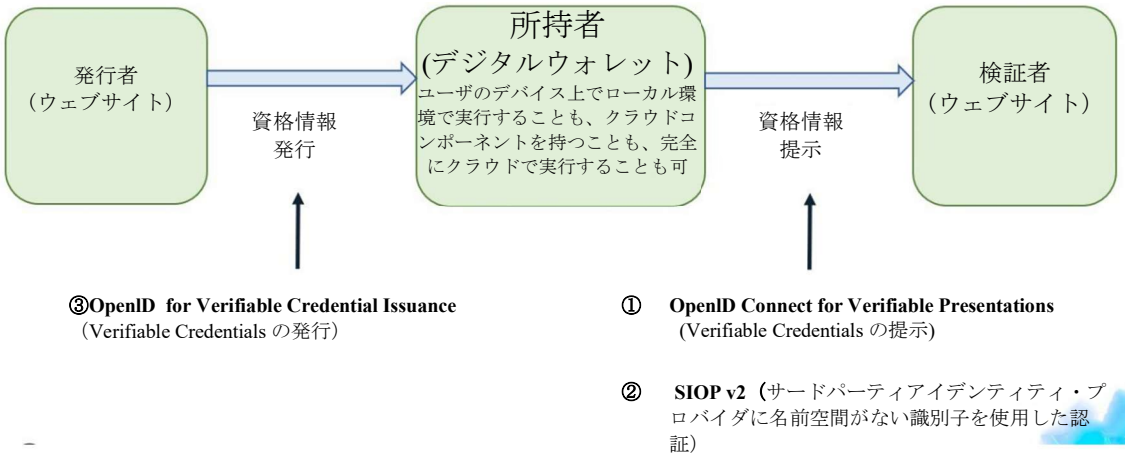
また、OpenID Connect は、そのセキュリティの堅牢性が実証済みであることでもよく知られている（[1]、[2]、[3]参照）。

Verifiable Credentials アプリケーションのために OpenID を拡張

OpenID for Verifiable Credentials は、OpenID Connect の上述の特性と機能を活用して、Verifiable Credentials アプリケーションで適用する。

次の図は、Verifiable Credentials エコシステムにおける登場人物を、それぞれのインタフェースと Verifiable Credentials のための OpenID の各サブプロトコルと共に示している。

「OpenID for Verifiable Credentials」仕様群のコンポーネント



- SIOP v2（SIOP v2）： 暗号的に検証可能な識別子を交換し、エンドユーザがコントロールする鍵情報を使用して認証するプロトコル
- OpenID Connect for Verifiable Presentations： OpenID Connect の拡張で、検証者が検証可能な提示を要求・受信できるようにする。
- OpenID Connect for Verifiable Credentials Issuance:： 資格情報発行を要求するための API および対応する認可フロー。

OpenID4VC は、サポートされる唯一の資格情報形式として JWT や JWS に縛られないことに注意することが重要である。OpenID4VC で実装に成功した他の資格情報形式の例としては、Linked Data Proofs や Anonymous Credentials[32]（AnonCreds)がある。さらに、OpenID4VC は実装者が選択した識別子タイプ（DID メソッドなど）、暗号スキーム、および失効スキームで動作するように設計されている。

OIDC4VP 101

OpenID Connect for Verifiable Presentations（OIDC4VP）は、OpenID Connect を拡張し、Verifiable Credentials を要求および提示する機能を提供する。そのため、検証可能な提示を伝達するために新しい「VP トークン」を導入し、提示される資格情報に関する RP の要件を指定し、検証者が結果を処理するのに役立つように、DIF Presentation Exchange[33] を「Claim」リクエストパラメータに完全統合している。

これは以下の図に示されている。

このフローでは、RP は自己署名付き OP 要求の上に資格情報の提示を要求する。自己署名付き OP（この場合はウォレットでもある）は、提示する資格情報を選択するために保有者と対話し、資格情報の提示を作成して、ID トークンとともに VP トークンで RP に送り返す。

[32] https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0.html#Hyperledger.Indy

[33] https://identity.foundation/presentation-exchange/

RP は資格情報を処理する前に、保持者と資格情報の紐づけ、資格情報の完全性および真正性を検証する。取るべき具体的な手順は OIDC4VP の範囲外で、資格情報の形式、暗号スキーム、および失効メカニズムによって異なる。

OIDC4VP でクエリ言語として使用されている Presentation Exchange（PEv2）仕様のバージョン 2 は現在鋭意開発中であり、OIDC4VP 仕様の例は PEv2 仕様の最新の変更点を反映していない場合があることに留意する必要がある。[34]

広範な例については、仕様書の付録を参照されたい。

SIOP v2 101

SIOP（自己署名付き OP）はすでに OpenID Core 仕様の一部であった（このバージョンは SIOP v1 として指定されている）。これにより、エンドユーザがアイデンティティ情報と署名鍵をコントロールできるようになった。自己署名付き OP を使用すると、エンドユーザは、エンドユーザが管理する鍵情報を使用して署名された自己署名付き ID トークンを使用して認証できる。

新たに登場した SIOP v2 は、SIOP v1 を現代の Verifiable Credentials アプリケーションの課題に適応させることを目的としている。それは以下の機能を導入している：

- エンドユーザ識別子として、処理前の生の JSON ウェブ鍵に加えて DID をサポートする
- 動的に自己署名された OP ディスカバリのサポート
- 「openid://」のようなカスタムスキームに加えて、HTTPS URL 経由での自己署名付き OP の実行をサポート。これにより、最新のスマートフォン OS やウェブウォレットで deep/app/universa の使用が可能になる
- すべての OpenID Connect フローを利用可能に。例えば、認可コードフローを使うことで、SIOP v1 で利用されていた従来の「インプリシット」フローと比較して、クラウド/ウェブウォレットが高度なセキュリティ機能と能力を活用できるようにする
- 「同一デバイス」フローに加えて、エンドユーザが資格情報にアクセスする場所とは異なるデバイス上で提示を開始できる「クロスデバイス」フローをサポートする
- ウォレットの管理のため OpenID Connect 登録メタデータのサポート[35]

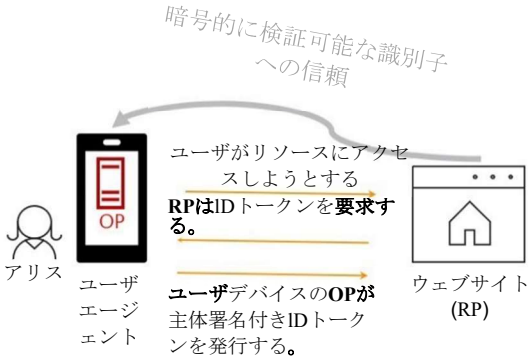
これにより、事前に登録され検証済み RP と自己署名付き OP の相互作用が可能になり、これはアドホックな相互作用に加えて、規制された Verifiable Credentials スキーム（eIDAS 2 など）にとって重要なイネーブラーである。

[34] （訳注）OpenID for Verifiable Presentations 1.0 では、クエリ言語は Digital Credentials Query Language となっている

[35] https://openid.net/specs/openid-connect-registration-1_0.html

次の図は、基本的なメッセージの流れを示している。

SIOP v2



－IDトークンは、ユーザが管理する鍵情報で署名される（2者間での主体識別子による擬名認証）。
－識別子はユーザがコントロールし、サードパーティのアイデンティティプロバイダに依存しない。
－ユースケースでエンドユーザ認証が必要な場合、つまりIDトークンの発行などOpenID Connectの機能が必要な場合、OpenID4VPと組み合わせて使用できる。

0)　エンドユーザがサイト（またはアプリ）にログインしようとする

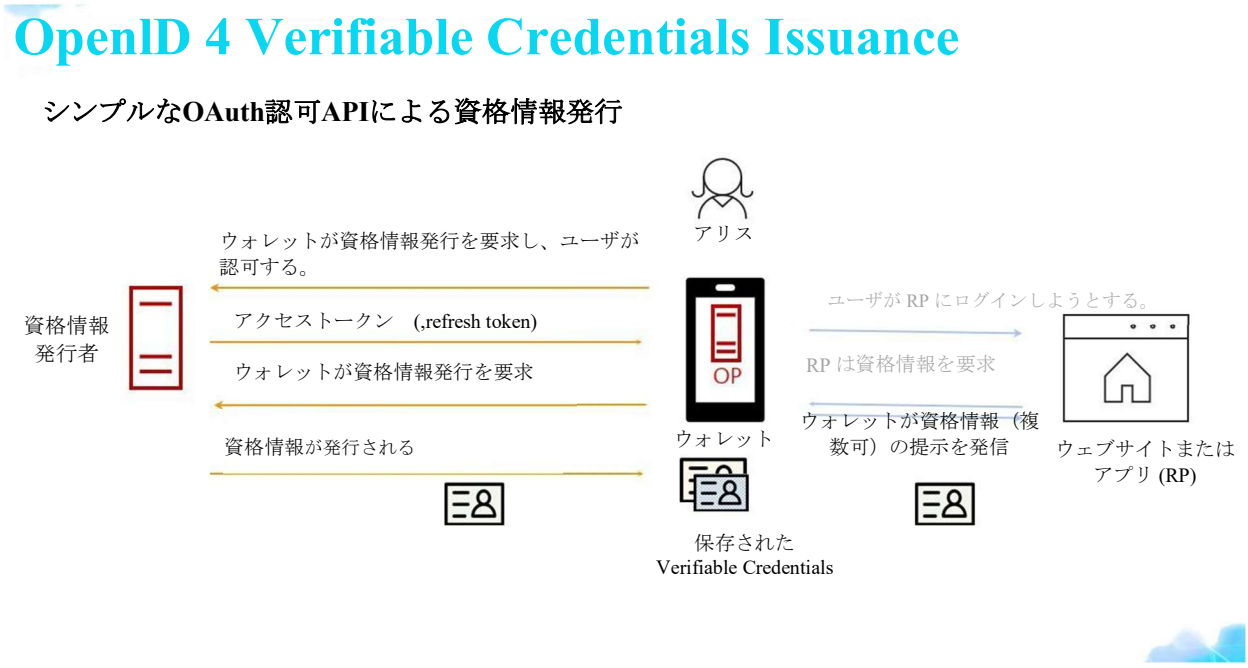
1)　サイトは、エンドユーザの自己署名付き OP に認証要求を送信する

2)　自己署名付き OP は（エンドユーザの代理として）、エンドユーザのコントロール下にある鍵で署名された ID トークンを発行する。自己署名付き OP のアーキテクチャに応じて、このような鍵はモバイルデバイスに常駐するか、クラウド（カストディアルウォレット）に保存される。自己署名付き OP は通常、RP 間の照合を防止するために、特定の検証者に特定の鍵を使用する。自己署名付き OP が同一 RP へのリクエストの相関を防ぎたい場合、エフェメラル鍵を使用することができる

自己署名付き OP は多種多様なウォレットアーキテクチャを可能にする。例えば、ウォレットはユーザのデバイス上で実行できるが、クラウド上で実行可能な環境を提供することもできる。ユーザエクスペリエンスは、モバイルアプリやウェブアプリケーションを通じて提供することができる。プロトコルの観点からは、すべての OpenID Connect フローを利用することができる。例えば、各配置・展開およびユースケースの必要性に合わせて多くの選択肢がある

OpenID4VCI 101

OpenID for Verifiable Credential Issuance（OpenID4VCI）は、資格情報の発行を可能にする。発行は資格情報発行 API を使用して行われる。この API から資格情報を取得できるようにするには、クライアント（通常はウォレット）に OAuth アクセストークンが必要であり、これは認可プロセスの過程で取得される。この仕様では現在、異なるシナリオのニーズに対応する 2 種類の認可プロセスについて記載している。



認可コードのフロー

このフローでは、ウォレットは資格情報発行者に OIDC/OAuth 認可要求を送信することでプロセスを開始する。例えばエンドユーザが資格情報発行者の認可エンドポイントに送信される。認可プロセス中、資格情報発行者はエンドユーザの認証および/または識別を行い、1 つ以上の資格情報を発行する同意を得る場合がある。認可要求が正常に完了すると、ウォレットには認可コードが発行され、トークンエンドポイントでアクセストークンと引き換える。

資格情報発行者は、リフレッシュトークンを発行して、エンドユーザとのさらなるやりとりなしにオンデマンド発行または資格情報のリフレッシュを可能にするなど、決定することもできる。

リプレイに対するセキュリティ対策として、すべてのトークンは送信者に制約されることがある。すなわち、トークンを使用する際にウォレットがその所有を証明しなければならない鍵情報にバインドされる。

このフローは、エンドユーザ・ジャーニーがウォレットから始まる場合に特に適している。例えば、エンドユーザがウォレットアプリをインストールしたばかりで、資格情報の最初のセットをインストールしたい場合、またはエンドユーザ・ジャーニーが検証者から始まり、エンドユーザのウォレットに必要な資格情報がない場合などである。どちらの場合も、ウォレットは適切な資格情報発行者の選択をエンドユーザに提供し、安全で便利な発行プロセスに直接進むことができる。

Pre-Authorized Code Flow

一連の流れが資格情報発行者のウェブサイトまたはアプリから始まり、ウォレットが後のステップで関与するシナリオがある。例えば、すでに認証済みのエンドユーザが試験を受け、合格後にデジタル証明書をダウンロードするよう提案されるケースである。この場合、資格情報に含まれるデータはほぼ完成しており、ウォレットはその資格情報を「受け取るだけ」で済む。

Pre-Authorized Code Flow は、そのようなシナリオに最適化されている。

プロセスは、資格情報発行者がエンドユーザのウォレットにリクエストを送信することから始まる。このリクエストには、ウォレットに対して、どの資格情報発行者からどの種類の資格情報をリクエストすべきかを指示する内容が含まれている。リクエストには Pre-Authorized Code が同梱されており、発行者の希望に基づいて追加のセキュリティ保護が必要かどうか示される。セキュリティ保護が必要なら、エンドユーザは Pre-Authorized Code を使用する際に PIN を入力するなどの必要がある。資格情報発行者は、リクエストを送信する代わりに、同じデータを含む QR コードを表示することもでき、これによりエンドユーザは別のデバイスに存在するウォレットを利用できる。

このフローでは、ウォレットはエンドユーザを資格情報発行者の認可エンドポイントに送る必要はない。その代わり、資格情報発行者のトークンエンドポイントで、事前に認可されたコードをアクセストークンと直接交換することができる。これは、エンドユーザのエクスペリエンスを簡素化するが、コードを特定のデバイスにバインドできないため、セキュリティリスクももたらす。このリスクを軽減するために、資格情報発行者は Pre-Authorized Code の発行につながるユーザ認証フロー中にエンドユーザとエンドユーザ PIN を決め、Pre-Authorized Code がトークンエンドポイントで使用されるときに、この PIN の提示を要求することができる。この PIN をどのようにエンドユーザに伝えるかは、Pre-Authorized Code の送信に使用されるチャネルとは異なるチャネルを使用して送信しなければいけないという条件を満たしていれば、実装次第である。

トークンの応答は認可コードフローと同じである。

資格情報エンドポイント

次に、上述のフローのいずれかを使用して取得したアクセストークンを使用して、資格情報エンドポイントで資格情報発行を要求する。ウォレットは、資格情報がバインドされる鍵情報を所有していることの適切な証明を、要求とともに送信しなければならない。

主な特徴

まとめると、OpenID4VC グループの主な特徴は以下の通りである：

- シンプル
- 開発者が慣れていて、親しみやすい
- 導入済みの OpenID Connect インフラを活用する（Verifiable Credentials の採用を促進する）
- セキュリティ
- 識別子（DID 方式など）、資格情報様式、暗号方式、および失効方式に関する柔軟性

まとめ

Verifiable credentials エコシステムで構成される標準は、その成熟度が多様であり、さまざまな SDO（標準化団体）で開発されている。グローバルに相互運用可能な Verifiable Credentials エコシステムへのキーは、特定のユースケースを可能にする既存のオプションや新たなオプションの中から、各コンポーネントを選択することである。これが、特定のユースケースに対してこのような選択を行う相互運用性プロファイルが出現してきた理由である。したがって、Verifiable Credentials エコシステムを実装するには、ユースケースのニーズとビジネス要件に応じて、多くの方法があることを認識する必要がある。

資格情報転送プロトコルとして OpenID4VC 仕様群を使用する特筆すべき長所の 1 つは、Verifiable Credentials 技術スタックの他のコンポーネント（エンティティ識別子タイプ（DID メソッドを含む）、資格情報フォーマット、失効スキーム、暗号スイート、信頼メカニズムなど）を実装者が独自に選択できることである。

これは非常に強力な拡張ポイントである。実装者は、新しい資格情報形式または新しい識別子タイプのサポートを追加または削除できる一方で、同じプロトコル上で資格情報を発行および提示できるからである。

以下に、OpenID4VC の発行・応答プロトコルと組み合わせることができる各コンポーネントの選択肢の概要を示す。

資格情報データモデル：1 つは W3C Verifiable Credentials データモデルで、汎用多目的データモデルである。もう一つは ISO/IEC 18013-5 標準で、これには、OpenID4VC プロトコル上で交換可能なデータモデルを含む携帯運転免許証の全体の技術スタックを定義している。ISO/IEC 23220-2 標準は、運転免許証に限らないモバイル端末で利用可能な身分証明書のデータモデルである。SMART Health Cards Framework は、FHIR データモデルを使用して「臨床セマンティク

ス」（どこで、誰に、どのようなワクチンを接種したか、接種者の属性は何か）を表現し、W3C Verifiable Credentials データモデルを使用して「アサーション・セマンティクス」（誰が何を言ったか、いつ言ったか、どうやって知ったか）を表現する。最初の 3 つのデータモデルにより、ウォレットは、資格情報を取得したデバイスがそれを提示するのと同じデバイスであることを証明することで、提示する資格情報の正当な所有を暗号的に証明することができる。このデバイスが認証情報を取得したデバイスと同じであることを暗号的に証明する仕組みは現在、SMART Health Card フレームワークでは利用されていない。その代わりに、別の身分証明書から取得したエンドユーザの資格情報と FHR 資格情報内の資格情報を検証者が照合することに依存している。

資格情報スキーマ：ISO/IEC 18013-5 および SMART Health Cards Framework では、名前空間および具体的な Claim 名が定義されているが、W3C Verifiable Credentials データモデルなどの他のデータモデル標準では定義されていない。実装者は、既存の名前空間および Claim 名のいずれにも当てはまらない場合、ユースケースに応じて名前空間および Claim 名を定義する必要がある。たとえば、W3C Verifiable Credentials データモデルを利用するユースケースでは、既存のスキーマや命名規則が適用できない場合、実装者は自分たちのユースケースに合わせてスキーマを拡張し、それに対応する「Vocabularies」[36]を定義する必要がある。

トラストフレームワーク：OpenID4VC は、クライアントと資格情報発行者間、RP とウォレット間の信頼確立に使用できるメカニズムを提供するが、確立が必要な信頼レベルの具体的な基準は提供していない。この機能を果たすには、トラストフレームワークが必要である。さまざまなグループが、信頼レベルの要件が異なる個々のユースケースをサポートするトラストフレームワークを開発している。

暗号スイート：ECDSA や EdDSA から、より高度な Camenisch-Lysyanskaya 署名や BBS 署名まで、さまざまな制約を持つ多種多様なデジタル署名アルゴリズムが使用されている。完全性の証明をどのように表現するかについても、さまざまな選択肢がある：IETF JWS/JWT、W3C CCG Data Integrity（以前は Linked Data Proofs と呼ばれていた）、Hyperledger Indy SDK で使用されている AnonCreds などである。アルゴリズムの選択肢のすべてが、NIST、BSI、ENISA などの関連する国家機関によって審査または承認されているわけではないことに注意。

資格情報と署名の形式：プロトコルは、JWT および JSON-LD 形式の W3C Verifiable Credentials データモデル、JSON および CBOR エンコーディングの ISO/IEC 18013-5 mDL データモデルとして表現された Verifiable Credentials をサポートする（ただし、これらに限定されない）。外部署名（コンパクトにシリアライズされた JWS）および埋め込み署名またはエンベロープされた署名をサポートする。

エンティティの識別子。Verifiable Credentials エコシステムでは、資格情報発行者、エンドユーザ、検証者の 3 つのエンティティが識別子を必要とする。通常、識別子は、資格情報上の署名を検証するために使用される暗号公開鍵を取得するためにも使用される。選択肢には、W3C 非集中型識別子（DID）v1.0、HTTPS URL、JWK、X.509 証明書などがある。

利用されるクエリ言語に収束があることに注意する。検証者がデジタル資格情報の提示を要求す

[36] このようなユースケースの一例は、https://ec.europa.eu/digital-building-blocks/code/projects/EBSI/repos/json-schema/browse/schemas

る場合、要求された資格情報の側面を指定できる必要がある。OIDC4VP は、Decentralized Identity Foundation（DIF）によって定義されたプレゼンテーション・エクスチェンジ（PE）v2.0 仕様[37]を使用する。

さらに技術的な詳細には、付録を参照するか、https://openid.net/wg/digital-credentials-protocols/specifications/ で完全なドキュメント（無料）にアクセスしていただきたい。また、OpenID for Verifiable Credentials 仕様群専用の Digital Credentials Protocols（DCP）[38] ワーキンググループの特別募集への参加を通じて、読者の皆様から本稿および標準についてコメントがあれば歓迎する。ワーキンググループの会合の詳細と参加要件は、https://openid.net/wg/digital-credentials-protocols/[39]でも入手できる。

実装の相互運用性テストを行う機会を探している場合は、OpenID Foundation が主催する Global Assured Identity Network(GAIN) Proof of Concept Community Group に参加することをご検討願いたい。これは、「ネットワークのネットワーク」を実現し、人々によるアイデンティティの証明（https://openid.net/cg/gain-poc/）を支援するというビジョンの実現を目指している。一部の参加者は、Verifiable Credentials のための OpenID 仕様群を使用して実装の相互運用性をテストしている。

最後に、Verifiable Credentials の大規模な採用を達成するのは、革命ではなく進化によるものである。本稿で、Verifiable Credentials の OpenID4VC 仕様群での作業が Verifiable Credentials の全体像にどのように適合するか、Verifiable Credentials の実装の一部として考慮すべき必要のあるとき、Verifiable Credentials の採用をどのように促進できるかについて説明できたと思う。

---

[37] （訳注）https://identity.foundation/presentation-exchange/にあるが、OpenID for Verifiable Presentations 1.0 では、Digital Credentials Query Language となっている https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#section-4-2.1

[38] 2025 年 7 月現在は、Digital Credentials Protocols (DCP)ワーキンググループで検討されている

[39] 2025 年 7 月現在は、Digital Credentials Protocols (DCP) ワーキンググループで入手できる

参考文献

[1] Daniel Fett, Ralf Küsters, und Guido Schmitz, "The Web SSO Standard OpenID Connect：詳細な形式的セキュリティ分析とセキュリティガイドライン", 米国電気電子技術者協会第 30 回コンピュータセキュリティの基礎シンポジウム (CSF 2017), 2017, S. 189--202. https://publ.sec.uni- stuttgart.de/fettkuestersschmitz-csf-2017.pdf

[2] Daniel Fett, Ralf Küsters, und Guido Schmitz, " OAuth 2.0 の包括的形式的セキュリティ分析", コンピュータとコミュニケーションセキュリティに関する第 23 回 ACM SIGSAC 会議の議事録(CCS 2016), 2016, S. 1204--1215. https://publ.sec.uni-stuttgart.de/fettkuestersschmitz-ccs-2016.pdf.

[3] Daniel Fett, Pedram Hosseyni, und Ralf Küsters, " OpenID 金融グレード API の詳細な形式的セキュリティ分析", 2019 年セキュリティとプライバシーに関する米国電気電子技術者協会会議(S&P 2019), 2019, Bd.1, S. 1054-1072. https://publ.sec.uni-stuttgart.de/fetthosseynikuesters-fapi-sp- 2019.pdf (編集)

[4] Nat Sakimura, John Bradley, Michael B. Jones, Breno de Medeiros, and Chuck Mortimore, OpenID Connect Core 1.0, November 2014.

付録

OpenID Connect 4 Verifiable Presentation の例

ISO/IEC 18013-5 mDL

以下は、ISO/IEC 18013-5:2021 形式の mDL 資格情報を要求する認可要求で、Claim パラメータがどのように使用されるかの標準的ではない例である：

```
"claims": {
  "vp_token": {
    "presentation_definition": {
      "id": "mDL-sample-req",
      "input_descriptors": [
        {
          "id": "mDL",
          "format": {
            "mdl_iso_cbor": {
              "alg": ["EdDSA", "ES256"]
            },
          "constraints": {
            "limit_disclosure": "required",
            "fields": [
              {
                "path": ["$.mdoc.doctype"],
```

```
                "filter": {
                  "type": "string",
                  "const": "org.iso.18013.5.1.mDL"
                }
              },
              {
                "path": ["$.mdoc.namespace"],
                "filter": {
                  "type": "string",
                  "const": "org.iso.18013.5.1"
                }
              },
              {
                "path": ["$.mdoc.family_name"],
                "intent_to_retain": "false"
              },
              {
                "path": ["$.mdoc.portrait"],
                "intent_to_retain": "false"
              },
              {
                "path": ["$.mdoc.driving_privileges"],
                "intent_to_retain": "false"
              }
            ]
          }
        }
      ]
    }
  }
}
```

詳細な説明は OIDC4VP 仕様の付録を参照のこと。

応答は ID トークンと VP トークンを含む。以下の例では、単一の ISO/IEC 18013-5:2021 mDL が VP トークンとして返される。ISO/IEC 18013-5:2021 mDL は、CBOR でも JSON でもエンコードできることに注意。

以下は、[SIOPv2]および本仕様を使用した場合に認可リクエストに成功した標準的ではない例である。

```
POST /callback HTTP/1.1
Host: client.example.org
Content-Type: application/x-www-form-urlencoded


id_token=<<Base64URL encoded ID Token>>
  &vp_token=<<Base64URL encoded ISO/IEC 18013-5:2021 mDL (CBOR in this example since the
```

```
requested format was `mdl_iso`)>>
```

以下は ID トークンの例である。presentation_submission が、RP が CBOR で表現された ISO/IEC 18013-5:2021 mDL を VP トークンの中で見つけるのをどのように支援するかを示す：

```
{
  "aud": "https://client.example.org/callback",
  "sub": "9wgU5CR6PdgGmvBfgz_CqAtBxJ33ckMEwvij-gC6Bcw",
  "iss": "9wgU5CR6PdgGmvBfgz_CqAtBxJ33ckMEwvij-gC6Bcw",
  "sub_jwk": {
    "x": "cQ5fu5VmG...dA_5lTMGcoyQE78RrqQ6",
    "kty": "EC",
    "y": "XHpi27YMA...rnF_-f_ASULPTmUmTS",
    "crv": "P-384"
  },
  "exp": 1638483944,
  "iat": 1638483344,
  "nonce": "67473895393019470130",
  "_vp_token": {
    "presentation_submission": {
      "descriptor_map": [
        {
          "id": "mDL",
          "path": "$",
          "format": "mdl_iso"
        }
      ],
      "definition_id": "mDL-sample-req",
      "id": "mDL-sample-res"
    }
  }
}
```

ISO/IEC 18013-5:2021 の mDL を診断表記で CBOR として符号化した、標準的ではない例は、OIDC4VP 仕様の付録にある。

AnonCreds (Anonymous Credentials)

以下は単純な提示の要求で「EuropeanBankIdentity」タイプの資格情報を保有者に依頼している。

```
{
    "response_type":"id_token",
    "client_id":"https://example.com/callback",
    "scope":"openid",
    "redirect_uri":"https://example.com/callback",
    "nonce":"67473895393019470130",
    ...
```

```
    "claims":{
        "vp_token":{
            "presentation_definition":{
                "id":"1",
                "input_descriptors":[
                    {
                            "id": "1",
                            "constraints": {
                                "fields": [
                                    {
                                        "path": [
                                            "$.credentialSchema.id"
                                        ],
                                        "filter": {
                                            "type": "string",
                                            "pattern":
                                    "https://example.com/…/EuropeanBankIdentity.json"
                                        }
                                    }
                                ]
                            }
                        }

                ]
            }
        }
    }
}
```

OpenID Connect はデータ最小化の原則を採用しているため、検証者は「limit_disclosure」プロパティを使用して、以下に示すように、特定の資格情報内の Claim のサブセットのみを要求することができる：

```
{
    "response_type":"id_token",
    "client_id":"https://example.com/callback",
    "scope":"openid",
    "redirect_uri":"https://example.com/callback",
    "nonce":"67473895393019470130",
    ...
    "claims":{
        "vp_token":{
            "presentation_definition":{
                "id":"NextcloudLogin",
                    "input_descriptors":[
                        {
                            "id":"ref2",
                            "name":"NextcloudCredential",
                            "format": {
                                "ac_vc": {
                                    "proof_type": ["CLSignature2019"]
```

```
                                    }
                                },
                                "constraints":{
                                    "limit_disclosure":"required",
                                    "fields":[{
                                        "path": [
                                            "$.schema_id"
                                        ],
                                        "filter": {
                                            "type": "string",
                                            "pattern":
                                    "did:indy:idu:test:3QowxFtwciWceMFr7WbwnM:2:BasicScheme:0¥¥.1
                                    "
                                        }
                                    },
                                    {"path":["$.values.email"]},
                                    {"path":["$.values.first_name"]},
                                    {"path":["$.values.last_name"]}]
                            }
                        }
                    ]
                }
            }
        }
}
```

「limit_disclosure」とともに「constraints」要素が、schema_id、email、first name、last name プロパティのみの開示を要求するために使用されることに注意。(「limit_disclosure」がなければ、「constraints」にマッチする資格情報は、そのすべてのプロパティが返される)。

この例は、検証者が W3C Verifiable Credentials の範囲を超えた形式の資格情報を要求できることも示している。この例では、検証者は「ac_vc 」という形式を使って、いわゆる Anoncred (Hyperledger Indy フレームワークの一部) を要求している。

自己署名付き OP からの応答は、ID トークンと VP トークンという 2 つの成果物から構成される。以下はそれらの成果物の例である。

ID トークンには「presentation_submission」が含まれ、要求された資格情報が結果内で見つかる場所に関するメタデータが含まれる。この場合、資格情報は VP トークンのルートにある資格情報のプレゼンテーション (提示) に含まれる。

```
{
    "iss": "https://self-issued.me/v2",
    "aud": "https://example.com/callback",
    "sub": "did:key:z6MkqUDiu3MHxAm...mscLT8E9R5CKdbtr7gwR8",
    "exp": 1645469476,
    "iat": 1645465876,
    "nonce": "cdb97870-a3be-49b4-aa55-8c7c7122178a",
    "_vp_token": {
        "presentation_submission": {
            "descriptor_map": [
                {
                    "path": "$",
                    "format": "ldp_vp",
                    "path_nested": {
```

```
                    "path": "$.verifiableCredential[0]",
                    "format": "ldp_vc"
                }
            ],
            "definition_id": "1",
            "id": "1"
        }
    }
}
```

そして以下が対応する VP トークンである：

```
{
    "@context":[
        "https://www.w3.org/2018/credentials/v1"
    ],
    "holder":"did:key:z6MkqUDiu3MHxAmuMQ8jjkLiUu1mscLT8E9R5CKdbtr7gwR8",
    "id":"urn:uuid:04816f2a-85f1-45d7-a66d-51764d39a569",
    "proof":{
        "domain":"https://example.com/callback",
        "jws":"...",
        "nonce":"cdb97870-a3be-49b4-aa55-8c7c7122178a",
        "proofPurpose":"authentication",
        "type":"Ed25519Signature2018",
        "verificationMethod":"did:key:z6MkqUDiu3..."
    },
    "type":[
        "VerifiablePresentation"
    ],
    "verifiableCredential":[
        {
            ...
            "type":[
                "VerifiableCredential",
                "EuropeanBankIdentity"
            ],
            "credentialSubject":{
                "id":"did:key:z6MkqUDiu3MHxAmuMQ8jjkLiUu1mscLT8E9R5CKdbtr7gwR8",
                "familyName":"Family001",
                "givenName":"Given001",
                "birthDate":"1950-01-01",
                "placeOfBirth":{
                    "country":"DE",
                    "locality":"Berlin"
                }
            },
            "id":"identity#EuropeanBankIdentity#33665527-50d6-484e-a93a-283ecb8d660b",
            "credential issuer":"did:key:z6MkgF2pvVNEFXCksupWKrdPhL6ubecis3AWbWVsr9bNAbwC",
            "proof":{
                "created":"2022-02-18T19:08:27Z",
                "creator":"did:key:z6MkgF2pvVNEFXCksupWKrdPhL6ubecis3AWbWVsr9bNAbwC",
                "domain":"https://api.preprod.ebsi.eu",
                "jws":"eyJiNjQiOmZhbHNlLCJjcml0IjpbImI2NCJdLCJhbGciOiJFZERTQSJ9..jH-
6rgdVLsvbEE_g2RIDl_AQou4s3DwGg4VE06K3ngvSzm1SKppDvA3UuEfb0dfMrZ_ShTKThM-gxJaUSarwAA",
                "nonce":"7ca07921-26da-4a65-9a2e-781599cc1894",
                "type":"Ed25519Signature2018"
```

```
                },
                "validFrom":"2021-08-31T00:00:00Z",
                "issuanceDate":"2021-08-31T00:00:00Z",
                        }
  ]
}
```

LD 証明フォーマットの VP を直接含んでいる。

なお、PE はバージョン 1.0 が公開されており、バージョン 2.0 は開発中である（2022 年 4 月現在）。バージョン 2.0 はバージョン 1.0 を大幅に簡略化し、実装が必須となるコアサブセットと、オプションの追加クエリー構成要素のセットを導入している。