これからの電子署名に関連した標準化動向

LangEdge,Inc.
有限会社 ラング・エッジ

プログラマ/取締役
宮地 直人

2022年12月23日

はじめに

発表者アイデンティティ>

氏名・所属：宮地 直人（有限会社ラング・エッジ/プログラマ）
Twitter：@le_miyachi
会員：JNSA電子署名WG/JT2A、OIDF-J会員、JIIMA会員
標準化：ISO TC154 メンバー、ISO/IEC JTC1 SC34 リエゾン
東京神田の片隅にある零細ソフトハウス（ぼっち企業）にて電子署名やPDF関連の製品開発をやりつつ標準化活動にも参加中。

宣伝>

2022年7月5日：電子署名保証レベル要約版 を公開しました！
ローカル署名・リモート署名・事業者型署名等のID連携した電子署名の保証レベルをJNSA電子署名WGメンバーで検討してまとめたものです。
是非ご覧ください！
https://www.jnsa.org/result/e-signature/2022/

時代は変わる…過去・現在・未来

第２期なう。時代は変わっても第１期に
作られた仕様標準は使われている。
しかしこれからの新時代（第３期）では
少し様相が変わって来ている…？
今日はその辺りのお話をします。

JNSA 電子署名保証レベル要約版で整理
https://www.jnsa.org/result/e-signature/2022/

電子署名基本
の標準仕様

電子署名 第１期（基礎）

電子署名＝**ローカル署名＋PKI**
長期保管可能なAdESフォーマット
ローカルに署名鍵を所有し利用する
等の仕様標準化が進む

EU電子署名指令
eSignature Directive

電子署名 第２期（ID連携）

クラウドを利用した署名サービス
PKI：ローカル署名からリモート署名へ
ID認証技術標準の取り込みが進む
クラウドで署名鍵を管理して利用する

欧州 eIDAS 1.0
Regulation

電子署名応用と
ID連携の標準仕様

電子署名 第３期（ID融合）

DIW：デジタルIDウォレットの登場
スマホで署名鍵を管理して利用する
属性も自分で管理して利用する（VC）
新しいトラスト構造（DID等）もある

欧州 eIDAS 2.0
Regulation

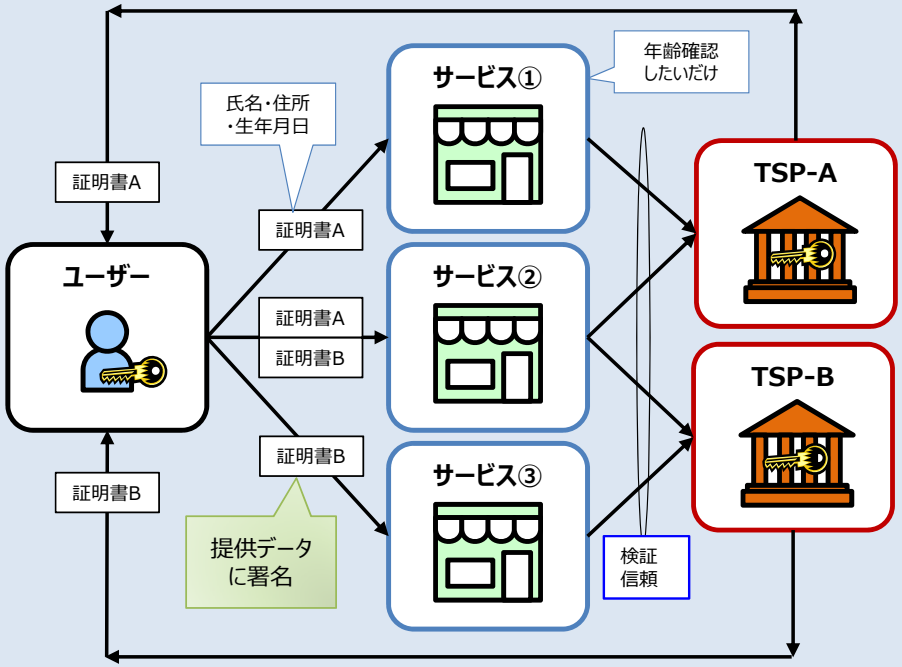
新しいIDと電子署名の標準仕様
※仕様策定が現在進行中

署名鍵の所有管理
の方法が変わるよ。

パラダイムシフトがおこる…かも？

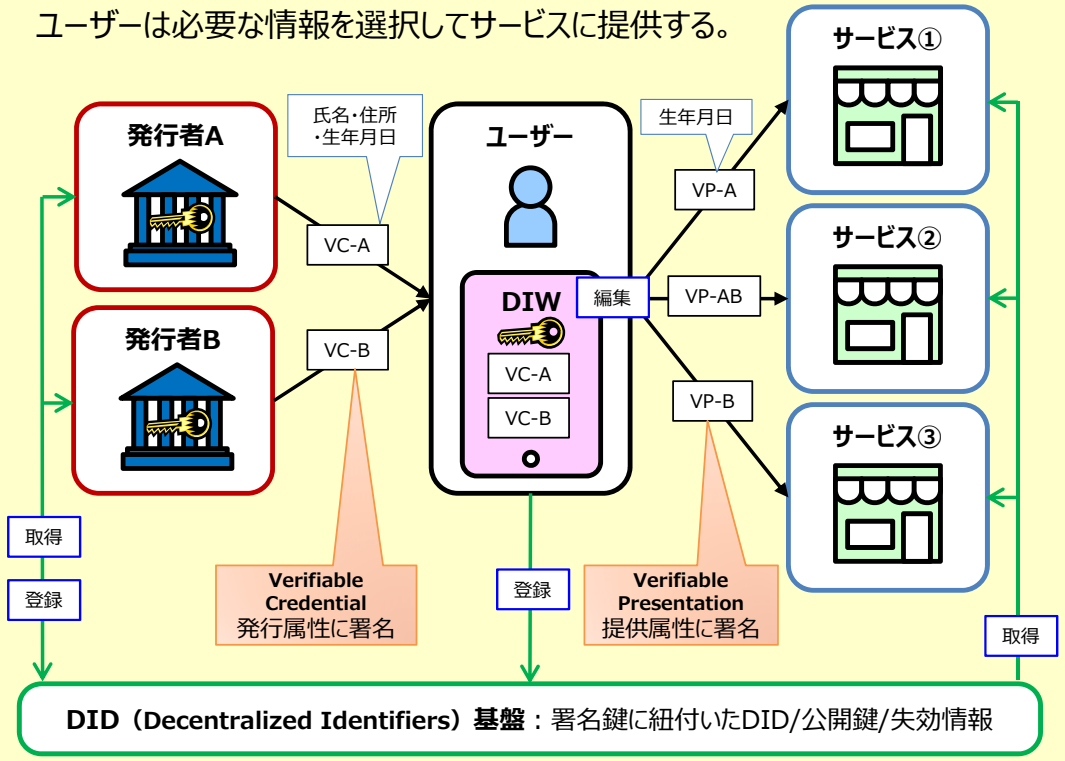
中央集権的な現在のモデル例
（ローカル署名＋PKIの例）

サービスはTSP（認証局等）を直接信頼して接続する。
サービスとTSPの数だけ相互接続されているので複雑。
ユーザーは署名した情報をサービスに提供する。



自己主権型アイデンティティのモデル例
SSI（Self-Sovereign Identity）

ユーザーのDIWを中心としたモデルとなる。
発行者はユーザーの身元確認した上でVCを発行する。
ユーザーは必要な情報を選択してサービスに提供する。



W3C: Verifiable Credentials Data Model

Verifiable Credentials はW3Cが標準化したデータモデルにすぎないが、
現在生じている新しい動きは全てVCが関連している。以下の関係図がベースとなる。

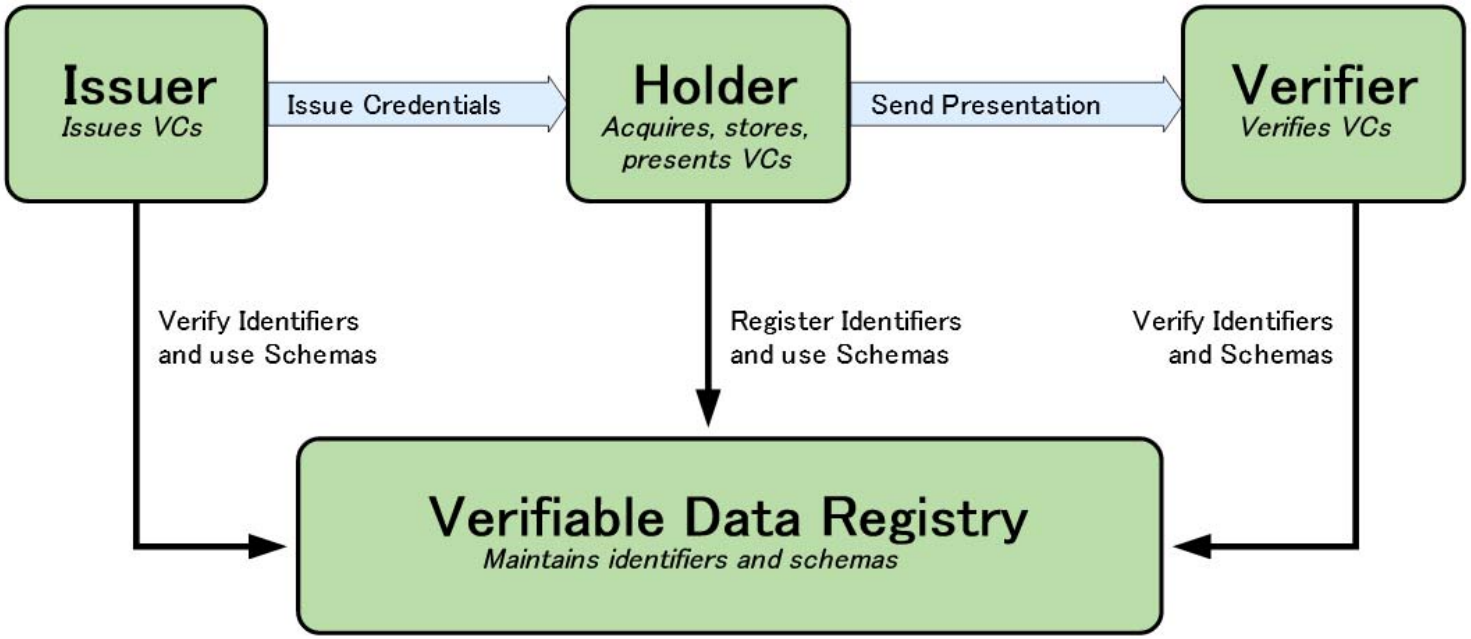


Figure 1 The roles and information flows forming the basis for this specification.

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

W3C: Verifiable Credentials 関連仕様

検証可能クレデンシャル：VC（Verifiable Credentials）
https://www.w3.org/TR/vc-data-model/
自己主権型のデジタル個人情報の集合体（アイデンティティ）を保証する、JSONベースのデジタル証明書の基本データ仕様。
ゼロ知識証明などの技術の組み合わせにより、個人情報の個人による「選択的最小開示」を実現することが出来る。
VCを使って卒業証明書や運転免許証等のデジタル証明書を実現することが出来る。

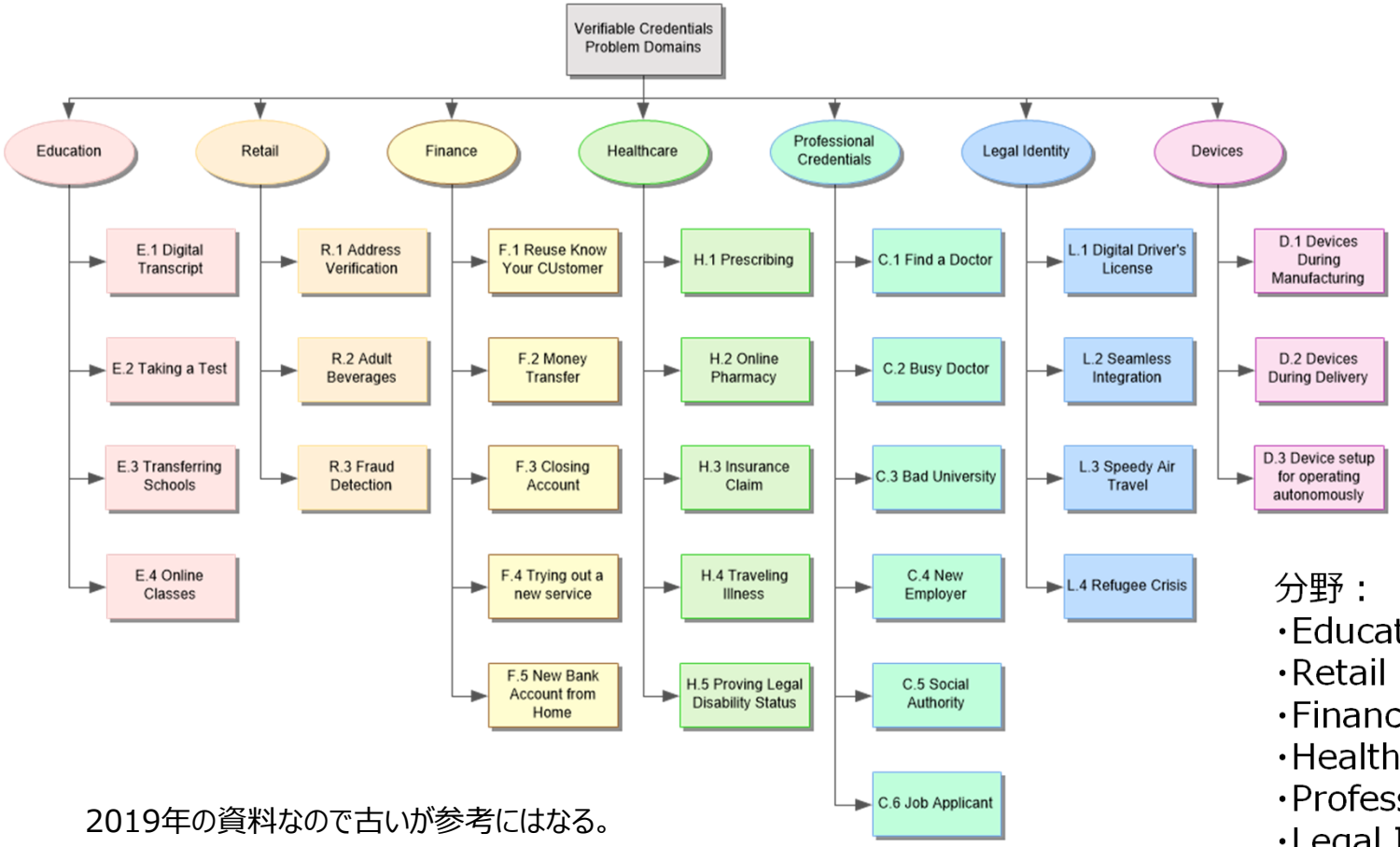
分散型ID：DID（Decentralized Identifier）
https://www.w3.org/TR/did-core/
IdP（IDプロバイダ）に依存しないURI形式のID仕様。
鍵に紐付いたIDであり、“DID Document” で検証に必要な公開鍵やエンドポイントを示す情報を公開する。
形式："did:メソッド:メソッド内の識別子"
メソッドの一覧：メソッド間は相互運用できない
https://w3c.github.io/did-spec-registries/
※ メソッドにはブロックチェーンが多いが必須では無い。

デジタルIDウォレット：DIW（Digital Identity Wallet）
スマホ上で動作するアプリであり、鍵の管理とデジタル署名やVCの管理を行うことが出来る。
鍵の保持方法はスマホのハード/システムに依存する。

Verifiable Credentials 例


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.edu/credentials/1872",
  "type": ["VerifiableCredential", "AlumniCredential"],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "alumniOf": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
      "name": [{
        "value": "Example University",
        "lang": "en"
      }, {
        "value": "Exemple d'Université",
        "lang": "fr"
      }]
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2017-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://example.edu/issuers/565049#key-1",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
      X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtj
      PAYuNzVBAh4vGHSrQyHUdBBPM"
  }
}
```

W3C: Verifiable Credentials Use Cases



2019年の資料なので古いが参考にはなる。

https://www.w3.org/TR/vc-use-cases/

- ASN.1・BER/DERのX.509に比較するとJSONベースなので可読性が高くテキストエディタで開いてもある程度把握できる。
- ワクチン接種証明書はVCで記述されている。デジタル署名としては楕円曲線暗号が使われている。

分野：
・Education（教育）
・Retail（小売）
・Finance（金融）
・Healthcare（ヘルスケア）
・Professional Credentials（資格証明書）
・Legal Identity（公的証明書）
・Devices（デバイス）

VCとDIWをめぐる世の中の動向

欧州：EUDIW（EU Digital Identity Wallet）

- 欧州委員会が推進、eIDAS 2.0の目玉であり ISO 23220 シリーズ他の標準準拠も推進。
- 2023年初頭に実装の実証となるToolkitを公開予定（2022年秋公開から遅延中）。
- Toolkitの実証実験後にEU各国は自国向けにEUDIWの実装をおこなう必要がある。
- 国民ID・電子旅券・mDL・国家資格・学位証明書等、幅広いVCを取り込む予定。

OAuth/OIDCやFIDOとは連携しているがスマホのプラットフォーマー（Apple/Google）の影が薄い気がする…

米国：mDL（モバイル運転免許証/mobile Driver's License）

- **Apple** Wallet に実装。**Google** Wallet でもベータ実装している模様。
- アリゾナ州、コロラド州、アイオワ州、オクラホマ州、ユタ州、ワイオミング州等で開始または予定。
- ISO 18013-5 定義の mdoc データモデルを利用、ISO 23220 シリーズにも準拠。

Microsoft：Microsoft Entra リリース（2022年5月31日）

- Azure AD・CIEM・Verfied ID（VC）等を統合したあらゆるIDを管理するID統合製品。
- Microsoft Entra Verified ID のドキュメント：
  https://learn.microsoft.com/ja-jp/azure/active-directory/verifiable-credentials/
- 現在はDIDとしてブロックチェーンを使わない "did:ion:ロングフォーム" を利用。
  ※ "ion" は本来BitCoinを使ったメソッドでBitCoinはショートフォームにて使われる。

OpenID：OpenID 4(for) Verifiable Credentials

- OpenID4CI・OIDC4VP・SIOPの3つで構成されたOAuth/OpenIDのVC拡張仕様。

DIWと電子署名の関係

DIW利用で考えられるのは以下の３パターン。ただしローカル署名として使われる可能性は低そうに思える。
EUDIWにおいても手探り状態のようで最初はVCとリモート署名の2つが混在して使われる可能性もある。

利用方法	説明
Verifiable Credentials	DIDではなくPKIを使ったJSONベースのデジタル署名でVCを利用する。 もちろんブロックチェーン等を使ったDIDを利用しても良いが、電子署名として考えると従来のPKIを信頼層に使った方が馴染みやすいだろう。VCで何が出来るのかまた従来の電子署名的な用途は何か等はこれから考えて行く必要がある。DIW本来の利用方法でありだんだん増えて行くと予想される。
リモート署名の署名認可	DIWをリモート署名認可のID認証器として利用する。 ID認証器としての利用はDIWの本来の用途ではないと言えるかもしれないが、現実的な利用方法であるとは言える。eIDAS2.0で言えば比較的容易にQualifiedなAdESのリモート署名を実現できる。またオンラインの身元確認にも使える。
ローカル署名	DIWでAdES等の既存のデジタル署名を利用する。 正直を言って署名鍵を安全にスマホに保存できるのであればDIWでローカル署名する意味はあまり無いと言える。おそらくローカル署名としての利用は少ないかほぼ無いと予想される。またオンラインの身元確認にも使える。

ISO: Verifiable Credentials 関連仕様

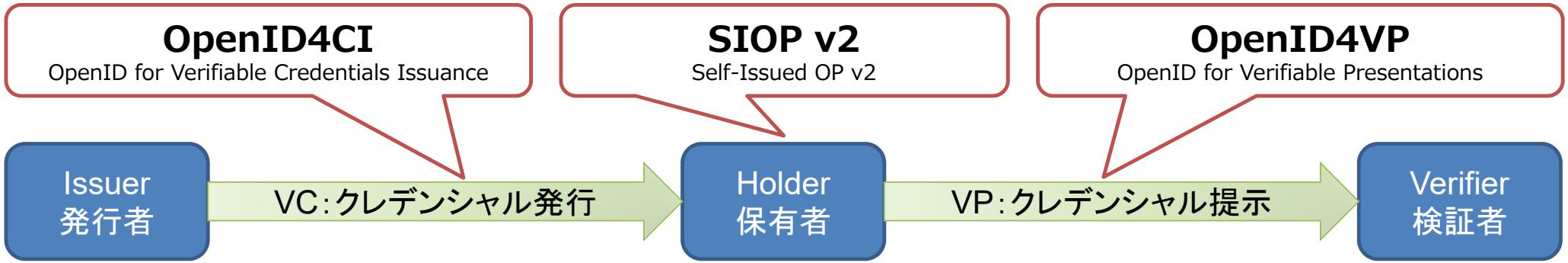
ISO/IEC 18013 Series : Personal identification - ISO-compliant driving licence		
18013-5:2021	Published	Part 5: Mobile driving licence (mDL) application https://www.iso.org/standard/69084.html
18013-6	AWS TS	Part 6: mDL test methods https://www.iso.org/standard/79805.html
18013-7	AWI TS	Part 7: Mobile driving licence (mDL) add-on functions https://www.iso.org/standard/82772.html

mDL
mobile Driver's License

ISO/IEC 23220 Series : Cards and security devices for personal identification - Building blocks for identity management via mobile devices		
23220-1	FDIS	Part 1: Generic system architectures of mobile eID systems https://www.iso.org/standard/74910.html
23220-2	AWI TS	Part 2: Data objects and encoding rules for generic eID systems https://www.iso.org/standard/79124.html
23220-3	AWI TS	Part 3: Protocols and services for issuing phase https://www.iso.org/standard/79125.html
23220-4	AWI TS	Part 4: Protocols and services for operational phase https://www.iso.org/standard/79126.html
23220-5	AWI TS	Part 5: Trust models and confidence level assessment https://www.iso.org/standard/79127.html
23220-6	AWI TS	Part 6: Mechanism for use of certification on trustworthiness of secure area https://www.iso.org/standard/80776.html

mobile eID systems

OpenID: Verifiable Credentials 関連仕様



OpenID4CI: OpenID for Verifiable Credentials Issuance (27-Oct-2022)

VC（クレデンシャル）発行に関する仕様。既存のOIDCのRP/OPとの相互運用を実現する。
https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

OpenID4VP: OpenID for Verifiable Presentations (6-Sep-2022)

クレデンシャルを提示するVPの仕様。検証者がOIDCを通じてDIWと接続できるようになる。
https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

SIOP v2: Self-Issued OP v2 (6-Sep-2022)

保有者自身でOPとして運用（self-issued ID Tokensの発行等）する為の仕様。v1からVP/DID等の拡張。
https://openid.net/specs/openid-connect-self-issued-v2-1_0.html

DIWとVCに関連した技術選択肢

コンポーネント	技術標準
ウォレット	EUDIW Toolkit, OpenWallet (Linux Foundation), Apple Wallet, Google Wallet
鍵保護 （署名鍵）	GP-SE (Secure Element), GP-TEE (Trusted Execution Environment), HSM, SIM ※ GP=Global Platform
公開鍵	W3C DID method, X.509 Certificate (PKI), Raw Keys
暗号	RSA, ECDSA, EdDSA, 耐量子暗号
EAAフォーマット （EAA:属性証明書）	オンライン：X.509 Certificate, W3C Verifiable Credentials, ISO/IEC 23220 オフライン：ICAO Doc 9303 (Visa/Passport), ISO 18013-5 (mDL), ISO/IEC 23220
署名フォーマット	AdES (ETSI/ISO 14533), RFC 7515 JWS, SD-JWT (SD=Selective Disclosure)
失効	W3C Status List 2021, X.509 CRL, RFC 6960 OCSP
信頼	EU Trusted List, X.509 PKI Domain, Verifiable Data Registry, OIDC Federation

見たことがある技術も
見たことがない技術も
新旧色々ある。

まだまだカオスな状況が続きそうです。
多くのベンダーも様子見しつつ主流に
なる技術を見極めようとしています。

最後に: Verifiable（検証可能）と言うこと

電子署名で生成する署名データはVerifiable Data（検証可能データ）です。その意味からJNSA電子署名保証レベルでは署名データの保証レベルとして**VDAL**を設定しました。
（※ VDAL: Verifiable Data Assurance Level）

ゼロトラストの観点から見ても検証することで信頼を得ることからVerifiableと言うことが非常に大事になっています。

Verifyする為にはIdentityの利用または融合が必要となります。これからは　電子署名も単純にドキュメントやデータにデジタル署名するだけではなく、様々なデジタル証明書であるVC（Verifiable Credentials）を組み合わせてサービスを構築し利用して行く必要があるでしょう。つまり新しい**Verifiableな世界**が来そうです。

ただしVerifiableな世界はまだ完成していません。欧州でも米国でも巨大企業でも色々なところで色々な仕様検討や試行錯誤が行われていますがまだ数年はかかるでしょう。今ならまだ間に合いますし、新しい世界や新しい技術を勉強することはとても楽しいです。まずは色々な標準技術を調べてみましょう。本資料がその一助になれば幸いです。