

教育機関におけるVerifiable Credentials 実証事例と今後の展開

2023/10/31

伊藤忠テクノソリューションズ株式会社

一般社団法人 OpenID ファウンデーション・ジャパン/代表理事

米国OpenID Foundation/共同議長 eKYC&IDA WG

富士榮 尚寛 (ふじえ なおひろ)



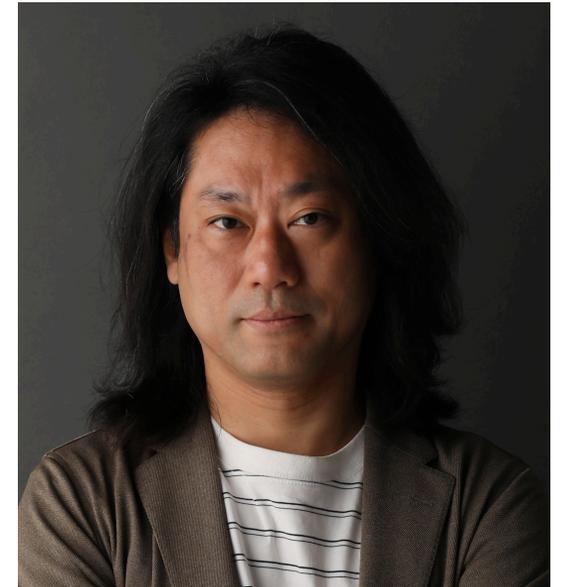
富士榮 尚寛 (ふじえ なおひろ)

自己紹介

- デジタルアイデンティティ分野で約20年の経験を持ち、大手自動車製造業のグローバルID基盤に関するコンサルティング～PMなどを歴任。
- 2018年よりOpenIDファウンデーション・ジャパンの理事に就任、KYC WGを設立。2020年1月より米国OpenID FoundationにてeKYC and Identity Assurance Working Groupの設立および共同議長に就任。2021年6月よりOpenIDファウンデーション・ジャパンの代表理事に就任。
- CTCではID基盤サービス「SELMID」の責任者

各種役割

- OpenIDファウンデーション・ジャパン代表理事/KYC WG発起人
- 米OpenID Foundation/eKYC&Identity Assurance WG共同議長
- 日本ネットワークセキュリティ協会/デジタルアイデンティティWG, ISOリエゾン
- 内閣官房Trusted Web推進協議会TFメンバ
- 国立情報学研究所/次世代認証連携検討作業部会メンバ
- 大学ICT推進協議会/認証基盤部会
- Microsoft MVP (2010年～)、Auth0 Ambassador、LINE API Expert



教育機関における証明書とデジタル化

様々な証明書が存在

- マクロクレデンシヤル（在学証明、学位、卒業証明など）
- マイクロクレデンシヤル（学修歴、出席など）

デジタル化（Digitization vs Digitalization）

- Digitization：単純にデジタル化する（PDF化など）
- Digitalization：機械可読な状態にする

デジタル化の意味

段階は様々

- 紙の削減（エコ的な意味）
- 高い利便性の提供
- 今までよりもセキュアで信頼できる
- 今まで出来なかったことを出来る様にする

→せっかくなら今まで出来なかったことをやりたい

※どうしても技術者の視点で真正性の担保、などに行ってしまうがちだが、ユースケース作りにはあまり役に立たない（個人的実感）

紙とデジタルの違いを正しく認識する

		紙プロセス	デジタルプロセス
前提		対面前提	オンライン前提
やりとりする相手との関係性	距離	近い	距離は関係ない
	信頼関係の構築	周辺環境や相手に関する様々な情報（容姿や振る舞いなど）を含め総合的に判断（感覚・経験による判断）～信頼	得られる情報は限定的であり、第三者によるお墨付きや技術面のサポートが必要（デジタル署名など）
	プライバシー	人は忘れる、という特徴あり	デジタルタトゥーとして残る可能性あり
証明書	保存期間	どちらかという利用者依存（長期保管されるケースも多い）	どちらかという発行者依存（トランザクション内のみの短期利用が多い）
	偽造	ハードルが高い（コスト・心理的障壁）	ハードルが低い（容易なデジタルコピー）



この辺りがVCで解決出来そう
（前段で語られているので省略）

その上でユースケースを分類

相手との距離、偽造によるインパクト

本来デジタル化で
メリットがあるケース

		相手との距離が	
		近い（対面）	遠い（オンライン）
偽造されると	困る	対面であってもリスクがある （無人シナリオ。後からトレースしても手遅れ） 例） • 鍵としての利用	なりすましやフェイクによるリスクがある （無人シナリオ。後からトレースしても手遅れ） 例） • オンライン申請 • 電子チケット、定期券 ※利用されてしまうと取り戻せない
	困らない	対面によりリスク低減ができる （有人。後から取り消せる・取り戻せる） 例） • ポイントカード	検証できなくてもリスクは低い （後から取り消せる・取り戻せる） 例） • 金銭等を伴わないカジュアルなサービス

従来のデジタル化の
アプローチ

証明書という特性からの分類

情報鮮度（結合度）、権威の必要性

ID連携では実現しにくかった領域

		鮮度（結合度）	
		重要 （付与されてすぐに利用）	それほどでもない （付与と利用の間に時間的なラグあり、または疎結合でシステム間での連携が困難）
権威	重要	認証、属性ベースの認可 (認証結果の伝達によるログイン・SSO、組織や役職によるアクセス制御)	身分証明、資格証明 (学位、ワクチン証明書、学修歴証明など)
	それほどでもない	リスクベース認証、動的認可 (IPアドレスや場所などのコンテキストベースの認可)	個人ベースの情報、評判 (個人端末/Walletに関する情報、レピュテーションなど)

従来のID連携の
アプローチ

まとめると

こんなケースに適用すると良さそう

- オンライン（非対面）での利用が前提
- 偽造されると困る
- 発行元の権威が必要
- 鮮度はそれほど求められない

ユースケースを分析

基本的に発行側ではなく検証側の目線で考える

事例	シナリオ	オンライン前提 (非対面?)	偽造されると困る (取り戻せない?)	権威が必要 (発行元が大事?)	鮮度は求めない (ID連携ではNG?)
慶應での実証実験	映画の割引チケット	× 最後は窓口	○ 使ったら終わり	△ それほど?	○ 映画館とID連携?
	卒業生向けサービス ログイン	○ 窓口に来にくい	○ セキュリティ大事	○ 経歴ロンダリング	△ 卒業生ID管理?
NIIでの実証実験	サービス利用の要件 とする (認可)	○ オンライン受講前提	○ セキュリティ大事	○ トラスト大事	○ 疎結合でスケール
EIC '19でのデモ	ゲストのKYC	○ 窓口に来にくい	○ セキュリティ大事	○ トラスト大事	○ 疎結合でスケール

次世代デジタルアイデンティティ基盤 @ 慶應義塾

在学・卒業証明等の個人証明をスマホアプリに載せ利用者自身が持ち運ぶ世界観の実現を目指す実証実験

- ・ オンライン・オフラインの両方で利用可能な身分証明書
- ・ オンライン利用時に従来のID基盤と異なりID発行元へ問い合わせがないことによる可用性・スケール確保
- ・ 分散台帳を利用することで証明書の真正性確認が可能

慶應義塾大学、次世代デジタルアイデンティティ基盤の実証実験を開始 在学証明書や卒業見込証明書をスマートフォンアプリへ発行

2020/10/26

慶應義塾大学

伊藤忠テクノソリューションズ株式会社

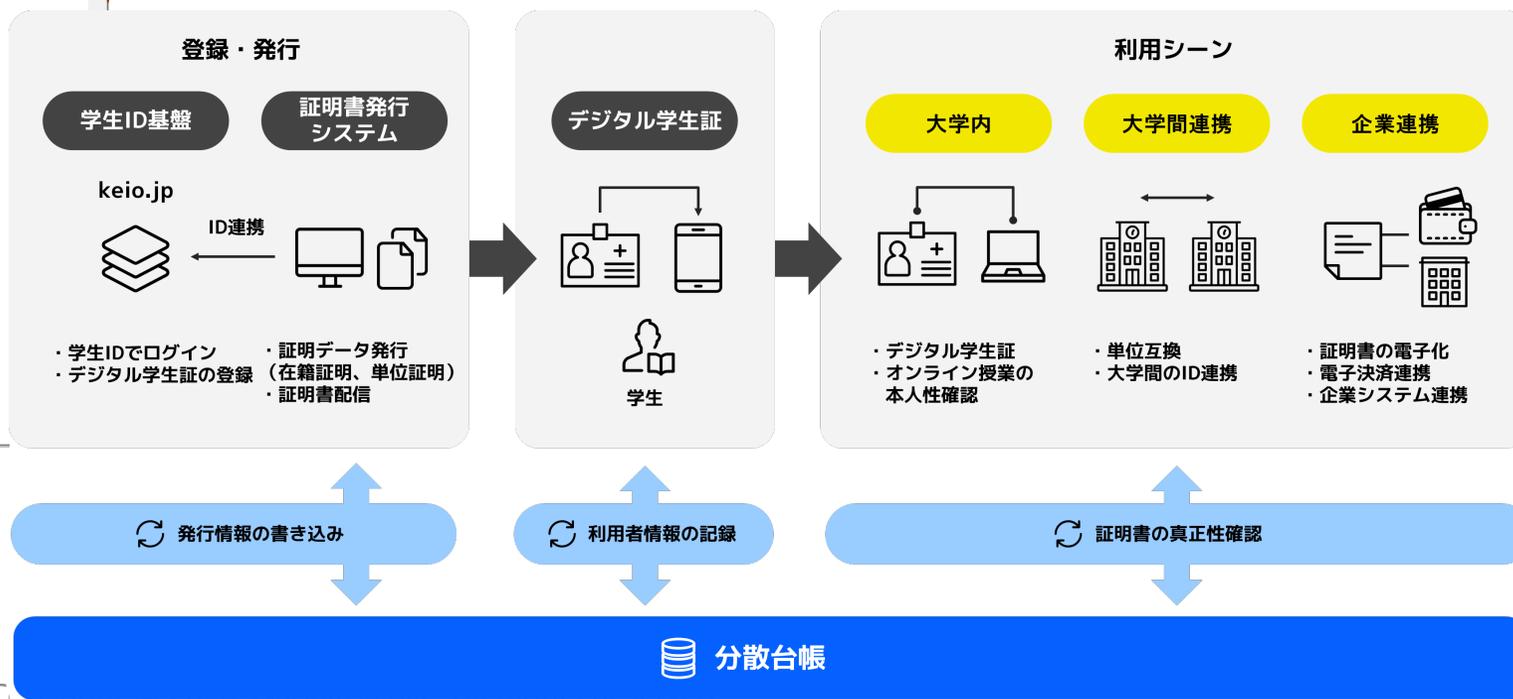
Japan Digital Design株式会社

株式会社ジェシービー

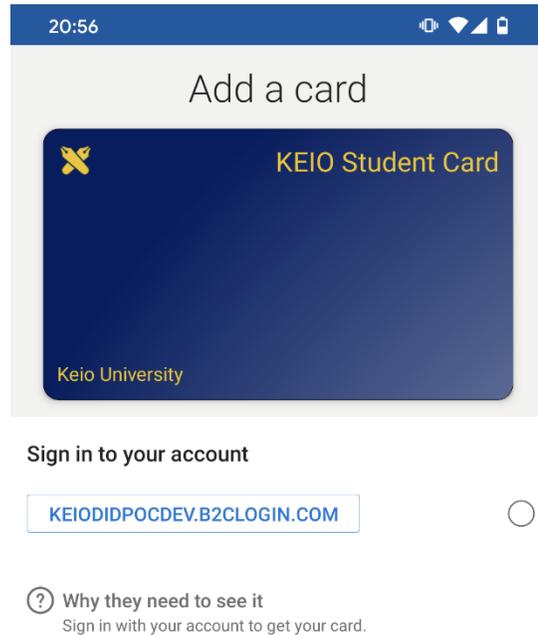
西日本電信電話株式会社

BlockBase株式会社

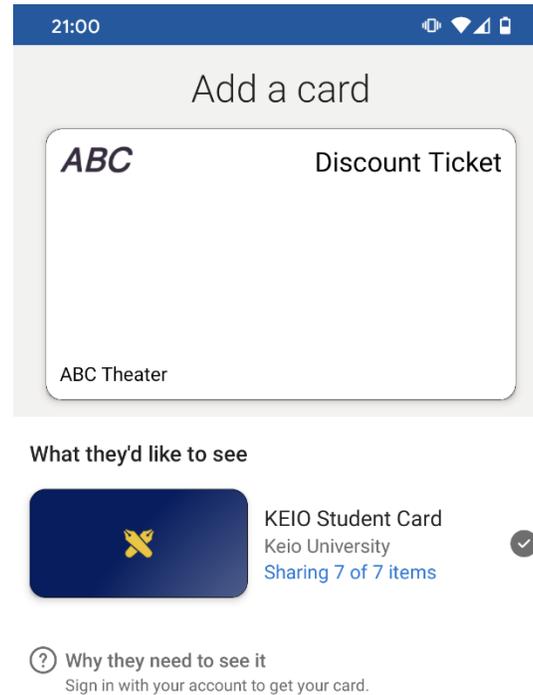
慶應義塾インフォメーションテクノロジーセンター（所長：中村 修）と慶應義塾大学SFC研究所ブロックチェーン・ラボ（代表：村井 純、副代表（技術統括）：鈴木 茂哉）は、伊藤忠テクノソリューションズ株式会社（代表取締役社長：柘植 一郎）、Japan Digital Design株式会社（代表取締役CEO：上原 高志）、株



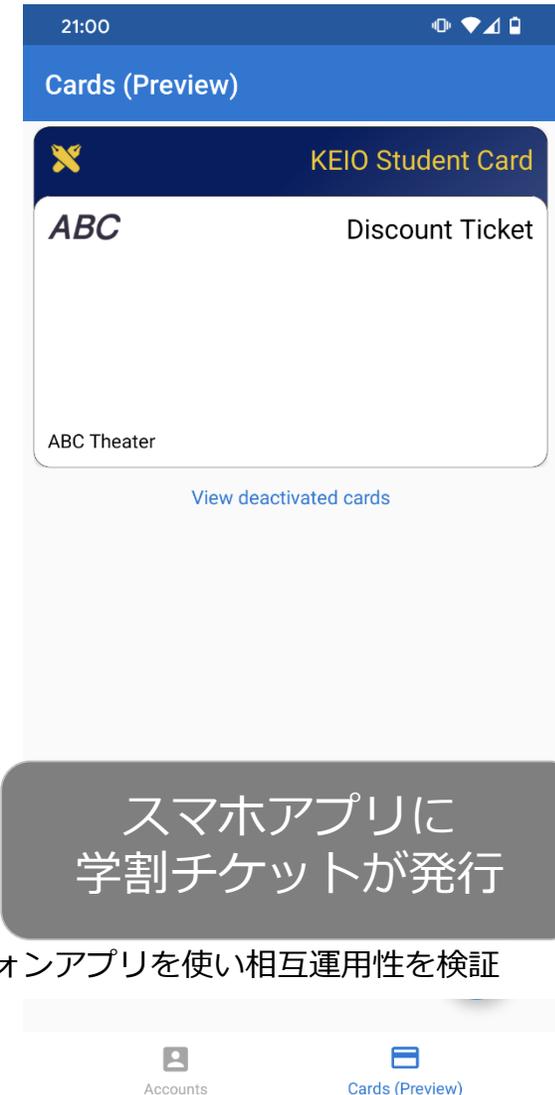
学生証を提示して学割チケットを入手する例



スマホアプリに
デジタル学生証を発行



デジタル学生証の提示
学割チケットを取得



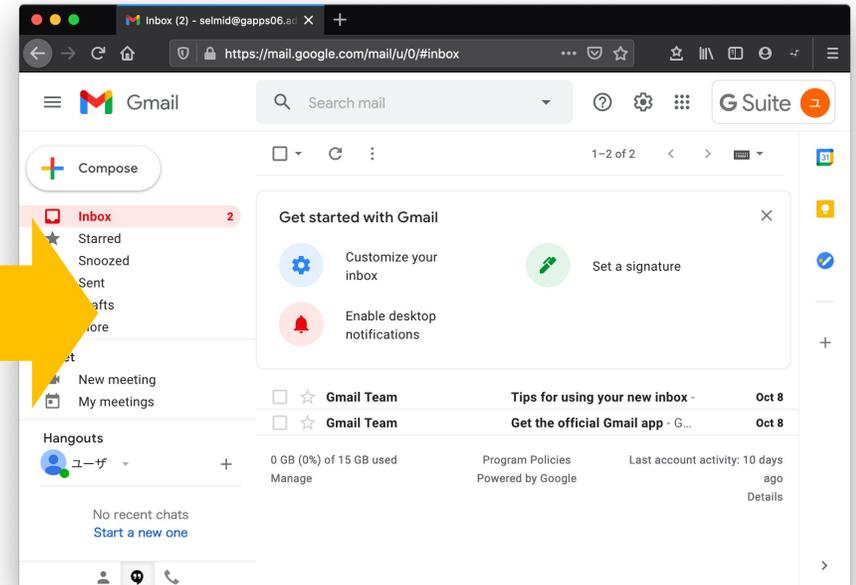
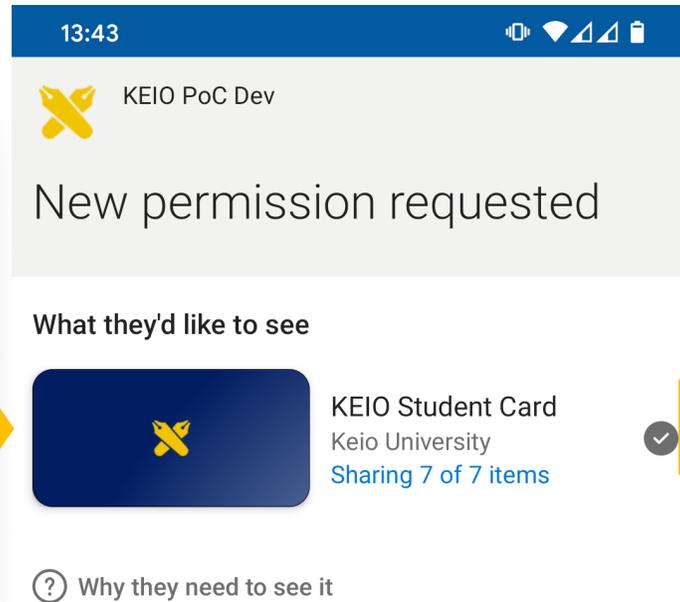
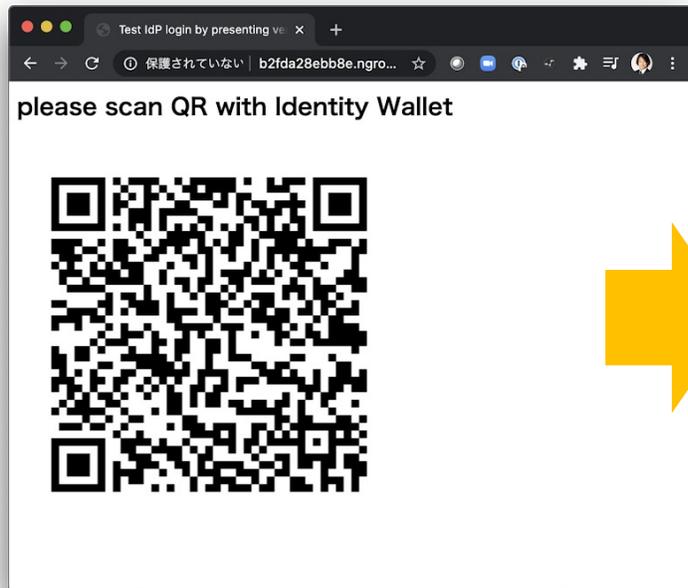
スマホアプリに
学割チケットが発行

※技術標準に対応した複数種類のスマートフォンアプリを使い相互運用性を検証



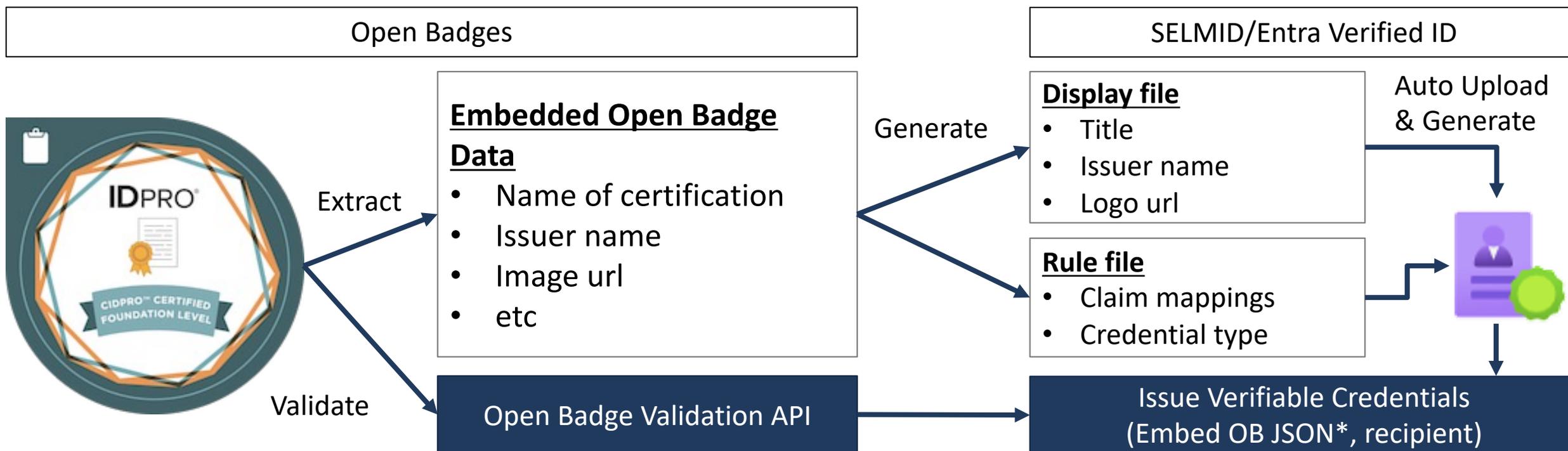
デジタル学生証でWebサイトへログインする例

- Webサイトを開き、QRを表示
- スマホアプリ（デジタル学生証）でQRを読み込み
- ログイン完了



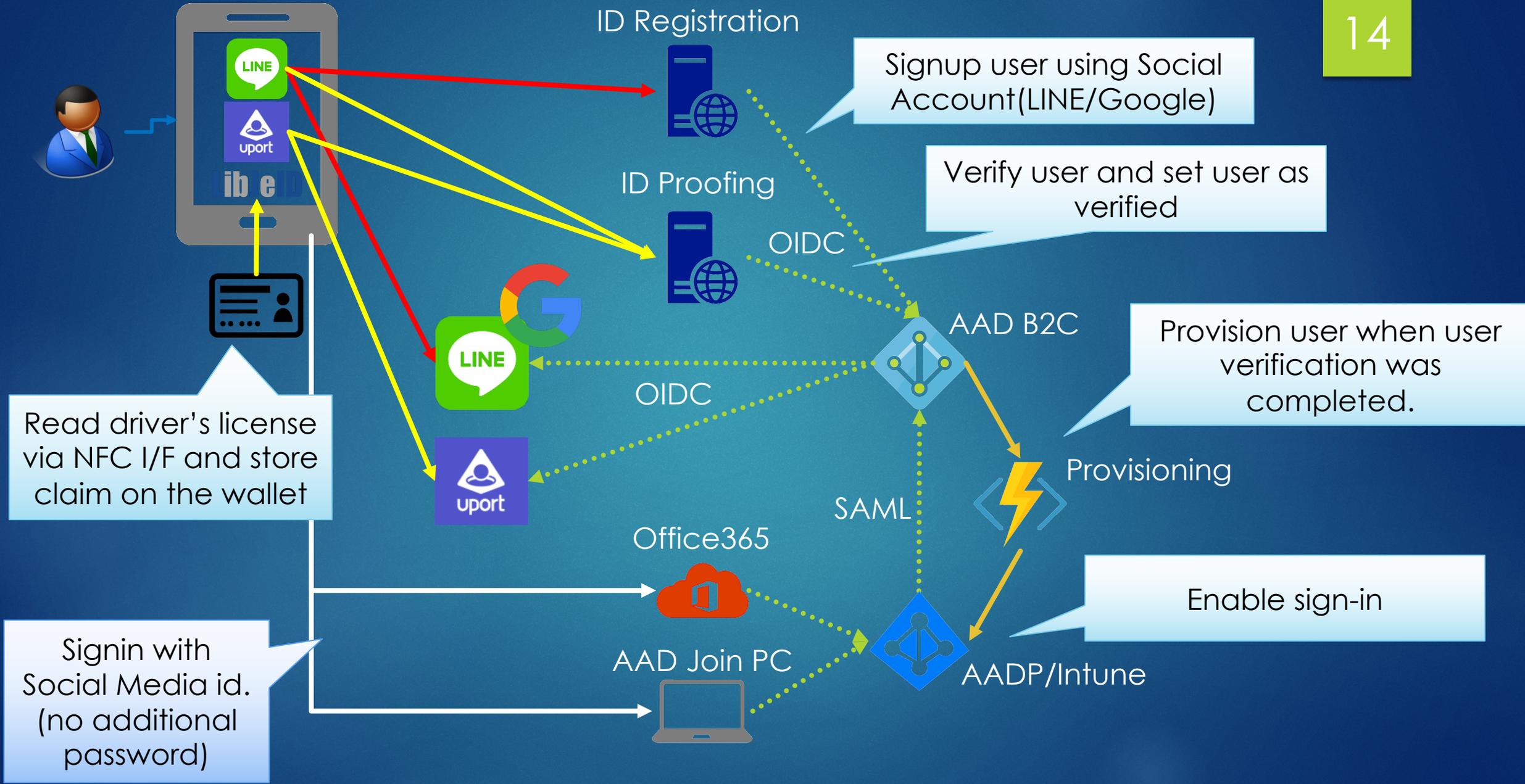
Microsoft Decentralized Identity Hackathonで3位入賞

- 発行済みOpenBadgeをVerifiable Credentialへ変換し、Walletへ格納する
- 検証者はVCの真正性に加えてOpenBadgeの検証も実施



* Verifiers are able to validate OB after verify VC

Overview



ID Registration

Signup user using Social Account (LINE/Google)

ID Proofing

Verify user and set user as verified

OIDC

AAD B2C

Provision user when user verification was completed.

OIDC

Provisioning

Read driver's license via NFC I/F and store claim on the wallet

SAML

Enable sign-in

Office365

Signin with Social Media id. (no additional password)

AAD Join PC

AADP/Intune

次のステップで行うべきこと

検証者の増加を目指し、次に発行者（大学等）へ

出口シナリオ		オンライン前提 (非対面?)	偽造されると困る (取り戻せない?)	権威が必要 (発行元が大事?)	鮮度は求めない (ID連携ではNG?)
例) 交通系	学生周遊券購入	○ 現在、学生はオンラインで学割不可	○ 使ったら終わり	○ トラスト大事	○ 疎結合前提
	入場券で割引	△ 最終的には対面だが、インバウンド送客に効果あり	○ 使ったら終わり	△ それほど?	○ 疎結合前提
	モバイル学生定期	○ 現在、学生はオンラインで定期が発行不可	○ 不正防止大事	○ トラスト大事	○ 疎結合前提

まとめ & おさらい

- 「デジタル化」の意義を考えて適合するユースケース検討を！
- トラスト・真正性ばかりに目をやらずに「今まで出来なかったこと」の実現に寄与できるシナリオ→検証者にとってメリットのあるシナリオにフォーカスを！