Trusted Web の実現に向けたユースケース実証事業

要件定義書

令和 6 年

電通総研

目次

1. 実証の目的

Trusted Web を活用することで、エンティティ間をまたいだ情報のトラストが検証できるようになり、KYC/KYB に関する証明書の発行者が検証可能な証明書（VC：Verifiable Credentials）を提供できるようになれば、KYC/KYB のデータの再利用が可能となって効率化され、トラストのある取引を促進する可能性がある。 本実証事業では、2022 年度の補助金・給付金に関する実証事業に関連する金融機関のユースケースを取り上げ、「金融機関における法人口座の開設」を例に、KYC/KYB に基づいたトラストのある取引を促進する新しい仕組みの検討と検証を行う。

2. システム概要・主体

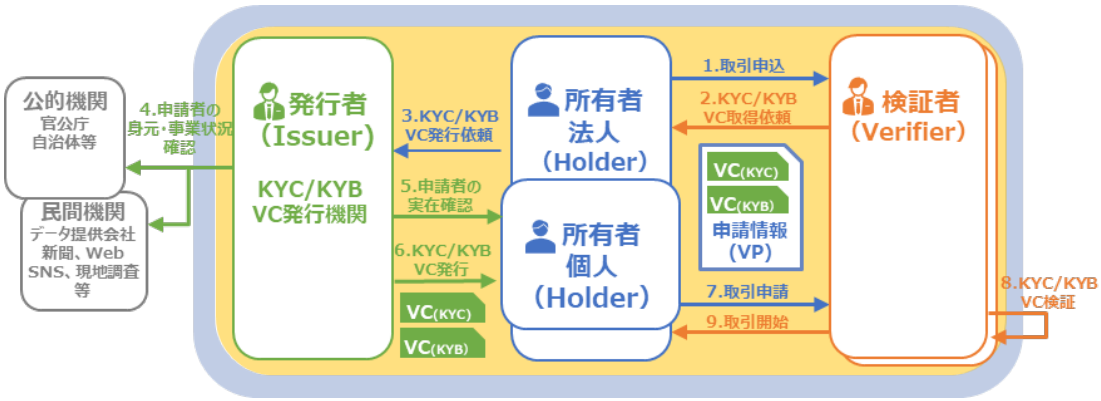

図 2.1 システム概要図

本事業の業務面は、金融機関等を対象とした eKYC 事業で数多くの実績がある ACSiON（アクシオン）と共に、KYC/KYB の VC 発行サービスの検討を行い、金融機関の協力を得てプロトタイプシステムを用いた実証実験を行う。またシステムアーキテクチャ面は OAuth2.0 と OpenID Connect（OIDC）のコア機能を API として提供している Authlete が参加 し、Authlete が最新仕様を同社製品に追加実装する OID4VCI をプロトタイプシステムのアーキテクチャに組み込む。

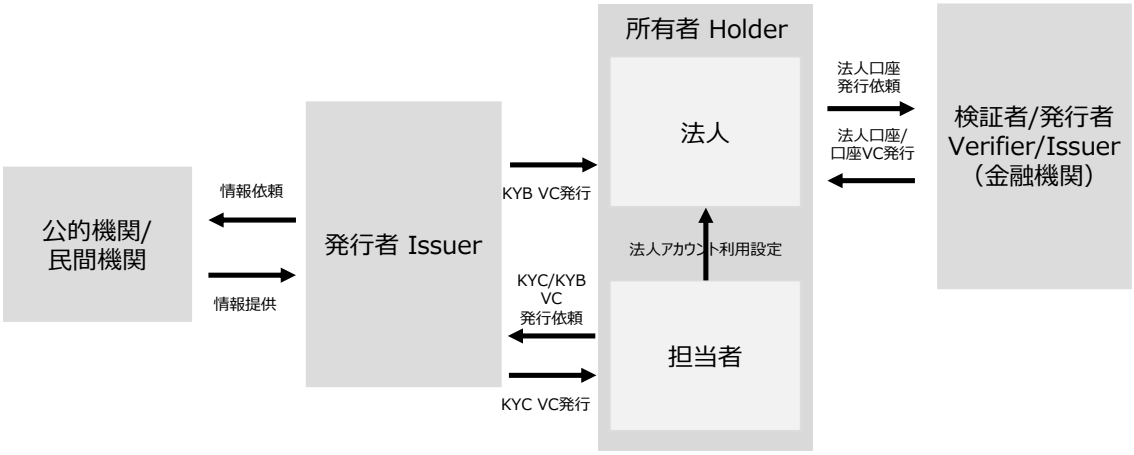

図 2.2 登場する主体

本事業は、これまで各金融機関においてアドホックに行われていた法人や個人の本人確認等の業務に、Trusted Web を活用した Issuer -Holder-Verifier モデルを導入し、Verifier は Issuer が発行する VC を信頼することで Holder と Verifier の業務効率化を期するものである。

- 所有者（法人）
  【役割】
  - 法人に関する本人確認証明書（以後 KYB VC）を検証者（金融機関）へ提出する。

  【課題】
  - 取引先である検証者（金融機関）が要求する法人の本人確認に関する情報・資料は、現状、複数の機関から取り寄せる必要がある。これを Issuer が発行する VC に集約することで、速やかにかつ手間なく提出したい

- 所有者（担当者）
  【役割】
  - 所有者（担当者）の個人の本人確認に関する VC（以後 KYC VC）の発行を発行者に依頼する。
  - 担当者は当該申請法人に在籍していることの証明書（雇用証明書・在籍証明書等）を提出し、在籍確認 VC の発行を発行者に依頼する。
  - 発行者に対して KYB VC の発行を依頼する。その際、KYC VC と在籍確認 VC を提示する。

  【課題】
  - 必要な本人確認、在籍確認を手間なく実施したい

- 発行者
  【役割】

- 所有者（担当者）の身元確認、企業に所属しているかどうかの確認を行い、それぞれの証明書を発行する
- 所有者（担当者）からの KYB VC 発行の依頼を受け、公的機関/民間機関に対し、KYB に必要となる情報の取得・確認要求を行い、所有者（法人）に KYB VC を発行する

【課題】

- KYB VC は、法人の本人確認に関する VC であるため、所有者や検証者、公的機関/民間機関の第三者である発行者が、公的機関/民間機関から KYB VC の発行に必要となる信頼できる情報を取得可能な環境を整備する必要がある。

- 公的機関/民間機関

【役割】

- 発行者からのリクエストに対して KYB に必要な情報（商号・名称、所在地、役員、代表者等）を提供する

【課題】

- 情報の取得者を確認し、正当な取得希望者に対して情報を提供することは可能だが、情報取得に関する申請に時間を要し、また取得する情報のフォーマットも取得する情報毎に異なる。

- 検証者/発行者（金融機関）

【役割】

- 所有者から、発行者が発行した VC を受け取り、口座開設に必要な手続きを実施する。
- 手続きが完了し、口座開設が完了した場合、口座 VC を発行する。

【課題】

- 顧客法人である所有者（法人）に関する KYB VC を速やかに手間なく取得したい

3. 実験企画

- 実施内容

  デモ動画による説明を行い、プロトタイプシステムを用いてロールプレイを実施予定。

- プロトタイプシステム

  KYC VC と KYB VC を発行し、法人口座開設までの流れを体験するシステム。プロトタイプシステムは一般公開しない。

- ステークホルダー(ヒアリング対象先)

  金融機関： 2 行

申請者(法人)：2 社

- 実施内容
  アプリは公開せず、デモ動画による説明を行い、プロトタイプシステムを用いてロールプレイを実施予定。

- 実施期間：約 1 ヶ月間

- スケジュール
  7 -8 月：参加者調整、ヒアリング開始
  9 月-10 月：KYC/KYB 調査、ヒアリング、ユースケース検討
  11 月：プロトタイプテスト実施
  12 月：実証実験実施、アンケート
  1 月：振り返り、最終報告書作成

4. 機能/非機能要件

機能/ 非機能	機能名	機能概要
機能	アカウント管理	VC 発行の申請を行うための個人・法人のアカウント管理機能
機能	KYC VC 発行申請	所有者が口座開設に必要な KYC VC の発行を申請する機能
機能	在籍証明 VC 発行申請	所有者が口座開設に必要な在籍証明 VC の発行を申請する機能
機能	KYB VC 発行申請	所有者が口座開設に必要な KYB VC の発行を申請する機能
機能	口座開設申請	所有者が口座開設の申請を行う機能
機能	デジタル証明申請一覧	過去の申請一覧。承認された申請は VC の発行（受取）が可能。
機能	デジタル証明一覧	過去に発行したデジタル証明の一覧。

非機能	可用性	プロトタイプのため障害発生時の機能停止は実装していないが、クラウドとブロックチェーンがベースにあるため基本的にはノンストップで稼働。
非機能	運用・保守性	・プロトタイプのため、メンテナンスの実施は計画していない。 ・バックアップ方針について 秘密鍵に関して Threshold ECDSA Signature（tECDSA）を使う場合は、ICP のルールに従って行う。tECDSA のかわりに Passkey を使う場合、サーバ（Firebase）に保存する認証関連情報は Firestore に保存され、Google が保守運用を行う。秘密鍵自体のバックアップは Passkey によって複数端末に保管される。VC のバックアップと共に今回は実装外。将来的には、WebAuthn の prf extension を使って暗号化し、クラウドに保存する予定。
非機能	性能・拡張性	業務量及び機能が増加した場合も、tECDSA 部分以外は Firebase・Expo/React-Native を活用してスケールアウトによるシステム運用を行うことができる。
非機能	セキュリティ	・今回のスコープでは暗号化は行わない。将来暗号化を行う場合、WebAuthn の prf extension を使用する。パスワードを使っているのは tECDSA で Google 認証を使うケースであり、本システムでパスワードは管理しない。 ・現在の実装方式だと、Wallet で署名して、IdToken と署名を同時に Canister に送るので、トークンインジェクションの問題は起こらない認識。 ただし、Passkey/WebAuthn 固有のセキュリティリスクには、常に備えておく必要がある。
非機能	移行性	VC を使った業務は現状行われていないため、現行業務からそのままトランジションすることは難しいが、KYC に関する現状ノウハウは活用することができる。