Personary の属性証明対応機能
基本設計書

1．目的

われわれは、PLR (Personal Life Repository)を用いてパーソナルデータの安全・安価な流通・活用を促進するスマートソサエティの基盤を構築する研究を進めている。その一環として、PLR の基本機能にデータの作成・閲覧・共有等のユーザインタフェースを加えた統合アプリである Personary を開発しており、それをもとに多様なアプリを開発しそれに基づくサービスを社会実装する計画である。

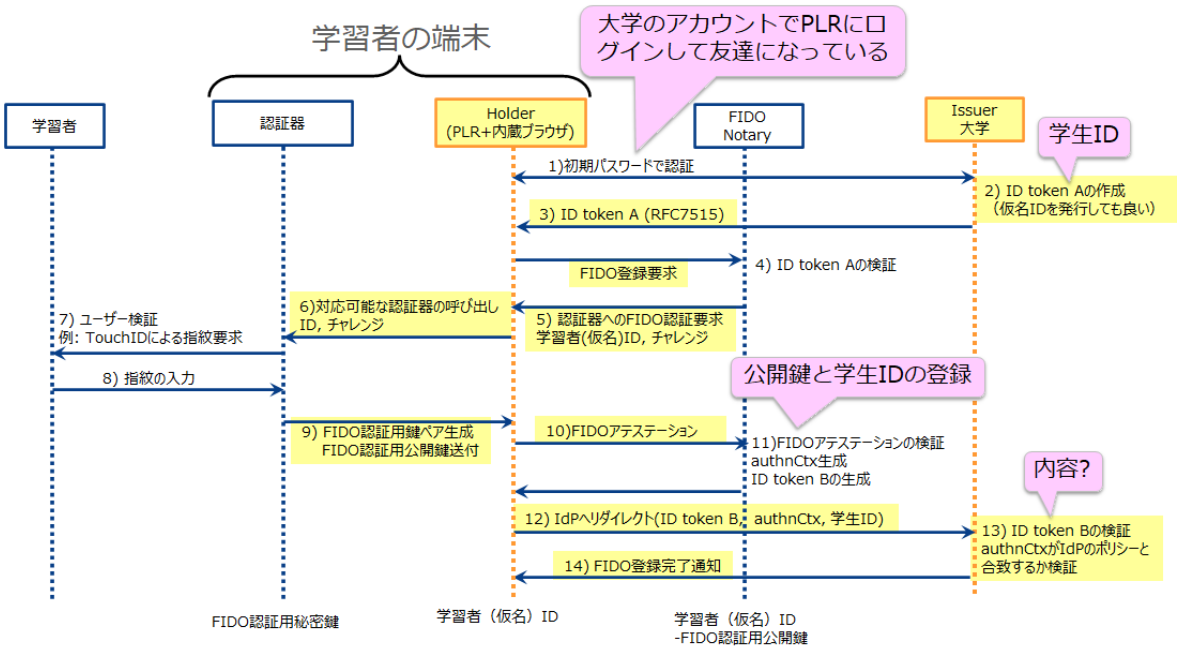
2．概要

検証可能属性証明(VC: Verifiable Credential)および検証可能属性提示(VP: Verifiable Presentation)を取り扱う機能を開発することにより、分散型の認証にかかる手間を削減し、ユーザビリティを高める。

3．仕様

下記の説明のうち#付きの部分(各図の黄色い部分)が Personary の機能である。つまり、Issuer と Holder と Verifier の機能を Personary において実現する。その一環として、Issuer と Holder と Verifier が ID トークン等を公開鍵によって検証するのに用いる Dart のメソッドを開発する。一方、FIDO Notary と VDR (Verifiable Data Registry)と VP の生成・検証サービスの開発は今回の作業の対象外である。これらは Web アプリであり、Personary がその Web API を呼ぶ。

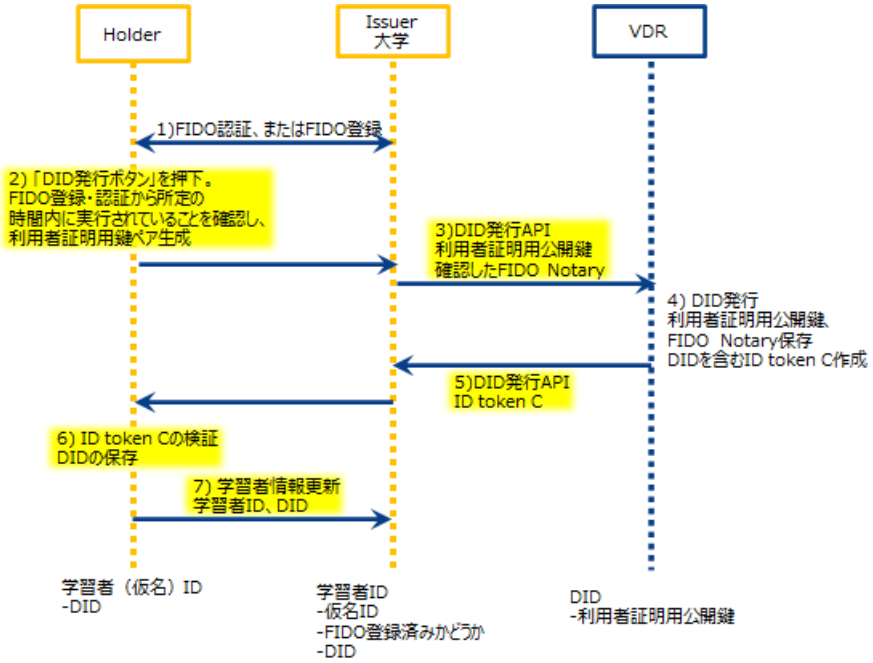
(1) FIDO 登録



1) Issuer (大学等)が Holder (学習者等)を認証(大学等のアカウントで PLR にログインして友達になる)
2) #Issuer が ID トークン A を作成して Holder のサービス利用履歴チャネルに投稿
3) #Holder が ID トークン A を FIDO Notary に送信して FIDO の登録を要求
4) FIDO Notary が ID トークン A を検証
5) FIDO Notary が認証器による FIDO 認証を Holder に要求
6) #Holder がその要求を認証器に送付
7) 学習者等(人間)がその要求を受理
8) 学習者等(人間)が指紋等を入力

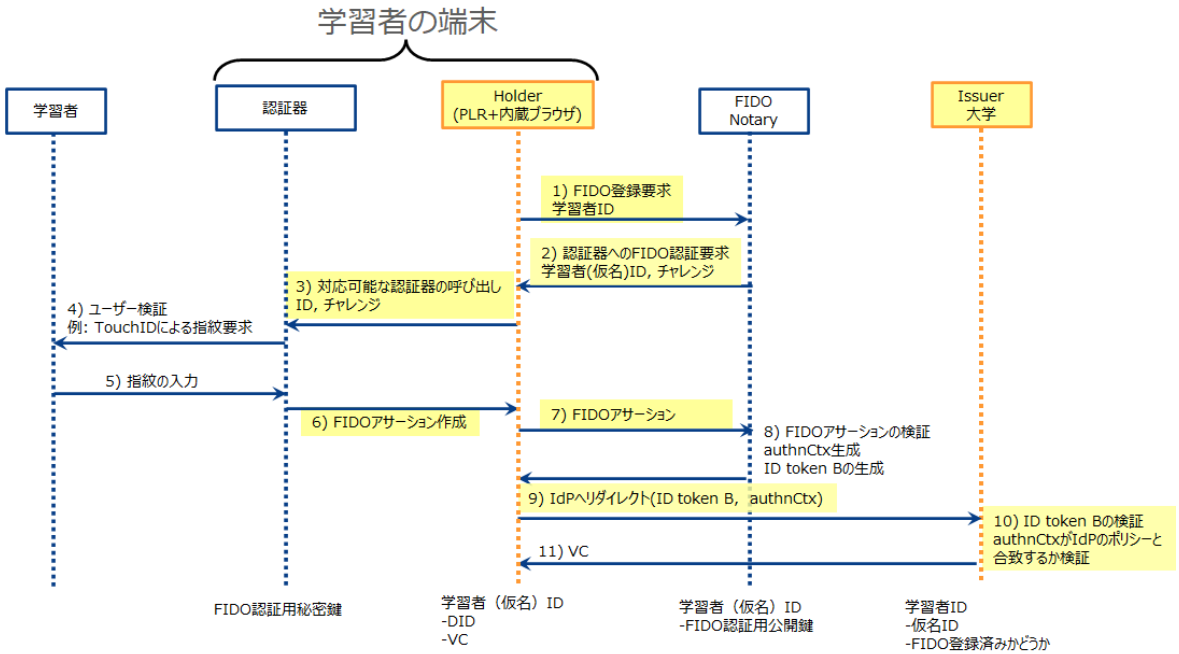
9)　認証器が FIDO 認証用鍵ペアを生成し Holder に FIDO アテステーションを返信
10) #Holder が FIDO アテステーションを FIDO Notary に転送
11) FIDO Notary が FIDO アテステーションを検証し ID トークン B と authCtx を生成して Holder に返信
12) #Holder がそれらと学習者等の学生 ID 等をサービス利用履歴チャネルに投稿
13) #Issuer が ID トークン B と authCtx を検証
14) #Issuer が Holder のサービス利用履歴チャネルに FIDO 登録完了の旨を投稿

(2) DID の発行



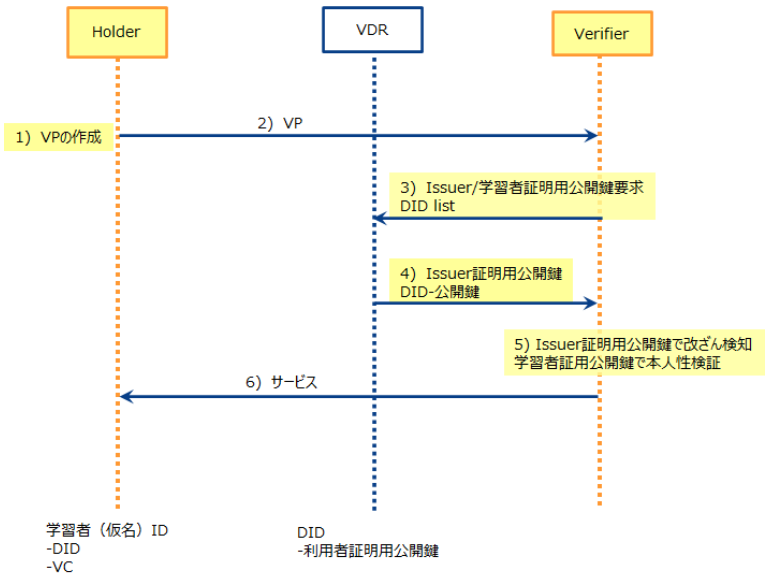
1)　#FIDO 認証または FIDO 登録から所定の期限が過ぎていれば Holder の要請により Issuer が Holder を FIDO 認証
2)　#Holder が利用者証明用鍵ペアを生成
3)　#Holder が Verifiable Data Registry の DID 発行 API を呼んで利用者証明用公開鍵と FIDO Notary の ID を渡す
4)　VDR が DID を発行し、DID を含む ID トークン C を作成
5)　VDR が Holder に ID トークン C を返信
6)　#Holder が ID トークン C を検証
7)　#Holder がサービス利用履歴チャネルに DID を保存

(3) VC の発行



1) #Holder が FIDO Notary の FIDO 登録要求 API を呼んで学習者 ID を渡す
2) FIDO Notary が認証器への FIDO 認証要求を返信
3) #Holder が認証器を呼び出して FIDO 認証要求を渡す
4) 学習者等(人間)がその要求を受理
5) 学習者等(人間)が指紋等を入力
6) 認証器が Holder に FIDO アサーションを返信
7) #Holder が FIDO アサーションを FIDO Notary に返信
8) FIDO Notary が FIDO アサーションを検証し authCtx と ID トークン B を生成
9) #Holder が FIDO Notary から受け取った ID トークン B と authCtx をサービス利用履歴チャネルに投稿
10) #Issuer が ID トークン B を検証
11) #Issuer が VC を生成して Holder のサービス利用履歴チャネルに投稿

(4) VP の生成と検証



1) #Holder が VP を生成
2) Holder が Verifier に VP を開示
3) #Verifier が VDR に Issuer 証明用公開鍵と学習者証明用公開鍵を要求
4) VDR が Verifer に Issuer 証明用公開鍵と学習者証明用公開鍵を返信
5) #Verifier が Issuer 証明用公開鍵で VP を検証し、学習者証明用公開鍵で本人性を検証
6) Verifier が Issuer にサービスを提供

(5) 開示条件と開示要請
属性データを本人が開示する条件および開示の他者による要請を利用者が記述する仕組み。

(6) 自動マッチング
(1)の開示条件と開示要請を満たす属性情報を自動的に抽出する機能。

(7) 自動開示
(2)で抽出された属性情報を(可能なら VP として)要請者に自動開示する機能。

以　上