Personary の属性証明対応機能
要件定義書

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．要件定義

(1) FIDO 登録

1) PLR の Issuer (大学等)が Holder (学習者等)を認証すること。
2) Holder が認証情報を FIDO Notary に送信して登録要求できること。
3) 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 に返信すること。
4) Issuer が authCtx を検証して FIDO 登録を完了すること。

(2) DID の発行

5) Holder が利用者証明用鍵ペアを生成し、VDR に DID 発行を要求すること
6) VDR が DID を発行し、Holder に情報を返すこと。
7) Holder が PLR のサービス利用履歴チャネルに DID を保存すること。

(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 を渡すこと。
2) #Holder が FIDO アサーションを FIDO Notary に返信すること。
3) 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
4) Issuer が ID トークン B を検証した上で VC を生成すること。

(4) VP の生成と検証

1) Holder が VP を生成できること。
2) Verifier が VDR に Issuer 証明用公開鍵と学習者証明用公開鍵を要求したうえで、検証できること。

(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

(5)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できること。

(7) 自動開示

(6)で抽出された属性情報を(可能なら VP として)要請者に自動開示できること。