SELMID

NIIオープンフォーラム2023

Moodleと連携した ラーニングクレデンシャルの発行と利活用 ～NII様での実証実験のご報告

2023/05/31

伊藤忠テクノソリューションズ株式会社
OpenIDファウンデーションジャパン
富士榮　尚寛

NIIにおけるデジタルクレデンシャルの状況

SELMID

FY22調達仕様より

- 学認 LMS(学習管理システム)を構築し、研究データ管理について学習するための講座(以下、研究データ管理講座)を提供してきた。 これらの講座では、すべての学習が修了したことを証明するオープンバッジを発行してお り、現在、発行したオープンバッジをユーザが管理するための保管場所であるデジタルウォ レットを構築し、将来的に提供することを検討している。
- 学認 LMS でも利用している Moodle 上で発行されたオープンバッジが Verifiable Credentials(以下、VC)に対応するように変換するゲートウェイ、変換された オープンバッジを保管するデジタルウォレット(以下、オープンバッジウォレット)、オー プンバッジウォレット上のオープンバッジを外部サービスへ送信するエクスポート機能を 構築する予定である。

OpenBadgeの活用に向けて以下の取り組みを行う
1. 汎用的な形式で利用者自身で持ち運べる様にする（VCへの変換、 Walletへの格納）
2. 外部サービスへ送信できる様にする（Verifierへの提示と検証）

目指す姿

要件

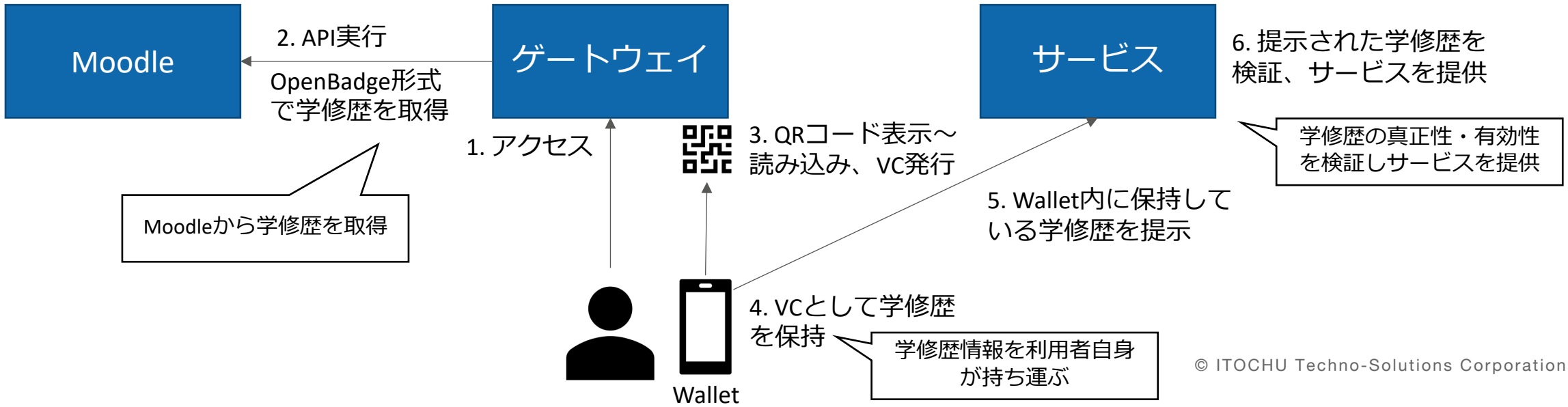
1. Moodleから学修歴情報を取り出してWalletに格納、利用者自身が持ち運ぶ
2. Walletに格納された学修歴の提示を受けたサービスは真正性・有効性の検証を行い権限に応じたサービスの提供を行う

例）学認LMSでセキュリティのトレーニングを受けた利用者は学認RDMで追加の領域を取得できる

検討する実現方式

- W3C Verifiable Credentials（VC）に対応したWalletを用いる
- Moodleが発行する学修歴（OpenBage形式）をVerifiable Credentialsへ変換するゲートウェイサービスを構築する

システムイメージ



技術的要素の検討

SELMID

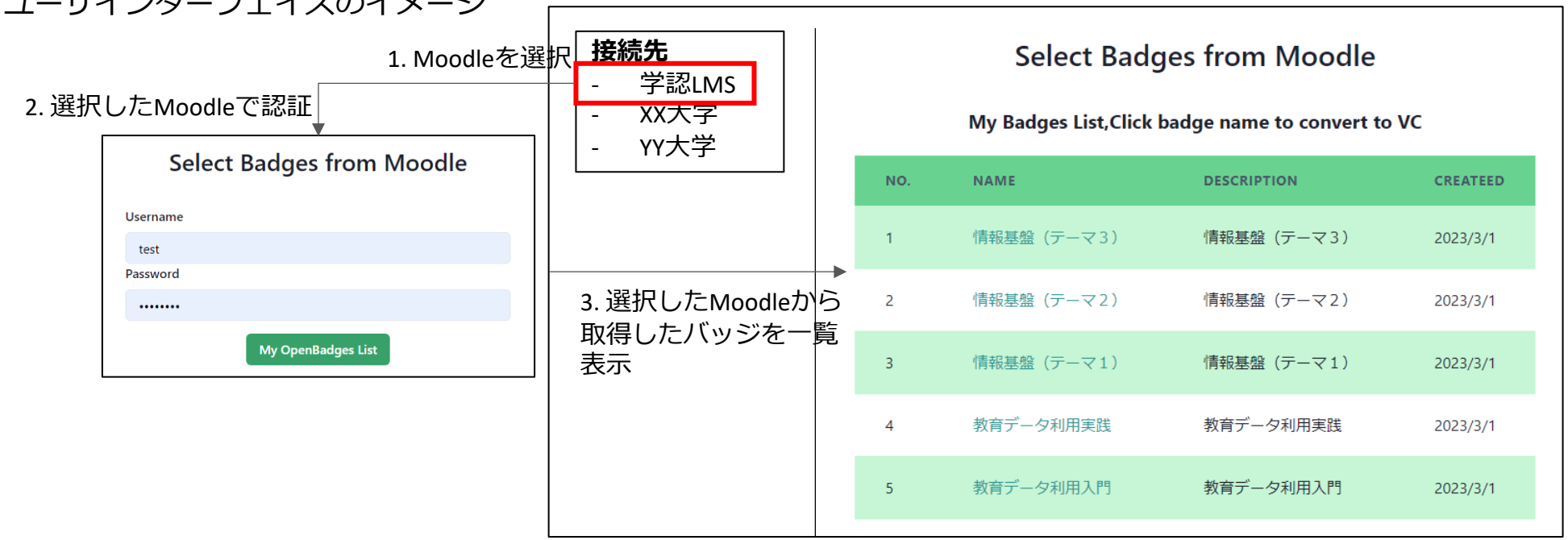
検討対象となった技術要素

#	対象	検討区分（大）	検討区分（小）	検討内容
A-1	Moodle	Moodleからバッジ情報を取得する方法	取得単位	ユーザ毎、複数ユーザ一括
A-2			発行対象ユーザの特定	識別方法、認証方法
A-3			発行形式	Moodle独自形式、OpenBadge形式
A-4			アクセス制御	公開・非公開設定による発行制御
B-1	ゲートウェイ	取得したバッジ情報の表示方法	バッジの管理ユーザインターフェイス	接続先となるMoodle
B-2				バッジの階層・区分
B-3		発行するVerifiable Credentialsに含める情報	OpenBadgeとVerifiable Credentialsの要素のマッピング	対象とする属性とマッピング、画像の形式、OpenBadge形式の維持
C-1	Wallet	発行したバッジの表示方法	Verifiable Credentialsの要素と表示方法	属性の型による表示方法、履歴の表示
C-2		要求されたバッジの提示方法	提示単位	組み合わせ、複数提示
D-1	提示先システム	提示されたバッジの検証方法	検証内容	真正性、有効性
D-2		バッジ保有者の検索方法	バッジ保有者の管理	管理方法、検索方法

B）ゲートウェイ：取得したバッジ情報の表示方法

SELMID

1. **バッジの管理ユーザインターフェイス：接続先となるMoodle**
   - 前述のとおりバッジを取得するためにはMoodleへAPIで接続する必要がある。ゲートウェイの位置づけをユーザが複数のMoodleで付与されたバッジをVerifiable Credentialへ変換するためのゲートウェイと位置付ける場合、複数のMoodleとの接続を行うことも今後検討することができる（各Moodleに前述のAPI設定が必要。本実証では単一のMoodleのみへの接続を行った）
   - ユーザインターフェイスのイメージ



2. **バッジの管理ユーザインターフェイス：バッジの階層・区分**
   - OpenBadgeやVerifiable Credentialには階層の考え方は存在しないが、教育現場等においては複数コースを修了することで認定されるようなユースケースも存在するためバッジ内の特定の属性（大阪教育大学ではVersion属性）を利用を利用して階層構造を表現することも実運用上は必要となる。そのケースにおいてはゲートウェイのユーザインターフェイスも工夫が必要となる

B）ゲートウェイ：発行するVerifiable Credentialsに含める情報

SELMID


```
{
  "recipient": {
    "identity": "sha256$34911a66e23c17862740a50089904d6d580bf10f0a491924b64905217e554d61",
    "type": "email",
    "hashed": true,
    "salt": "badges1676119330"
  },
  "badge": {
    "name": "testbadges_jpeg",
    "description": "テスト",
    "image": “ /QPAh0k8G・・中略・・U5ErkJggg==",
    "criteria": {
      "id": "https://moodle.selmid.me/badges/badgeclass.php?id=6",
      "narrative": "Users are awarded this badge when they complete the following requirement:¥n* This badge has to be awarded by a user with the following
role:¥nManager¥n¥n"
    },
    "issuer": {
      "name": "New Site",
      "url": "https://moodle.selmid.me/",
      "email": "",
      "@context": "https://w3id.org/openbadges/v2",
      "id": "https://moodle.selmid.me/badges/issuer_json.php?id=6",
      "type": "Issuer"
    },
    "@context": "https://w3id.org/openbadges/v2",
    "id": "https://moodle.selmid.me/badges/badge_json.php?id=6",
    "type": "BadgeClass",
    "version": "",
    "@language": "en"
  },
  "verify": {
    "type": "hosted",
    "url": "https://moodle.selmid.me/badges/assertion.php?b=0f287357c71a6afd611f6aef35b4ec499173cf6e&obversion=2"
  },
  "issuedOn": "2023-02-28T04:06:13+00:00",
  "evidence": "https://moodle.selmid.me/badges/badge.php?hash=0f287357c71a6afd611f6aef35b4ec499173cf6e",
  "expires": "2024-02-28T00:00:00+00:00",
  "@context": "https://w3id.org/openbadges/v2",
  "type": "Assertion",
  "id": "https://moodle.selmid.me/badges/assertion.php?b=0f287357c71a6afd611f6aef35b4ec499173cf6e&obversion=2"
}
```


https://moodle/badges/assertion.php?obversion=2&b=1a6…中略…c8

受信者情報（ハッシュ）

取得したimageのiTXTにassetion全体をセット

ログインしたユーザの情報からメールアドレスを取得

バッジ画像

Badgeの発行日・有効期限

ゲートウェイでの発行日・VCの有効期限

C）Wallet

本実証においてVerifiable Credentialを格納するためにMicrosoftが提供しているMicrosoft Authenticator、および伊藤忠テクノソリューションズ株式会社およびBlockBase株式会社のメンバがOSSとして公開（MITライセンス）しているモジュールを利用した（Verifiable Credentials関連機能はMicrosoft Entra Verified IDを利用）

https://github.com/did-developer-community/custom-identity-wallet

Walletの概要は以下の通りである

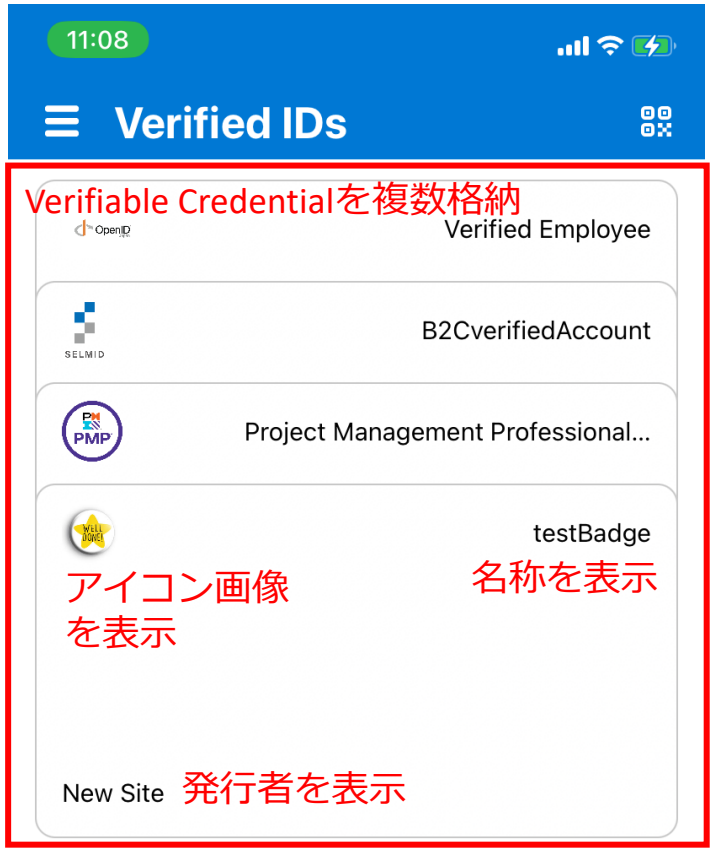
【基本機能】

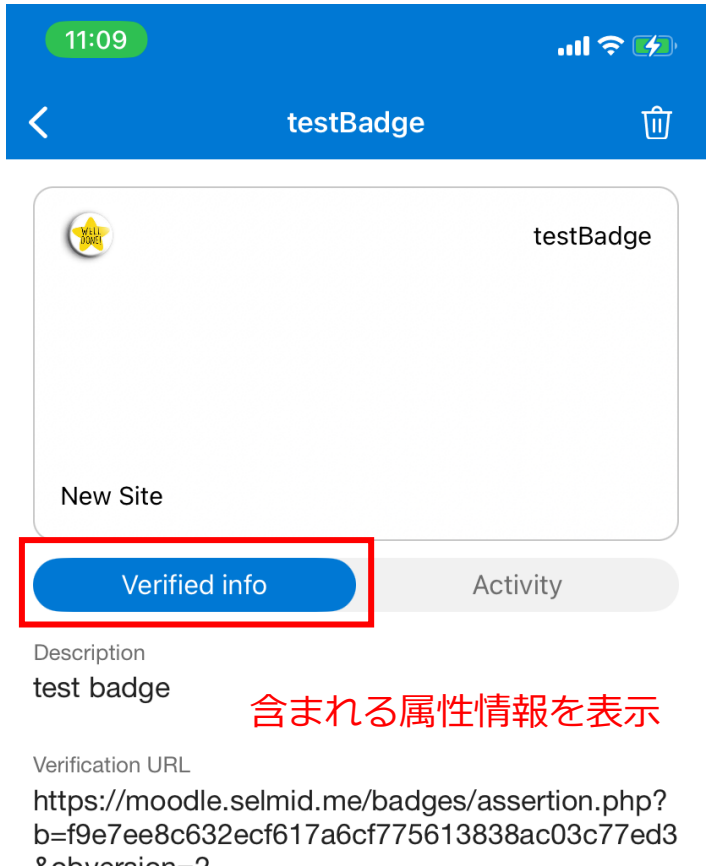
- Verifiable Credentials発行要求の読み取り～格納
  - OpenID for Verifiable Credential Issuanceプロトコルに対応したVerifiable Credential発行者（本実証においてはゲートウェイ）の提示する発行要求（一般にQRコードに埋め込まれたURL形式）を読み取り、発行者へVerifiable Credentialの発行を要求する
  - 発行されたVerifiable CredentialをWallet内に格納する
- Verifiable Credentialsの提示
  - OpenID for Verifiable Credential Presentationプロトコルに対応したVerifiable Credential検証者（本実証においてはゲートウェイ。提示先システム）の提示する提示要求（一般にQRコードに埋め込まれたURL形式）を読み取る
  - 検証者からの要求されたCredential Typeに適合したVerifiable CredentialをWallet内から取得し、ユーザの選択に従いVerifiable Presentationを作成し、検証者へ提示する

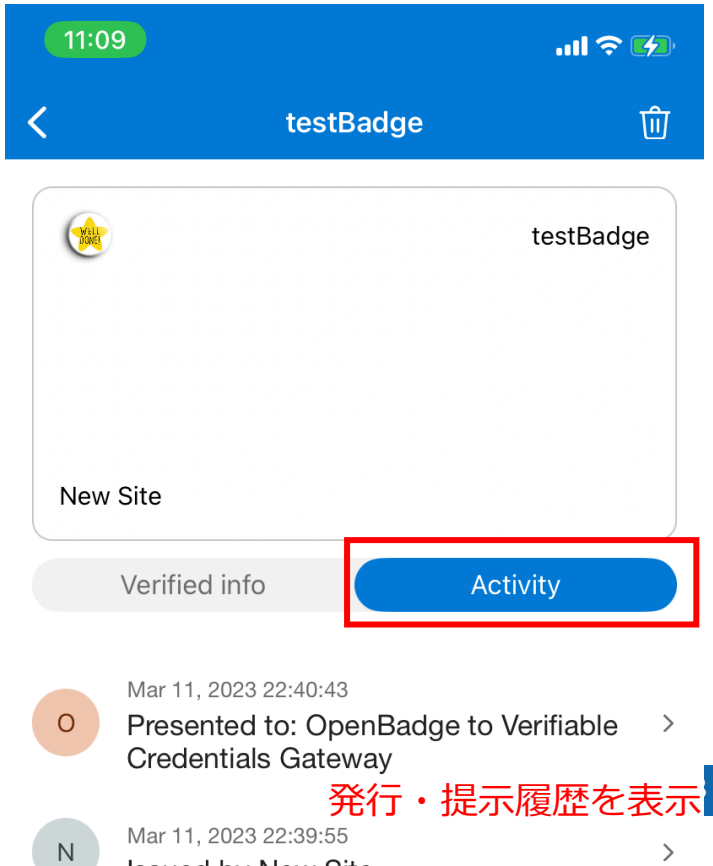
C）Wallet：発行したバッジの表示方法

SELMID

1. **Verifiable Credentialsの要素と表示方法：属性の型による表示方法、履歴の表示**
   - Wallet内に格納されるVerifiable Credentialの表示に関するユーザインターフェイスは以下を考慮する
     - 複数のVerifiable Credentialを格納するため、ユーザが保持しているVerifiable Credentialを視認・識別できること
     - 各Verifiable Credentialが持つ属性情報を確認できること
     - 各Verifiable Credentialの発行～提示等の履歴を確認できること
   - 以下、WalletとしてMicrosoft Authenticatorを利用した場合の例を示す



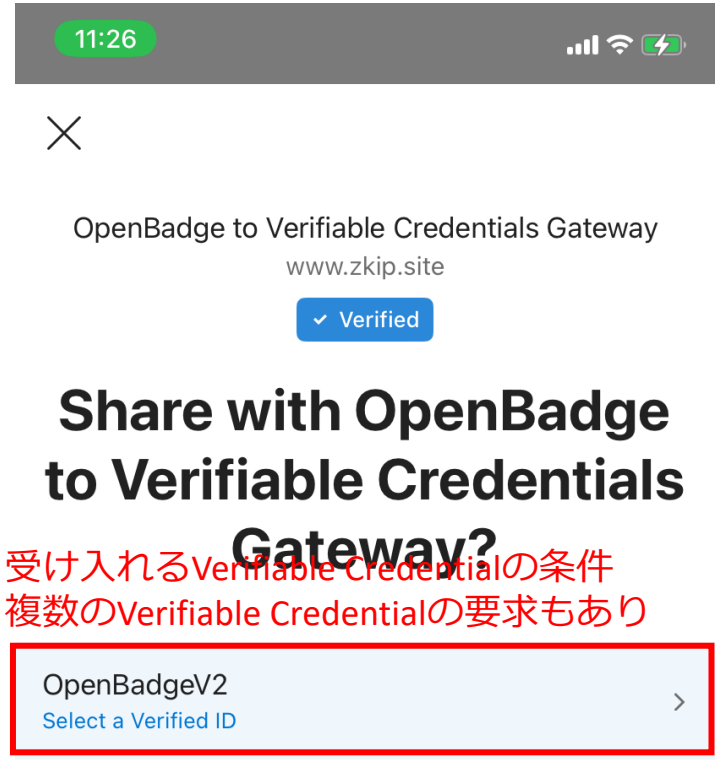


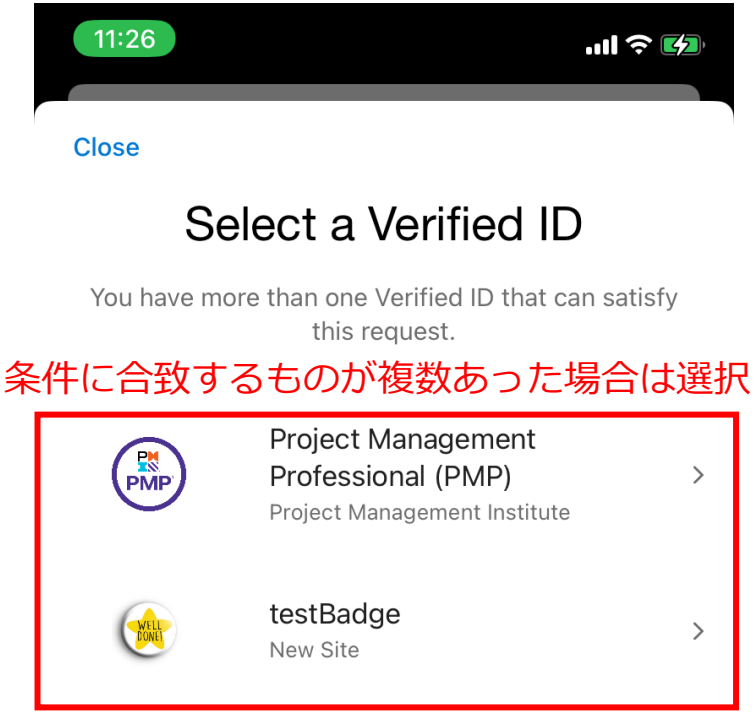


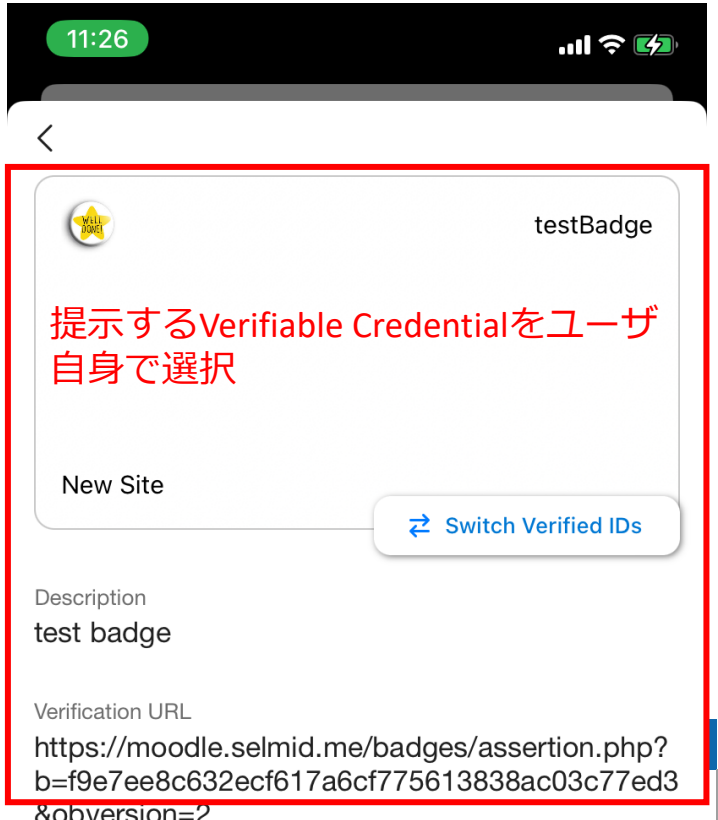
C）Wallet：要求されたバッジの提示方法

SELMID

1. **提示単位：組み合わせ、複数提示**
   - 提示先システムがWallet内に格納されるVerifiable Credentialの提示を求める際の要求技術仕様はDecentralized Foundationの定めるPresentation Exchangeに基づいて実行される（https://identity.foundation/presentation-exchange/spec/v2.0.0/）
   - よく利用される要求パターンとして以下のようなものが考えられ、Walletは対応するユーザインターフェイスの実装が求められる
     - 複数のVerifiable Credentialを一括して要求する
     - 条件に合致したVerifiable Credentialの提示を要求する
   - 以下、WalletとしてMicrosoft Authenticatorを利用した場合の例を示す







D）提示先システム：提示されたバッジの検証方法

SELMID

1. **検証内容：真正性、有効性**
   - 本実証においてWallet内には以下が格納される
     - Moodleの発行するOpenBadgeから生成したVerifiable Credential
     - 生成したVerifiable Credential内に埋め込まれたMoodleが発行したOpenBadgeそのもの
   - 加えて、Walletから提示先システムに対してVerifiable Credentialを提示する際にはVerifiable PresentationがWalletにより生成される
   - それぞれが検証可能な資格証明ではあるが検証の目的と方法が異なる

検証対象	検証目的	検証方法
Verifiable Credential	意図した発行者が発行したものか	Verifiable Credentialのissに指定されたDIDが指し示すDID DocumentがリンクされているDNSドメインが意図するサービス（今回だとゲートウェイ）を管理している事業者と合致しているか？（事前に受け入れる事業者を登録しておく許可リスト方式が考えられる）
	途中で改ざんされていないか	Verifiable Credentialのissに指定されたDIDが指し示すDID Document内に登録されている公開鍵を使ってVerifiable Credential自体に施されたデジタル署名の検証ができるか？
	意図したユーザに対して発行されたものか（別のユーザから提示されていないか）	Verifiable CredentialのcredentialSubjectに指定されたDIDと、Verifiable Presentationのissに指定されたDIDと合致しているか？
	有効なものか（期限が切れていないか）	Verifiable CredentialのexpirationDateを迎えていないか？
	有効なものか（取り消しされていないか）	Verifiable Credentialのissに指定されたDIDが指し示すDID Document内に指定された有効性確認手法（本実証ではW3C StatusList2021仕様を利用）に基づき有効性が確認できるか？
OpenBadge	意図したユーザに対して発行されたものか	OpenBadge内のRecipientのIdentityがVerifiable Credential内に記録された識別子（本実証ではメールアドレス）と合致するか？（本実証ではBadgr Validatorを利用し検証）
	有効なものか（期限切れ、取り消し済みでないか）	OpenBadgeのAssertionを正しく検証できるか？（本実証ではBadgr Validatorを利用し検証）
Verifiable Presentation	途中で改ざんされていないか	Verifiable Presentationのissに指定されたDIDが指し示すDID Document内に登録されている公開鍵を使ってVerifiable Presentation自体に施されたデジタル署名の検証ができるか？

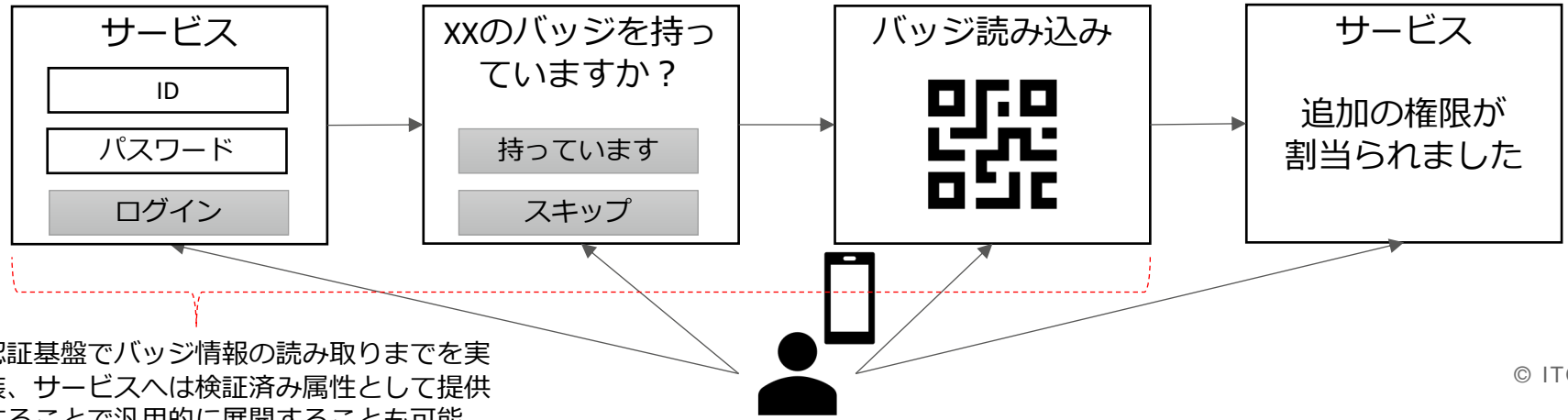
D）提示先システム：バッジ保有者の検索方法

2. バッジ保有者の管理：管理方法、検索方法

- バッジに関する情報を保持している箇所は「Moodle」、「ゲートウェイ」、「Wallet」の3か所となる
- 提示先システム側からバッジを保有している可能性があるユーザに対してバッジの提示を求めることで、ユーザに対するベネフィットを提供したり、アクセス制御を行うためには、以下の方法が考えられる
  - 提示先システムで発行されたバッジと発行先ユーザの一覧を取得し利用する
  - 提示先システムにユーザがアクセスした際にバッジを提示することでベネフィットが得られる等の表示を行うことで提示を促す

バッジ情報保持箇所	保持している情報	提示先システムからの利用方法
Moodle	当該のMoodle上で発行されたバッジと発行先ユーザの一覧	当該のMoodleのAPIを利用して発行済みバッジの情報を定期的に取得する
ゲートウェイ	ゲートウェイでVerifiable Credentialに変換されたバッジと発行先ユーザの一覧	ゲートウェイ上で発行履歴を管理し、提示先システムへAPI等で提供する
Wallet	Wallet利用ユーザがVerifiable Credentialに変換したバッジの一覧	提示を促し、利用者自身で選択させる

- ユーザのプライバシ等を考慮すると提示先システムへ利用者がアクセスした際に当該バッジを保有している場合は提示をするように促すことで利用者の意思を尊重することが望ましいと考えられる（以下、操作イメージ）



総括

仕様書記載の以下に関する技術的要素の検討を実施した。

- Moodleから発行されたオープンバッジをウォレットに登録するための実装方法
  - ゲートウェイからAPIを利用しMoodleへアクセス、ユーザ自身により発行済みバッジを取得し、Verifiable CredentialとしてWalletへ保管、提示先システムへユーザの意思により提示していく方法の実装を行った
- ウォレット内にあるデジタルクレデンシャルを選択して提示するための実装
  - 提示先システムへ提示するバッジを選択することが可能な実装を行った
- ユーザから提示されたデジタルクレデンシャルを活用するための実装方法
  - SAMLのクレデンシャルプロバイダとしての実装を行い、既存のSAML IdP/SPと連携することでクレデンシャルを属性として提供することの検討を行った

OpenBadge v3/VC2.0に向けた課題も明らかとなった。

- マルチリンガルの表現
- Endorsementの表現
- 階層化されたクレデンシャルの表現

今回作成したGatewayとWalletのソースコード

SELMID

NII様のレポジトリでMITライセンスで公開されています。

- Gateway
  - https://github.com/RCOSDP/credentialwallet_gateway
- Wallet
  - https://github.com/RCOSDP/credentialwallet_wallet