基本設計書

2024年3月15日

Version 1.0

目次

[1. 業務フロー 2](#_Toc158796685)

[1.1. 業務フロー図 2](#_Toc158796686)

[1.2. シーケンス図 2](#_Toc158796687)

[2. 機能一覧 3](#_Toc158796688)

[2.1. ウォレット機能 3](#_Toc158796689)

[2.2. マイナンバーカード情報代理発行機関システム機能 4](#_Toc158796690)

[2.3. 組織所属証明書発行機関システム機能 5](#_Toc158796691)

[2.4. イベント参加証明書発行機関システム機能 6](#_Toc158796692)

[2.5. メッセージングサービス追加機能 7](#_Toc158796693)

[3. ネットワーク構成 8](#_Toc158796694)

[4. 画面遷移 9](#_Toc158796695)

[4.1. ウォレットアプリの画面構成 9](#_Toc158796696)

[4.2. メッセージングアプリの画面構成 9](#_Toc158796697)

[5. 画面構成 10](#_Toc158796698)

[5.1. ウォレットアプリの画面構成 10](#_Toc158796699)

[5.2. メッセージングアプリの画面構成 10](#_Toc158796700)

# 業務フロー

## 業務フロー図

タイムライン

自動的に生成された説明

**図 1-1：業務フロー図**

## シーケンス図

詳細は[別紙\_ユースケース設計書.pdf](https://drive.google.com/file/d/1p-DWLv6Jke5osqD2dlKrt94PDyNJ8oKv/view?usp=drive_link)を参照ください。

# 機能一覧

## ウォレット機能

**表 2-1：ウォレット機能一覧**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 機能分類 | 機能 | 説明 | 備考 |
| 1 | その他 | 利用開始 | 初回のセットアップフロー |  |
| 2 | 認証 | ロック解除受付 | 認証が必要なタイミングで指紋やPINによるロック解除により認証する |  |
| 3 | 証明書管理 | 証明書一覧 | 発行したVCを一覧表示する |  |
| 4 | 証明書管理 | 基本４属性VC発行 | xIDアプリと連携してマイナンバーカードを読み取り取得した情報をVCとして取得する | OID4VCプロトコル準拠  vc+sd-jwt |
| 5 | 証明書管理 | 社員証VC発行 | クレデンシャルオファーのフローで社員証をVCとして取得する | OID4VCプロトコル準拠  vc+sd-jwt |
| 6 | 証明書管理 | イベント参加証 | クレデンシャルオファーのフローでイベント参加証をVCとして取得する | OID4VCプロトコル準拠  jwt\_vc\_json |
| 7 | 証明書管理 | 証明書詳細 | 取得したVCの詳細を表示 |  |
| 8 | 証明書管理 | 発行機関情報 | VCの発行者の情報を表示 |  |
| 9 | 証明書管理 | QRコード表示 | 所有している証明書の内容をQRコードで表示 | イベント参加証(jwt\_vc\_json)のみ |
| 10 | 証明書管理 | 証明書検証 | 提示された証明書のQRコードを読み取り証明書を検証する | イベント参加証(jwt\_vc\_json)のみ |
| 11 | SIOP | SIOPv2要求受付 | SIOP要求を読み取りデータ提供同意(認可)のUIを表示する |  |
| 12 | SIOP | SIOPv2結果送信 | ペアワイズ識別子を発行してIDトークンとして要求元に送信する |  |
| 13 | OID4VP | VPトークン要求受付 | VPトークン要求を読み取りデータ提供同意(認可)のUIを表示する |  |
| 14 | OID4VP | VPトークン送付 | 要求に合致するクレームを選択してVPを生成、送信する |  |
| 15 | OID4VP | 選択開示 | VP要求に応じて開示するクレームを選択するUI |  |
| 16 | 提供先管理 | 提供先一覧 | VCを提供した相手先を一覧表示する |  |
| 17 | 提供先管理 | 提供先詳細 | VCを提供した相手先の詳細を表示 |  |
| 18 | 提供先管理 | 提供情報詳細 | 提供先に対して、提供日時、クレームの情報を表示する |  |
| 19 | 設定 | メニュー | 設定機能のメニューと各種リンクを表示 |  |
| 20 | 設定 | バックアップ | HDウォレットのシード、発行ずみVC、提供履歴をファイルでエクスポート | 提供履歴には提供先毎に秘密鍵から導出されるアドレスを含めておく |
| 21 | 設定 | リカバリー | バックアップでエクスポートしたファイルをインポートして各種情報を復元する | 提供先毎に払い出したペアワイズのキーペアはHDウォレットの機能で再生成してアドレス情報を使って対応付けを復元する |
| 22 | 性能要件 | レスポンスタイム | 適切なフレームワークを使用してユーザビリティを毀損しない操作感を提供する | Android: Kotlin  iOS : Swift |
| 23 |  | 効率的なデータ処理 | 暗号対象のデータを選別することにより、必要なデータのみを処理し、処理能力・速度を確保する |  |

## マイナンバーカード情報代理発行機関システム機能

**表 2-2：マイナンバーカード情報代理発行機関システム機能一覧**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 機能分類 | 機能 | 説明 | 備考 |
| 1 | 管理機能 | キーペア登録 | VCの署名に使用するキーペアを生成、登録する | 管理者がCLIで実行する(GUIの提供は様調整)  公開鍵の形式はJWKとX.509を選択できる |
| 2 | VC発行 | xIDアクセストークン取得 | 基本４情報を取得するAPIにアクセスするためのアクセストークンを取得する | OAuth2の認可フローを実装する |
| 3 | VC発行 | 基本４情報VC発行 | ウォレットからVC発行要求を受けて、xIDのAPIから基本４情報を取得、VCを発行する |  |
| 4 | OV証明書 | CSR生成 | OV証明書取得に必要なCSRを生成する |  |
| 5 | OV証明書 | 証明書保存 | OV証明書をデータベースに保存する | VCのヘッダーに格納するx5c、x5uに必要なOV証明書 |
| 6 | 性能要件 | レスポンスタイム | 適切なAWSリソースの使用によりユーザを不快にさせない |  |
| 7 |  | スケーラビリティ | 適切にAWSリソースをスケールアウトさせ、アクセス過多に対しても適切に処理を行う |  |
| 8 |  | 可用性 | リソースを分散させ監視することでサービスの可用性を担保する |  |
| 9 |  | ロギング | AWS Cloud Watch Logsにログを格納することにより、ローテーションと監視を行う |  |
| 10 | 安全性要件 | 脆弱性 | 最新のライブラリの使用と一般的なコーディングガイドラインに従った実装を行い、脆弱性からアプリケーションを守る |  |

## 組織所属証明書発行機関システム機能

**表 2-3：組織所属証明書発行機関システム機能一覧**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 機能分類 | 機能 | 説明 | 備考 |
| 1 | 管理機能 | キーペア登録 | VCの署名に使用するキーペアを生成、登録する | 管理者がCLIで実行する(GUIの提供は様調整)  公開鍵の形式はJWKとX.509を選択できる |
| 2 | VC発行 | 社員情報登録 | 登録のフォーマットを入力としてシステムのデータベースに社員情報を登録する | フォーマットは当該システムで独自に定めるものとする |
| 3 | VC発行 | クレデンシャルオファー生成 | 登録した社員情報を選択して、VC発行用リンク(or QRコード)を生成する | 発行者が社内の連絡チャネルで発行対象者に通知  クレデンシャルオファーにはPinコード要求内容が含まれる |
| 4 | VC発行 | 社員証VC発行 | VC発行用リンクから発生する発行要求に対して社員証VCを発行する |  |
| 5 | OV証明書 | CSR生成 | OV証明書取得に必要なCSRを生成する |  |
| 6 | OV証明書 | 証明書保存 | OV証明書をデータベースに保存する | VCのヘッダーに格納するx5c、x5uに必要なOV証明書 |
| 7 | 性能要件 | レスポンスタイム | 適切なAWSリソースの使用によりユーザを不快にさせない |  |
| 8 |  | スケーラビリティ | 適切にAWSリソースをスケールアウトさせ、アクセス過多に対しても適切に処理を行う |  |
| 9 |  | 可用性 | リソースを分散させ監視することでサービスの可用性を担保する |  |
| 10 |  | ロギング | AWS Cloud Watch Logsにログを格納することにより、ローテーションと監視を行う |  |
| 11 | 安全性要件 | 脆弱性 | 最新のライブラリの使用と一般的なコーディングガイドラインに従った実装を行い、脆弱性からアプリケーションを守る |  |

## イベント参加証明書発行機関システム機能

**表 2-4：イベント参加証明書発行機関システム機能一覧**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 機能分類 | 機能 | 説明 | 備考 |
| 1 | 管理機能 | キーペア登録 | VCの署名に使用するキーペアを生成、登録する | 管理者がCLIで実行する(GUIの提供は様調整)  公開鍵の形式はJWKとX.509を選択できる |
| 2 | VC発行 | イベント情報登録 | 登録のフォーマットを入力としてシステムのデータベースにイベント情報を登録する | フォーマットは当該システムで独自に定めるものとする |
| 3 | VC発行 | クレデンシャルオファー生成 | 登録した社員情報を選択して、VC発行用リンク(or QRコード)を生成する | 発行者が社内の連絡チャネルで発行対象者に通知  クレデンシャルオファーにはPinコード要求内容が含まれる |
| 6 | VC発行 | イベントVC発行 | VC発行用リンクから発生する発行要求に対してイベントVCを発行する |  |
| 7 | OV証明書 | CSR生成 | OV証明書取得に必要なCSRを生成する |  |
| 8 | OV証明書 | 証明書保存 | OV証明書をデータベースに保存する | VCのヘッダーに格納するx5c、x5uに必要なOV証明書 |
| 9 | 性能要件 | レスポンスタイム | 適切なAWSリソースの使用によりユーザを不快にさせない |  |
| 10 |  | スケーラビリティ | 適切にAWSリソースをスケールアウトさせ、アクセス過多に対しても適切に処理を行う |  |
| 11 |  | 可用性 | リソースを分散させ監視することでサービスの可用性を担保する |  |
| 12 |  | ロギング | AWS Cloud Watch Logsにログを格納することにより、ローテーションと監視を行う |  |
| 13 | 安全性要件 | 脆弱性 | 最新のライブラリの使用と一般的なコーディングガイドラインに従った実装を行い、脆弱性からアプリケーションを守る |  |

## メッセージングサービス追加機能

**表 2-5：メッセージングサービス追加機能一覧**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 機能分類 | 機能 | 説明 | 備考 |
| 1 | Element | SIOPv2ログイン | SIOP要求をリンク(or QRコード)で表示する |  |
| 2 | Synapse | SIOPv2ログイン処理 | SIOPレスポンスを受け取りIDトークンを検証する。検証OKならログインを成功させる |  |
| 3 | Element | 年齢証明VC取得要求 | VPトークン要求をリンク(or QRコード)で表示する |  |
| 4 | Synapse | 年齢証明VC取得 | VPトークンを受け取り検証する |  |
| 5 | Element | 年齢証明VC検証結果表示 | 検証結果を表示する |  |
| 6 | Element | 所属組織VC登録要求 | VPトークン要求をリンク(or QRコード)で表示する |  |
| 7 | Synapse | 所属組織VP検証 | VPトークンを受け取り検証する |  |
| 8 | Element | 所属組織VC検証 | チャット開始時、相手方の所属VCを取得して検証する |  |
| 9 | Element | イベント参加証明VC取得要求 | VPトークン要求をリンク(or QRコード)で表示する |  |
| 10 | Synapse | イベント参加証明VC取得 | VPトークンを受け取り検証する |  |
| 11 | Element | イベント参加証明VC検証結果表示 | 検証結果を表示する |  |
| 12 | 性能要件 | レスポンスタイム | 適切なAWSリソースの使用によりユーザを不快にさせない |  |
| 13 |  | スケーラビリティ | 適切にAWSリソースをスケールアウトさせ、アクセス過多に対しても適切に処理を行う |  |
| 14 |  | 可用性 | リソースを分散させ監視することでサービスの可用性を担保する |  |
| 15 |  | ロギング | AWS Cloud Watch Logsにログを格納することにより、ローテーションと監視を行う |  |
| 16 | 安全性要件 | 脆弱性 | 最新のライブラリの使用と一般的なコーディングガイドラインに従った実装を行い、脆弱性からアプリケーションを守る |  |

# ネットワーク構成

ダイアグラム

自動的に生成された説明

**図 3-1：ネットワーク構成図**

# 画面遷移

## ウォレットアプリの画面構成

詳細は、[OWND Project UI Components](https://www.figma.com/community/file/1337646811875545930/ownd-project-ui-components) (Figmaデザイン) を参照ください。

## メッセージングアプリの画面構成

詳細は、[OWND Project UI Components](https://www.figma.com/community/file/1337646811875545930/ownd-project-ui-components) (Figmaデザイン) を参照ください。

# 画面構成

## ウォレットアプリの画面構成

詳細は、[OWND Project UI Components](https://www.figma.com/community/file/1337646811875545930/ownd-project-ui-components) (Figmaデザイン) を参照ください。

## メッセージングアプリの画面構成

詳細は、[OWND Project UI Components](https://www.figma.com/community/file/1337646811875545930/ownd-project-ui-components) (Figmaデザイン) を参照ください。