

Personal Credential Manager User Manual

June, 2022

PCM Overview

The “Personal Credential Manager” is a fully-featured Self Sovereign Identity wallet based smartphone application for Android and iPhone platforms. The Application enables a natural user to participate as a principal of an organization within the SSI-based Gaia-X ecosystem in a privacy-preserving, trustful and secure way. This comprises the following main functionalities:

- Establishment of trustful connections to other parties
- Reception and management of verifiable credentials from other parties (e.g., a principal credential from a Gaia-X participant)
- Presenting Verifiable Presentations to other parties in a proved manner
- Secure storage and management of respective secrets



Personal Credential
Manager



How to download the application

The PCM app can be downloaded in two ways.

1. Google Play Store

Users can search and download the 'Principal Credential Manager' Application from Google Play Store.

1. PCM app icon



Note: PCM app is not yet available at Google Play Store. APK file can be downloaded from here: [GAIA-X-PCM](#)

2. Apple App Store

Users can search and download the 'Principal Credential Manager' Application from Apple App Store.

Note: Its not yet available for download on Apple store. You can request to the app by sending message to getpcm@vereign.com with your Apple email

Getting Started

1. Onboarding

- a. On starting the application the user needs to complete the registration process. The application introductory screens come up first, if the application is started for the first time.

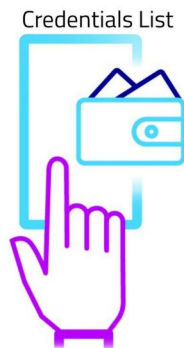
App Introduction



Personal Credential Manager



1.1 PCM Splash Screen



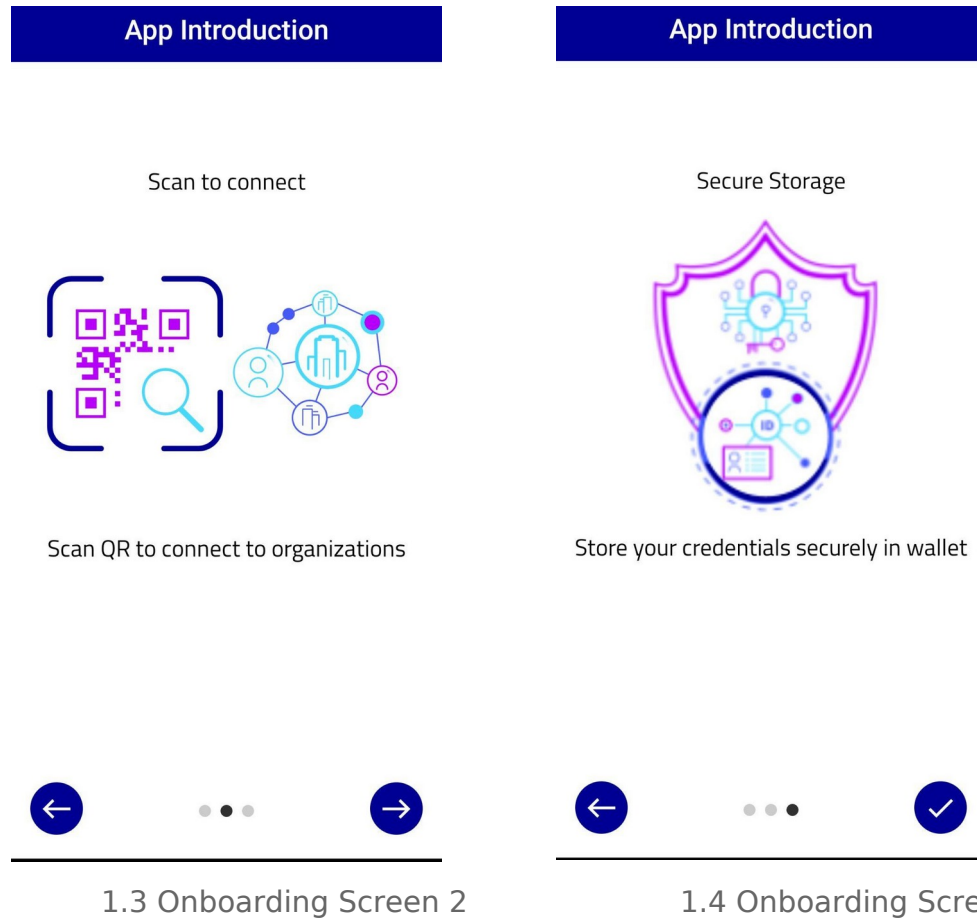
Get the list of issued credentials

Skip










1.1 Onboarding 1st








- i. Users can either click on the "Skip" button to skip these introductory screens or can click on the "Next" button to go through the screens.



- ii. Once done, the user should click on the “Finish” button to proceed further.
- b. The next screen is Terms and Conditions Screen , the user has to give consent to proceed further for registration.

<div><div>Terms & Conditions</div><div> Please read and agree to the terms and conditions below before using this application.</div><div><p>These Terms and Conditions set out the rights and obligations of all users regarding the use of the Service. Your access to and use of the Service is conditioned on Your acceptance of and compliance with these Terms and Conditions. These Terms and Conditions apply to all visitors, users and others who access or use the</p></div><div><div><input type="checkbox"/> I, have read, understand and accept the terms and conditions.</div></div><div><div></div><div></div></div></div> <div>1.5 Terms and Conditions</div>	<div><div>Terms & Conditions</div><div> Please read and agree to the terms and conditions below before using this application.</div><div><p>These Terms and Conditions set out the rights and obligations of all users regarding the use of the Service. Your access to and use of the Service is conditioned on Your acceptance of and compliance with these Terms and Conditions. These Terms and Conditions apply to all visitors, users and others who access or use the</p></div><div><div> I, have read, understand and accept the terms and conditions.</div></div><div><div></div><div></div></div></div> <div>1.6 Terms and Conditions</div>
--	---

- c. The next screen is the registration screen. On this screen, the user has to enter and submit a valid email address to register with the GAIA-X Federation Services.

Registration	OTP Verify
<p>Enter Email</p> <input type="text" value="Enter Email"/>	<p>Enter OTP</p> <input type="text" value="Enter OTP"/>
	<p>55 Seconds Left</p>
<div><p> Please enter a valid email address</p></div>	<div><p> Enter the OTP sent on entered email address</p></div>
<div><div></div><div></div></div>	<div><div></div><div></div></div>
1.7 Registration	1.8 Verify OTP


- d. On the next screen the user needs to submit the OTP received on the above entered email address and get it verified. If the user does not receive the OTP, the resend OTP functionality can be availed after 60 seconds.


OTP Verify


Enter OTP


300790

44 Seconds Left



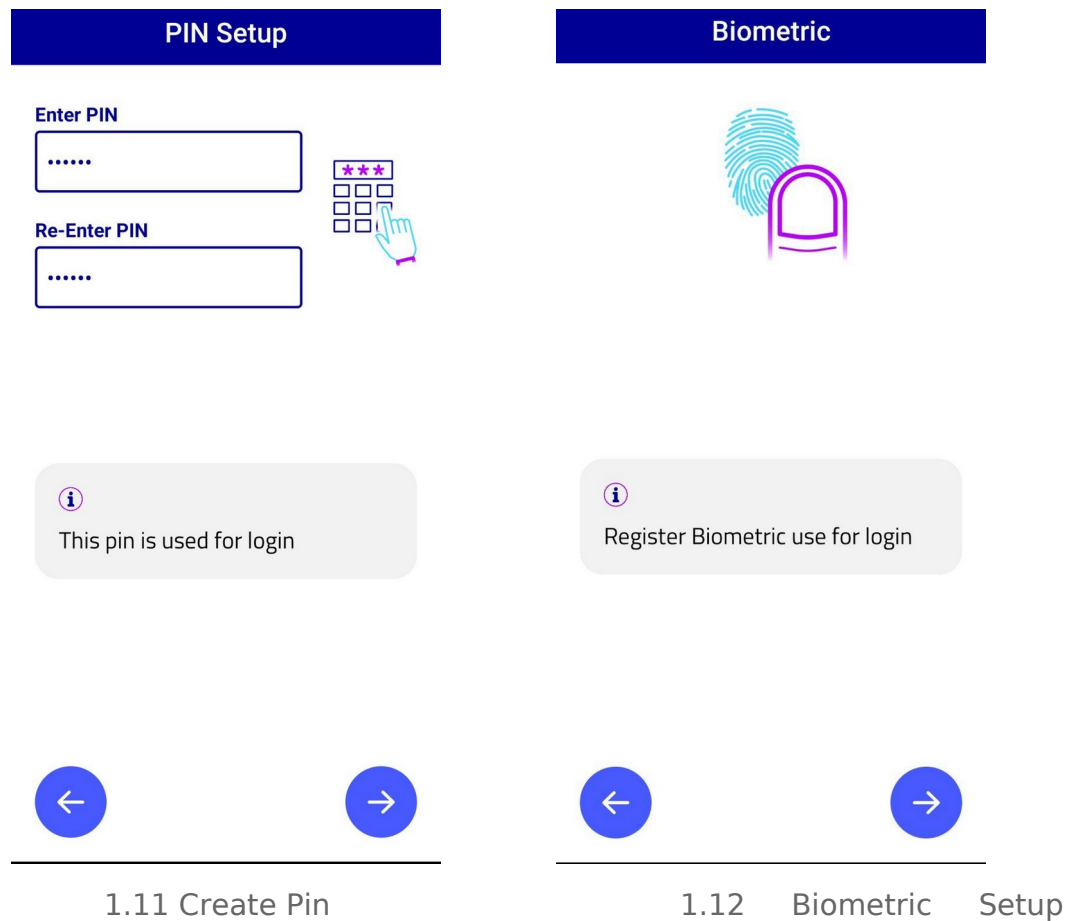

OTP verified successfully





1.9 OTP verified successfully

- e. After a successful OTP Verification, the user needs to set up the App/ Wallet PIN (6 Digit) and configure Biometric (If the device supports), for wallet and device authentication .

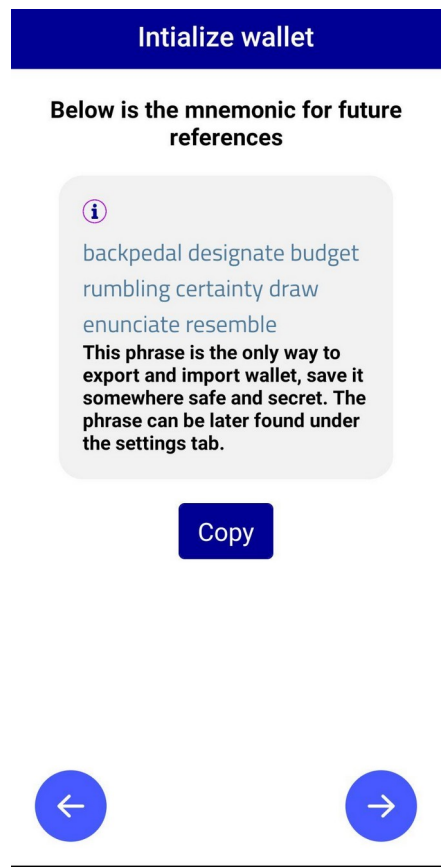


- f. Once the PIN is set up, Users are presented with two options: :
- Import Wallet: If the user holds an exported wallet file off a pre-existing wallet and its corresponding mnemonic, then the user can use Import wallet, to retrieve all the pre-existing wallet data. If the user is an old user of the PCM App and has the previous wallet exported then the user can import the wallet by clicking the “Import Wallet” button. This redirects the user to Import Wallet Screen.



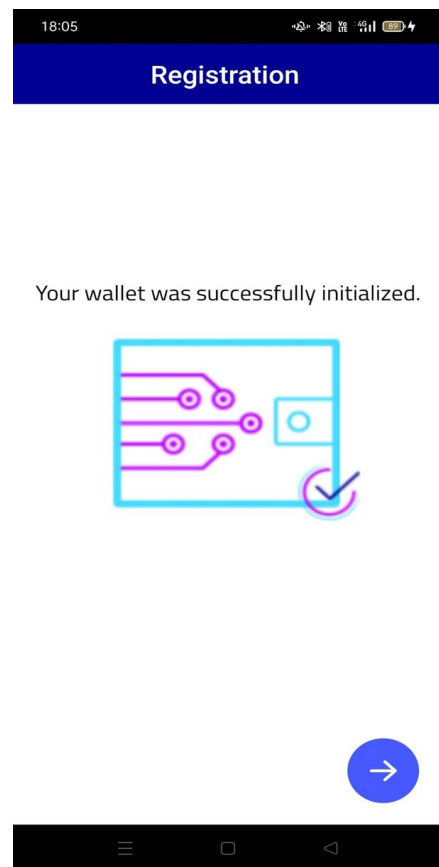
1.13 Initialization Screen

- ii. Initialize Wallet: A user who wants to initialize a new unique wallet, can use the Initialize Wallet function. On clicking the initialize wallet button, the App displays a mnemonic. The user needs to copy and store this mnemonic securely for export and import functions. (mnemonic can also be viewed in setting section of PCM app)
To be noted: Mnemonic is used to encrypt/ decrypt/ secure the wallet.



1.14 Initialization Screen

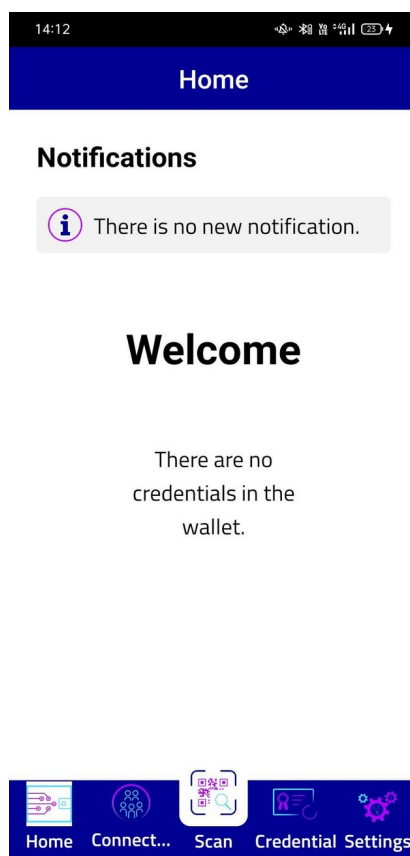
Successful Screen



1.15

Registration

- g. On clicking the 'Next' button, the App creates a wallet, and redirects the user to the wallet welcome screen.



1.16 Home Screen

Features

1. Connection

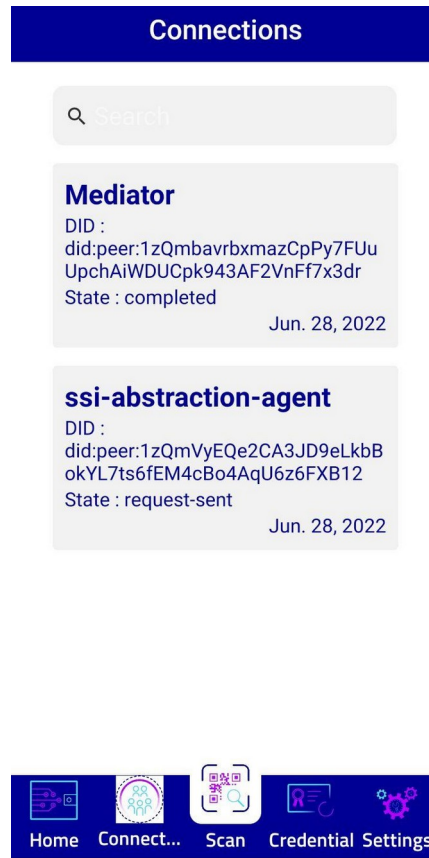
The Connection in Aries Framework forms secure messaging channels called DID Communication or DIDComm. DIDComm messaging provides a secure, interoperable, and flexible general messaging overlay for the entire internet. So to communicate with an Organization a PCM Application needs a Trusted Connection established between the PCM application and Organizations OCM. Over these established Trusted connections only the PCM app can receive credentials and proof requests.

1. Create Connections :

To establish a connection with an Organization the user can either scan the QR code provided by that organization using the 'Scan' option available on the menu bar at the bottom of application, or by entering the Invitation URL provided by the Organization. The user next needs to provide consent to proceed further, and finally from the Connection Invitation screen the user needs to accept the connection by clicking on 'Yes'. The successful connections can then be viewed from the List Connections Screen.

2. View Connections :

A user can view the successfully established connections from the 'Connections' tab on the menu bar at the bottom of the app. This tab lets a user check all his available connections and displays "No connections available" if there are no connections.

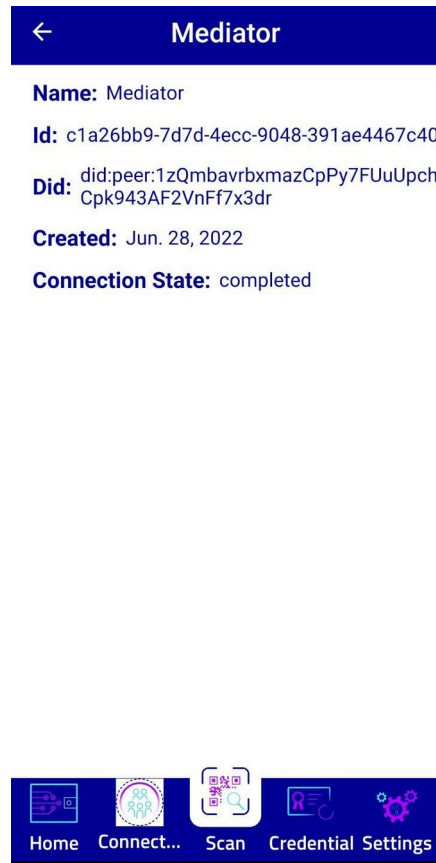


2.1 View Connections

3. View Connection Details

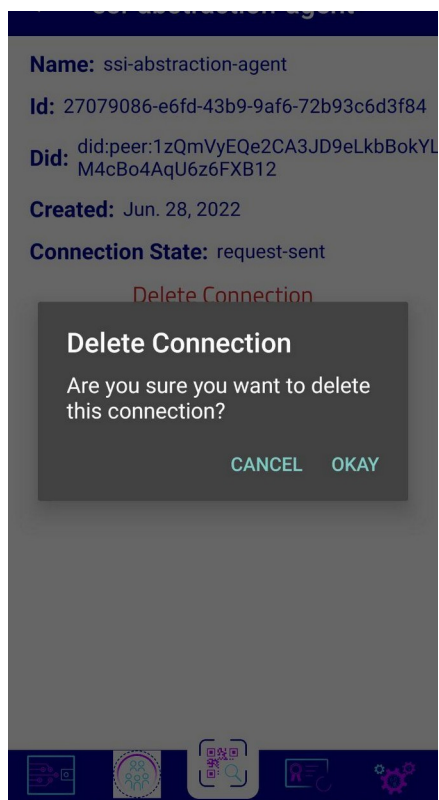
By clicking on a connection from the connection list, a user can view details with respect to the connection.

2.2 Connection Details



4. Delete Connection

- a. If the user wishes to delete a specific connection, from the connection list the user needs to select the connection, expand it to view details, and then using the delete button, delete the connection.



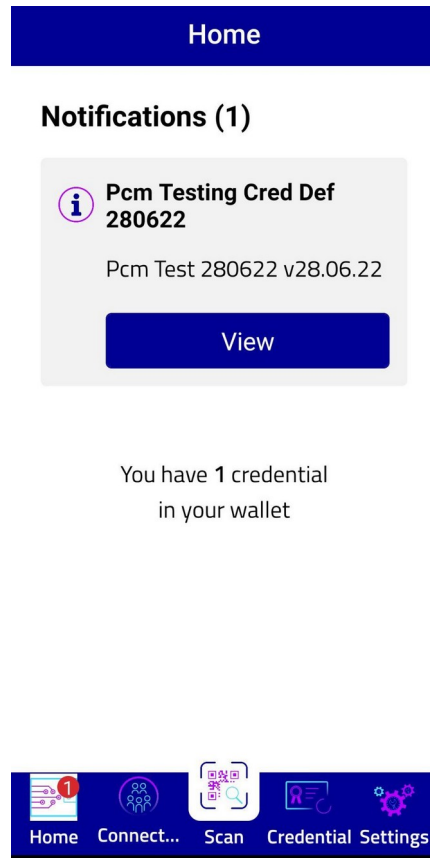
2.3 Delete Connection

3. Credentials

A credential is a set of one or more claims made by the same entity. A verifiable credential is a set of tamper-evident claims and metadata that cryptographically prove who issued it. The PCM App allows a user to hold multiple Verifiable Credentials based on W3C standards. Following is an overview of how a user can interact with credentials.

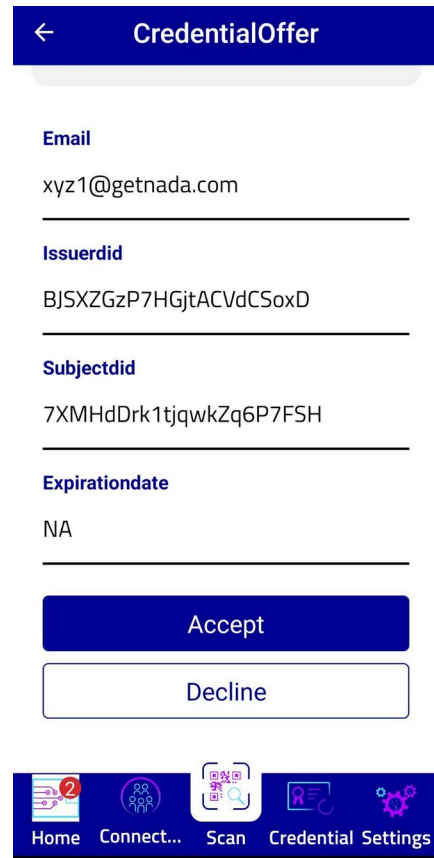
1. Offered Credentials

- a. A user can view credential offers on the home screen. The user can click on this offer to view, accept or decline its acceptance. Once the user accepts the credential, it gets stored uniquely on the user's PCM wallet and the user can view it from the Credentials List.



3.1 Credential Offer Notification

Accept



3.2 Credential Offer



The credential is on the
way



Cancel

Credential added to the
wallet



Done

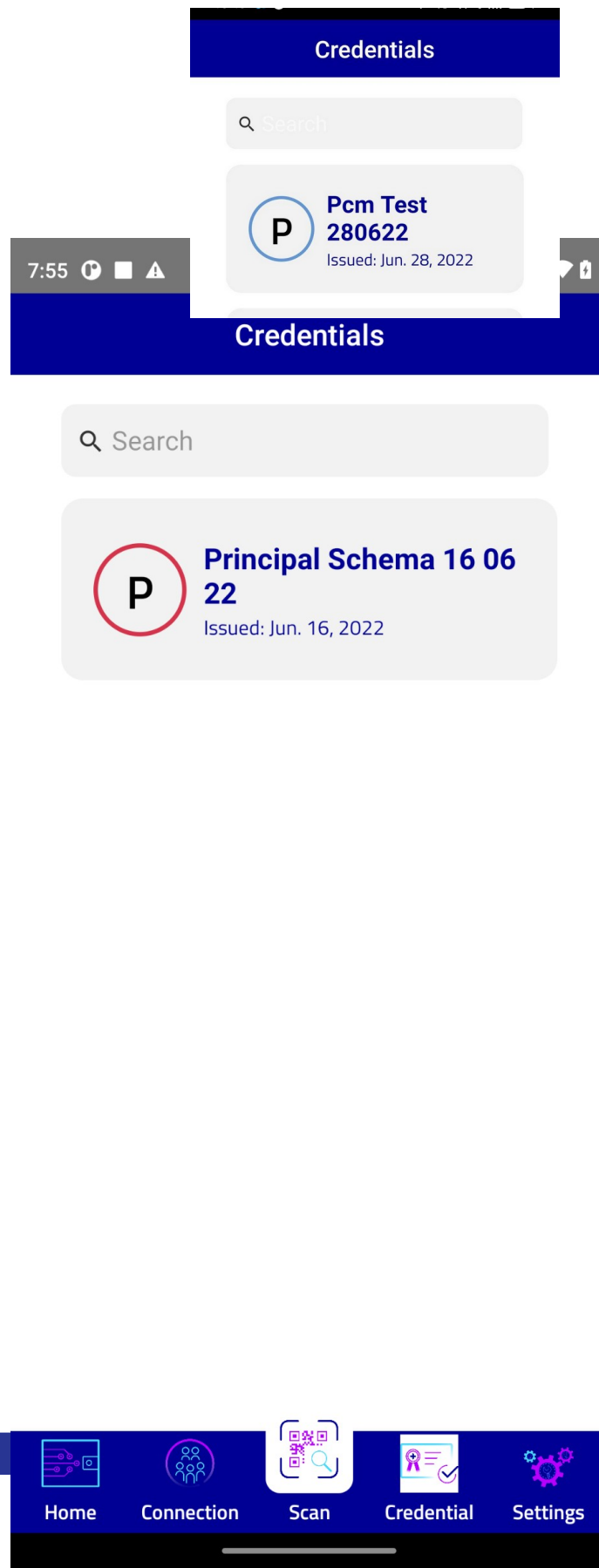
3.3 Credential Acceptance State

3.4 Credential Received

State

2. View Credentials

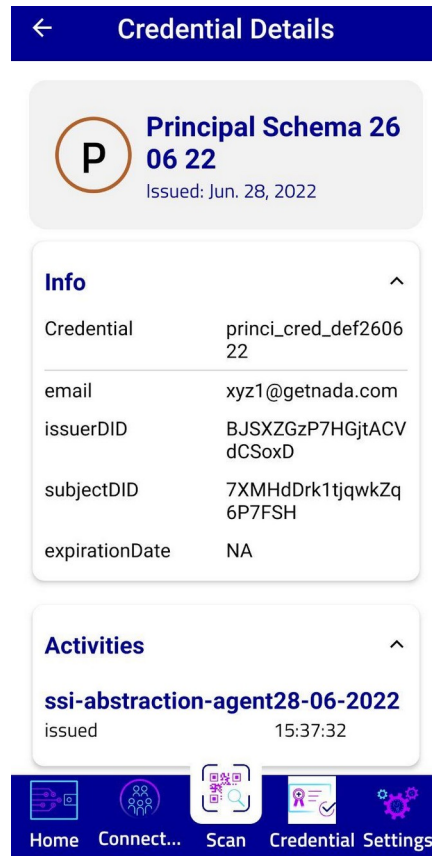
- a. A user can view successfully accepted credentials from the 'Credentials' tab on the menu bar at the bottom of the app. This tab facilitates the user with all the credentials held by the PCM App.



3.5 View Credentials

3. View Credential Details

- a. By clicking on any credential from the credential list, a user can view details with respect to the specific credential.



3.6 View Credential Details

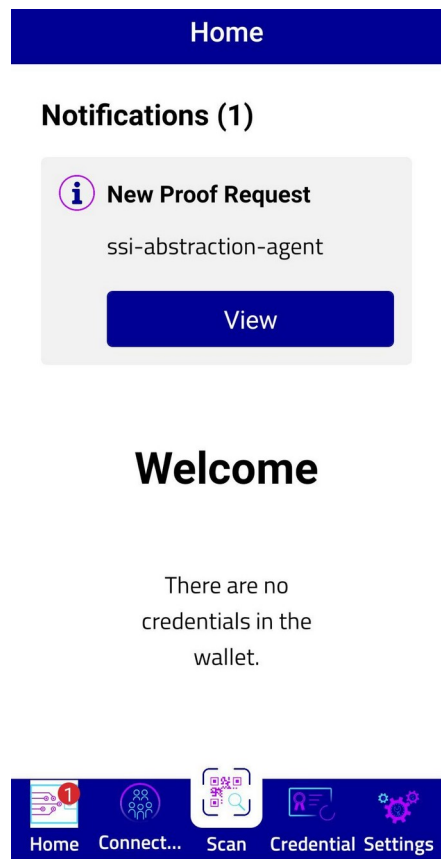
4. Proof Presentation

To verify the identity of a user, a verifier initiates Proof Presentation Request to the PCM User on the PCM App. A PCM user can view this proof request received, can accept or decline sharing credentials or credential attributes requested in the

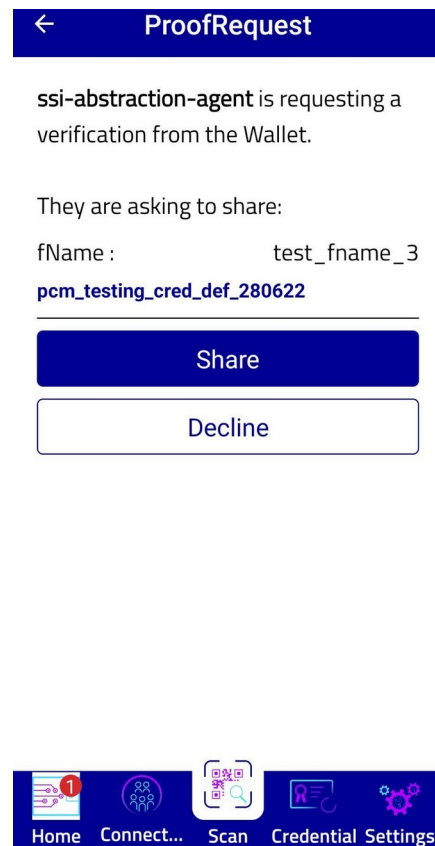
request. A PCM user can also view the detailed information with respect to the history of presentations shared with verifiers.

1. Share Verifiable Credentials

- a. The User receives the Proof Presentation Request on the homescreen of the PCM App. The user next needs to expand the request to view the credentials requested and accept or decline to share as needed. Also if the user has multiple credentials with the same Schema-Id or Credef-Id, the user has the power to choose which credential to share.



4.1 Proof Request Notification

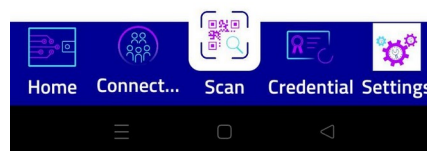
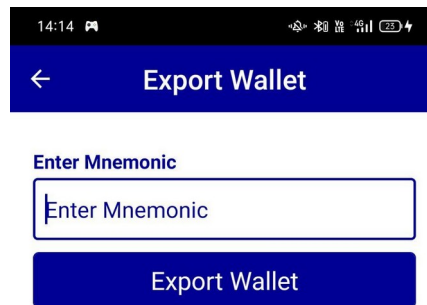


4.1 Share Proof

5. Export Wallet

To provide portability for the PCM wallet, the PCM App provides the Export Wallet Feature. To avail this the user should :

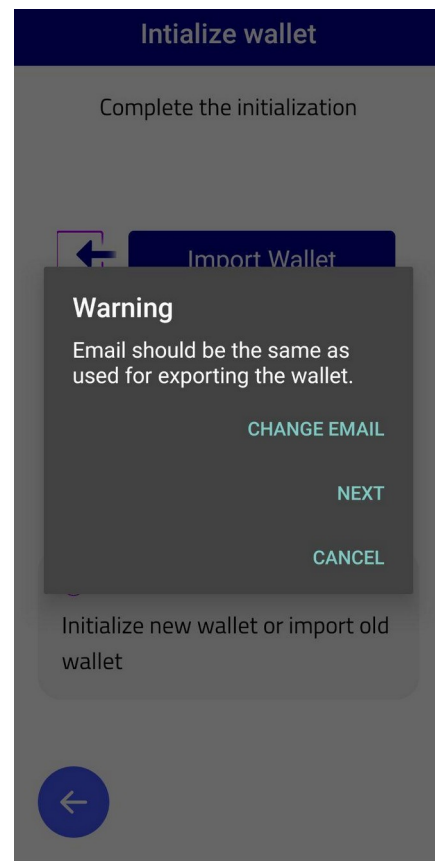
1. Click on the Settings Screen and then navigate to the Export Wallet screen.
2. The user is now requested to enter the mnemonic provided before wallet creation (In case if the user fails to save it at time of wallet initialization then the User can view the mnemonic from the View mnemonic tab under settings). Once the correct mnemonic is provided the user can click on the “Export Wallet” button. The application might ask for permission for file read and write, once provided the PCM App will export the wallet to local storage and navigate the user back to settings.



6. Import Wallet

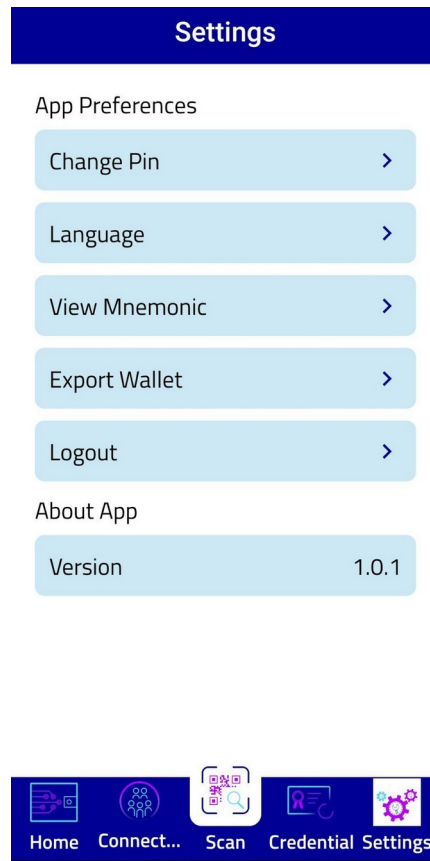
In case a user wants to move the wallet to a new device, the Import wallet function on the new device will help the user to import an already exported wallet.

1. The Import wallet function can be initiated during the onboarding process after pin creation.
2. The user needs to click on "Import Wallet" to initiate the process.
3. Next the user is expected to upload the wallet file previously exported, and then enter the corresponding mnemonic (save earlier with wallet file). It should also be noted that the email provided should be the same as one used while exporting the wallet.
4. Once both are provided, the PCM app validates them and restores the wallet on the device.

**6.1 Initialization****6.2 Import Wallet**

7. Settings

The settings tab provided in the PCM app facilitates the user to change wallet pin, set language, view mnemonic, export wallet, and logout functions.



7.1 Settings Screen

1. Change Pin

- a. The user can change the wallet Pin by first entering the current Pin and then updating it with new Pin after verification of original Pin

← ChangePin

Enter Old Pin

6 Digit PIN

Enter New PIN

6 Digit PIN

Re-Enter the New PIN

6 Digit PIN

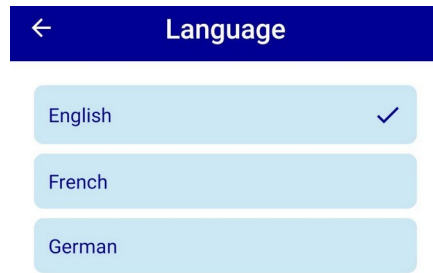
Change PIN

Home Connect... Scan Credential Settings

7.2 Change Pin

2. Language

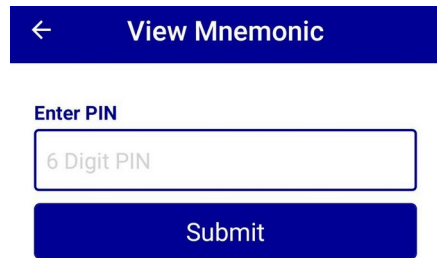
- a. If the user wishes to change the language of the PCM application, the Language setting will come into play. The languages offered are English (default), German, French.



7.3 Change the language

3. View Mnemonic

- a. To view mnemonic, users can use the View Mnemonic feature. Under this the user is required to re-enter the wallet Pin, for user verification before Mnemonic is shown.

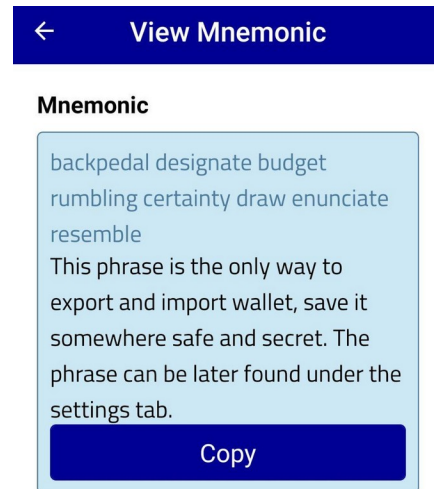


← View Mnemonic

Enter PIN

6 Digit PIN

Submit



← View Mnemonic

Mnemonic

backpedal designate budget
rumbling certainty draw enunciate
resemble

This phrase is the only way to
export and import wallet, save it
somewhere safe and secret. The
phrase can be later found under the
settings tab.

Copy



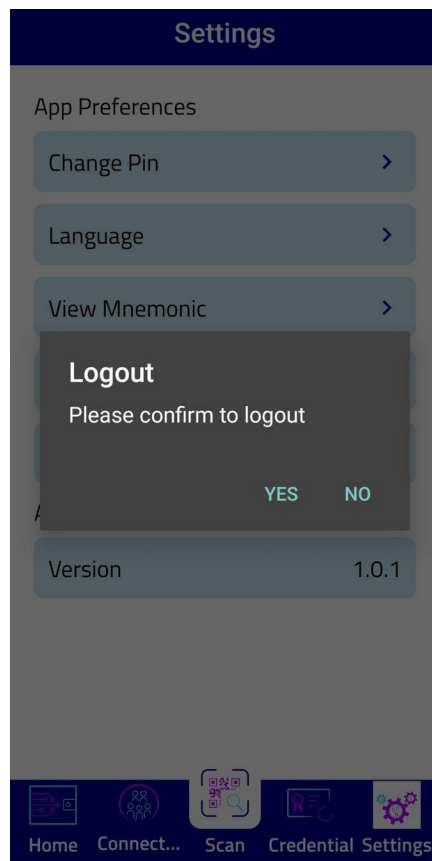
7.4 Enter Pin



7.5 View Mnemonic

4. Logout

- a. The user can Logout of the application using the Logout option.



7.6 Logout