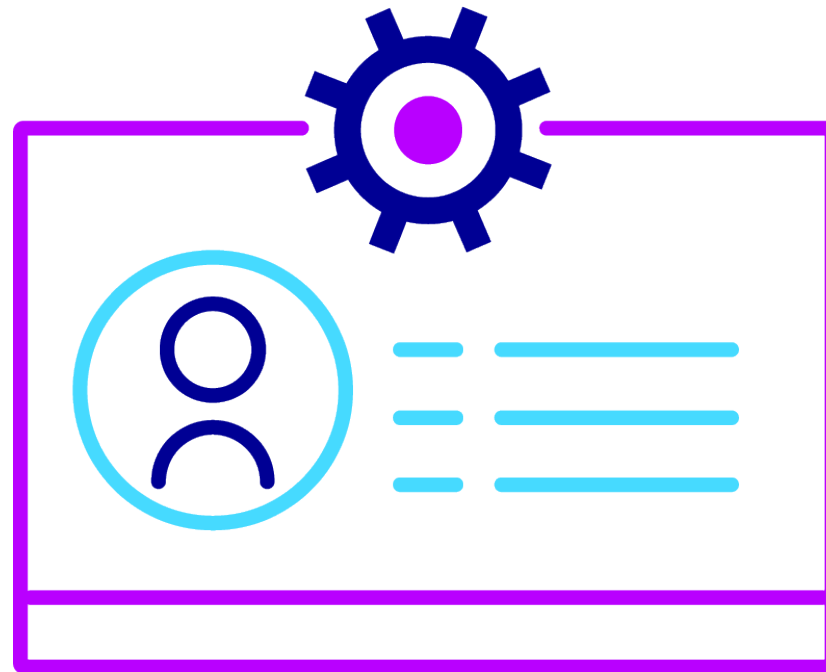


GXFS Personal Credential Manager



User Manual

Revision table

1.0	June 2022 Initial release	
1.1	March 2023 Update	* Remove OTP verification * Added “Delete account” feature

Copyright and Published by

©Vereign AG, Kolinplatz 10, 6300 Zug, Switzerland

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA



Table of Content

Table of Contents

1 Overview.....	4
2 Install mobile application.....	4
3 Getting started.....	5
3.1 Onboarding.....	5
3.2 Features.....	11
3.2.1 Connections.....	11
3.2.2 Credentials.....	15

3.2.3 Proof Presentation.....	18
3.2.4 Export/Import wallet.....	19
3.2.5 Settings.....	21



1 Overview

The GXFS “Personal Credential Manager” is a full-featured smartphone-based 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 sovereign, transparent, privacy-preserving, secure and trustworthy 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 proven manner
- ✓ Secure storage and management of respective secrets

2 Installation of the GXFS PCM

The GXFS PCM mobile application is available for Android and iOS operation systems and can be downloaded from the respective stores

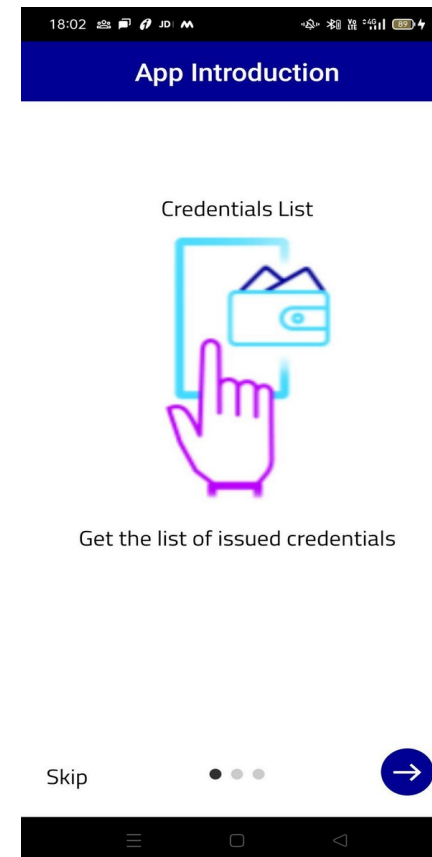
Google Play Store	You may search and download the GXFS Personal Credential Manager from Google Play Store(https://play.google.com/store/apps/details?id=eu.gaiax.difs.pcm)	
Apple App Store	You may search and download the GXFS Principal Credential Manager from Apple App Store (https://apps.apple.com/app/gxfs-pcm/id1662845551)	

3 Getting started

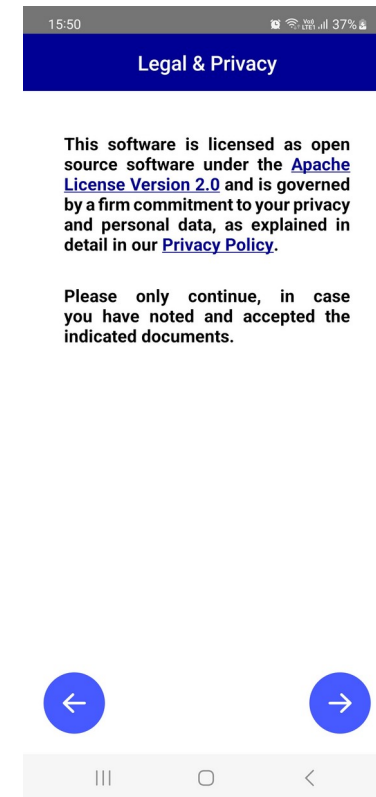
3.1 Onboarding

- a) After starting the application you need to complete the registration process. The application introductory screens come up, if the application is started for the first time.

You may either click on the “Skip” button to skip these introductory screens or you can click on the “Next” button to go through the screens.

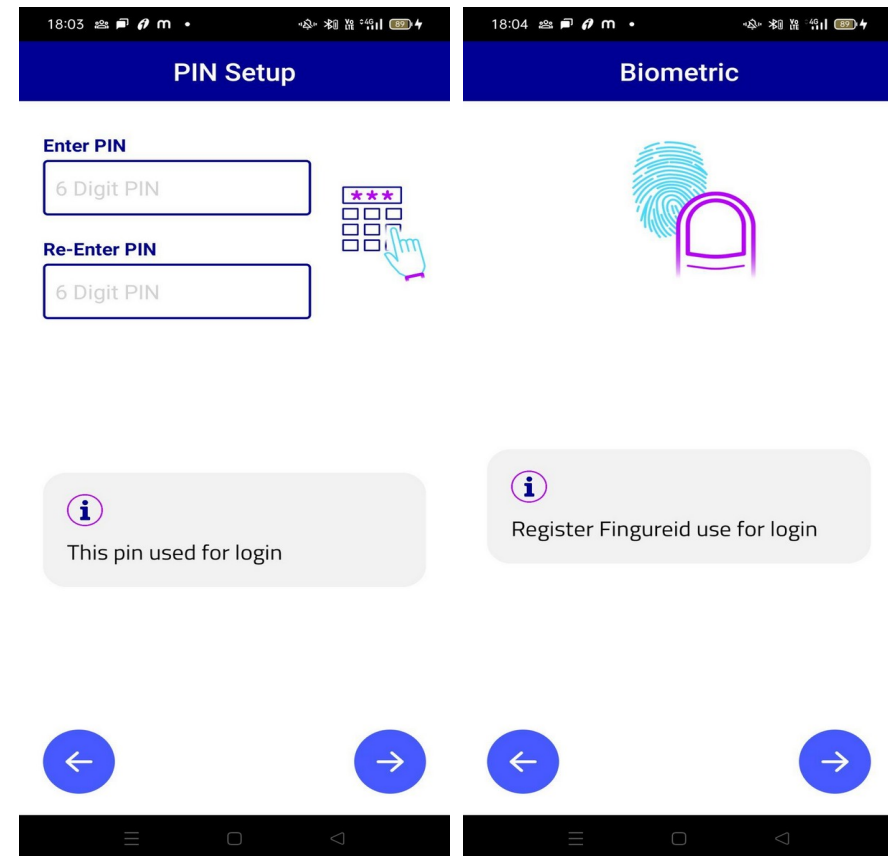


- b) The Legal & Privacy screen is a requirement in order to properly inform you about the applicable licensing terms and data protection policy.



- c) For securing the login and for wallet authentication, you are prompted to set up a PIN (6 Digit).

You may additionally provide your Biometrics for ease of use (if this option is supported by your device).



d) Once the PIN is set up, you are presented with two options:

- Import Wallet
- Initialization



e) **Import Wallet**

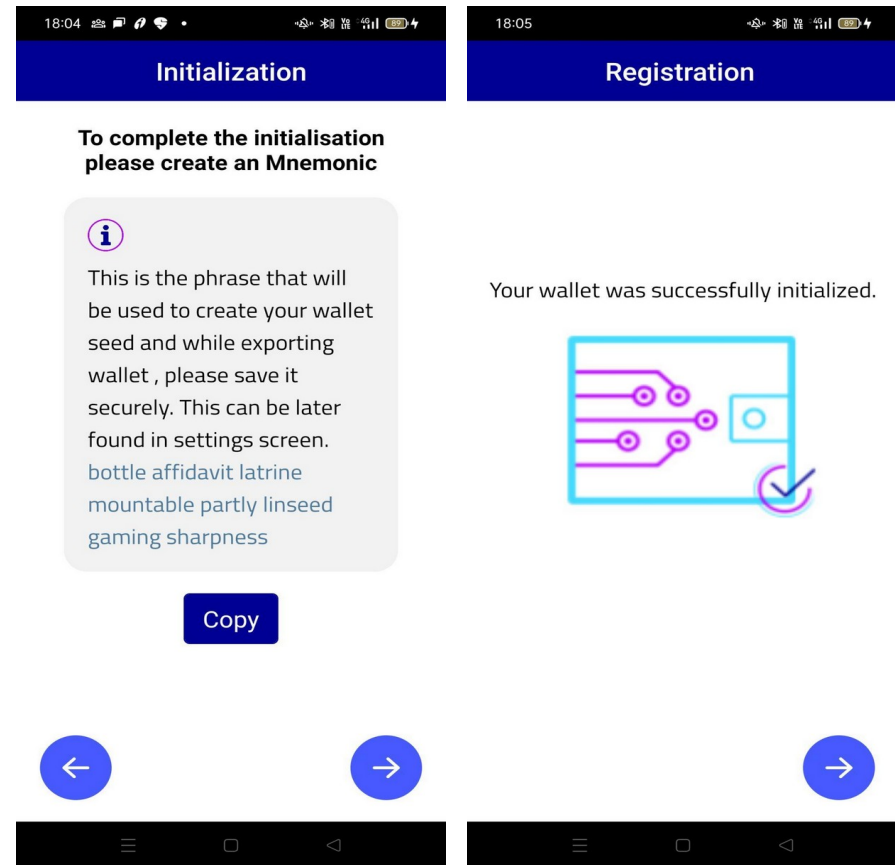
If you previously used the GXFS PCM and you have the previous wallet exported, then import the wallet by clicking the “Import Wallet” button. This redirects you to the Import Wallet Screen ([See section 3.2.4](#))

f) Initialization

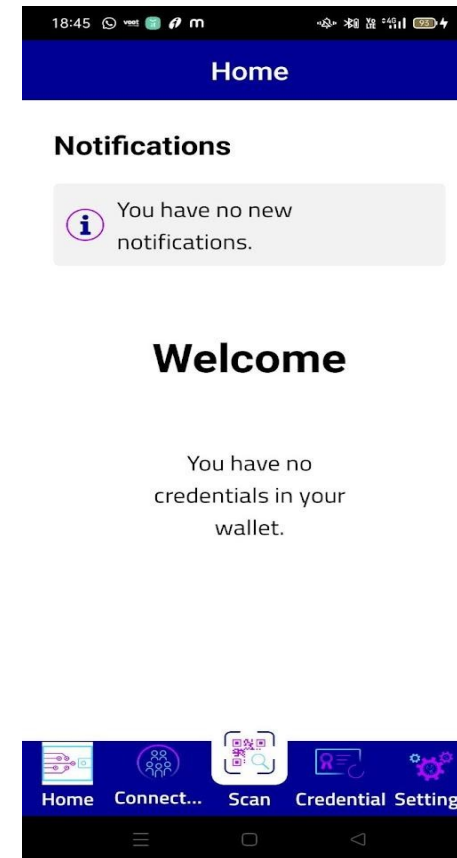
If you want to create a new unique wallet, select the "Initialization" button.

Upon clicking the Initialization button, the App displays an individual mnemonic and you are strongly advised to write it down or copy it and keep this mnemonic somewhere safe, because this mnemonic is a mandatory requirement for exporting or importing your wallet later on. Hence, you will need this mnemonic in case you either want to backup your wallet or restore such a backup. Your individual mnemonic can also be found in the Setting section of your PCM later on.

Note: Mnemonic is used as seed to create the wallet.



Once the wallet is successfully created you will be redirected to the Home screen.



3.2 Features

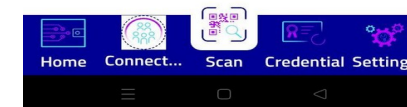
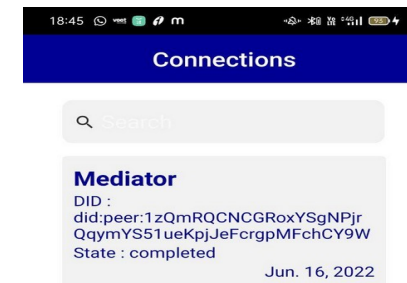
3.2.1 Connections

A Connection via the Aries Framework establishes secure messaging channels called DID Communication or DIDComm. Such DIDComm messaging provides a secure, interoperable, and flexible general messaging overlay for the entire internet. To communicate securely, a trusted connection between the PCM application and Organizations OCM is required. Over these established trusted connections only the GXFS PCM can receive credentials and proof requests.

a) Establish Connections

To establish a connection with an individual organization you 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.

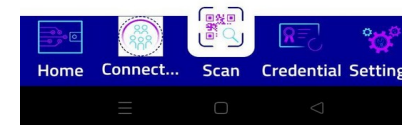
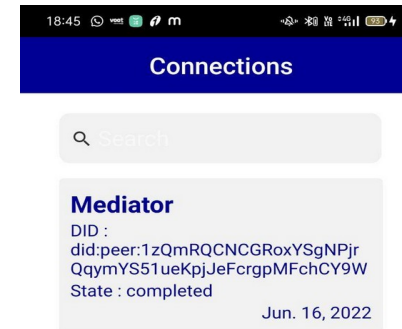
You will then be prompted to provide your consent to proceed further. And finally you are required to accept the connection by clicking on 'Yes'.



b) **View Connection**

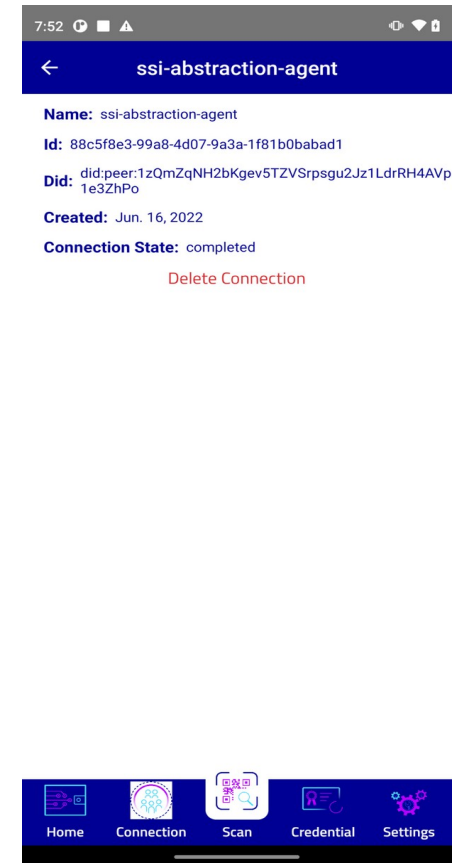
You can inspect all successfully established connections under the 'Connections' tab on the menu bar at the bottom of the app.

"No connections available" is displayed in case there are no connections, yet.



c) **View Connection Details**

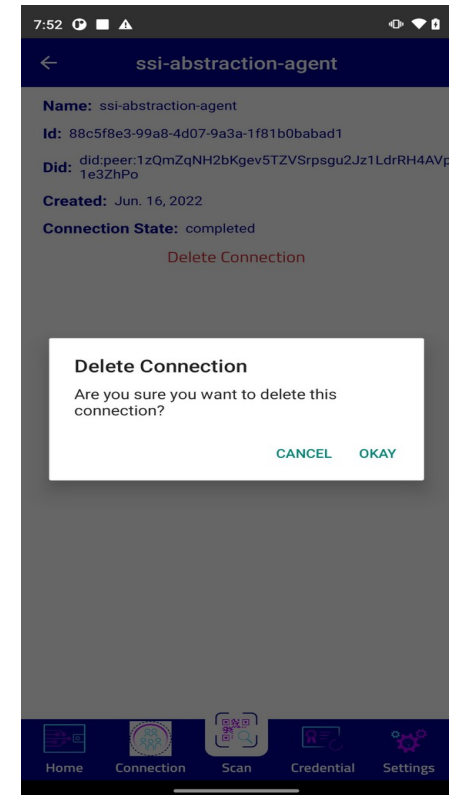
By clicking on an individual connection in the connection list, you can view the details with respect to this particular connection.



d) **Delete Connection**

If you want to delete a specific connection, you need to select the respective connection from the Connections list and thereby expand it to view its details (as described above).

After that, you just need to select the “Delete Connection” button and confirm that you indeed want to delete this individual connection



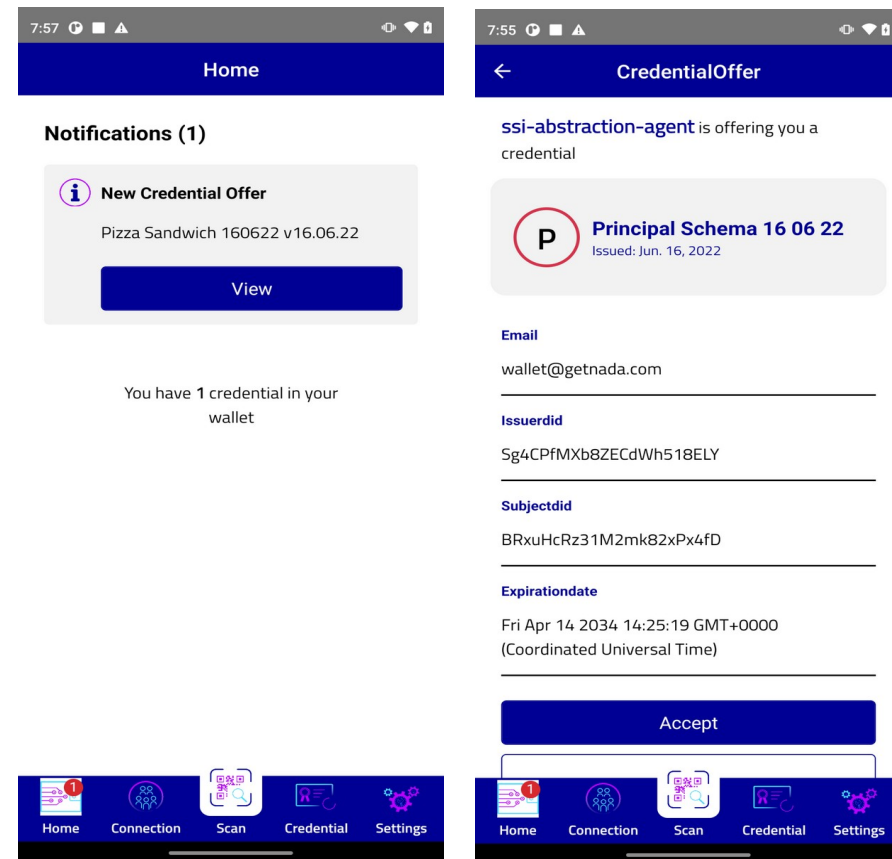
3.2.2 Credentials

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 proves who issued these claims (including its metadata). The GXFS PCM allows you to hold multiple Verifiable Credentials based on W3C standards. In the following an overview is provided, on how you can choose to interact with such credentials.

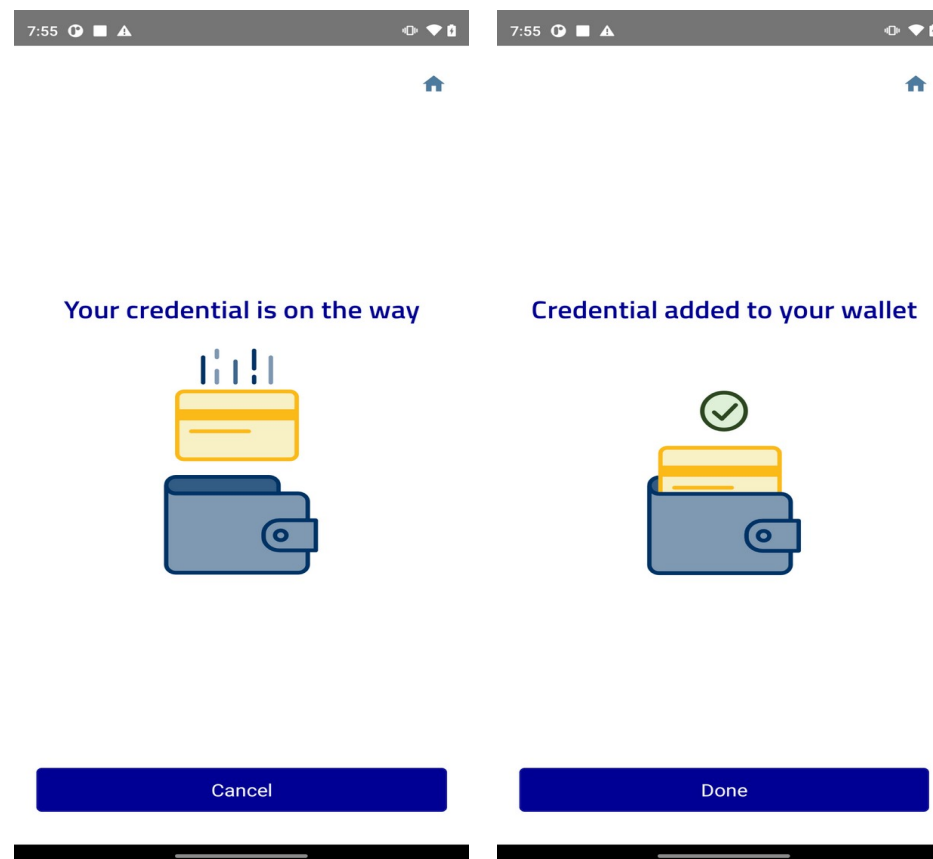
a) Receiving Credentials

You are prompted with a Notification on the Home screen, in case a credential offer is received by your GXFS PCM.

You can click on this offer to review it, and either choose to “Accept” or “Decline” it.



Once you accept a credential, it is stored in your PCM wallet and from now on you may inspect it in your “Credentials” List.

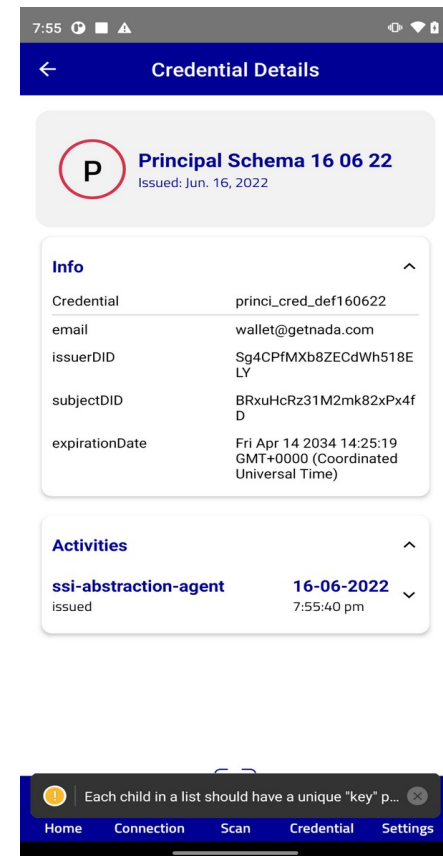
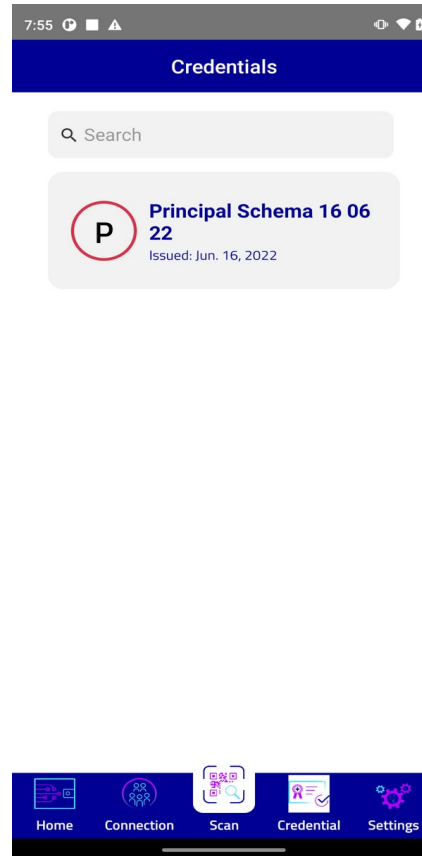


b) View Credentials

You can view any successfully accepted credentials from the 'Credentials' tab on the menu bar at the bottom of the app.

This tab shows all the credentials held by your PCM App.

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



3.2.3 Proof Presentation

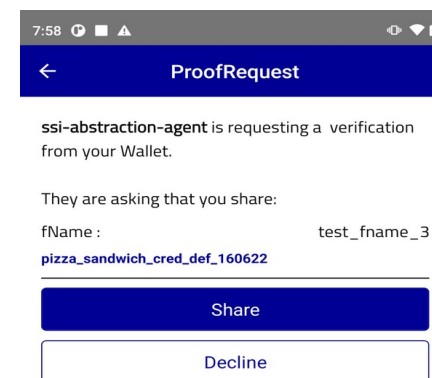
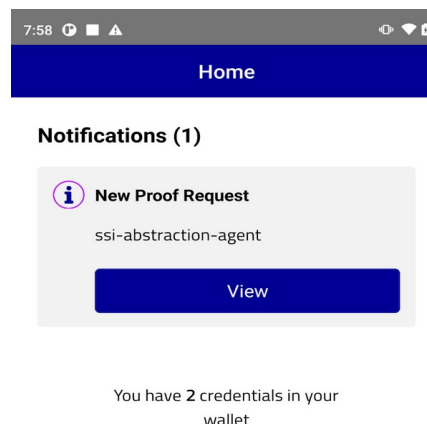
To verify your identity, a verifier may initiate a Proof Presentation Request and send it to your GXFS PCM. You will be prompted with this proof request on your Home screen, and you may either accept or decline sharing the specified credentials or credential attributes. To provide you with an overview and transparency you will have the opportunity to check the detailed information, with respect to the history of your presentations shared with individual verifiers.

Share Verifiable Credentials

On your Home screen, you are prompted with a Notification in case of any Proof Presentation Requests.

You may expand the request to view the credentials requested and either accept or decline to share as needed.

In the event of you holding multiple credentials with the same Schema-Id or Credef-Id, you may choose which credential to share.



3.2.4 Export/Import wallet

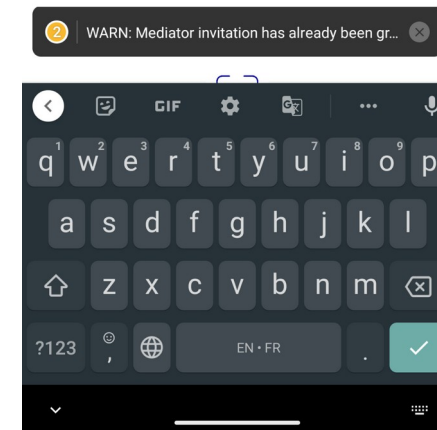
a) **Export wallet**

Click on the 'Settings' menu and then navigate to the "Export Wallet" option.

Now you are requested to enter the mnemonic phrase provided before wallet creation (in case the user fails to save it earlier then the User can view the mnemonic from the View mnemonic tab under settings).

Once the correct mnemonic is provided, 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.



b) Import wallet

In case you want to use the GXFS PCM on a new device, the import wallet function on the new device provides you with the opportunity to import an already exported wallet.

The Import wallet function can be initiated during the onboarding process after pin creation.

You just need to click on "Import Wallet" to initiate the process.

Next you are expected to upload the wallet file previously exported, and then enter your individual and secret mnemonic (saved or written down earlier).

Once both are provided, the GXFS PCM app validates and in case everything is provided correctly, restores the wallet on the new device.



3.2.5 Settings

The `Settings` menu provide functionalities like Change wallet pin, set language, view mnemonic, view applicable legal terms (like privacy policy and license terms), export wallet, logout functions and delete all data. These Features are rather self-explanatory.

Remove all data

Selecting `Remove all Data` button and then confirming the action, all data within your wallet (your GXFS PCM) will be erased. Such data includes any Connection, Credentials and personal Settings.

Your wallet and the overall GXFS PCM will be reverted in to initial state.

Once all data is delete the only way to restore it is to Import it from previously saved backup. The import wallet function is described in the previous section .

