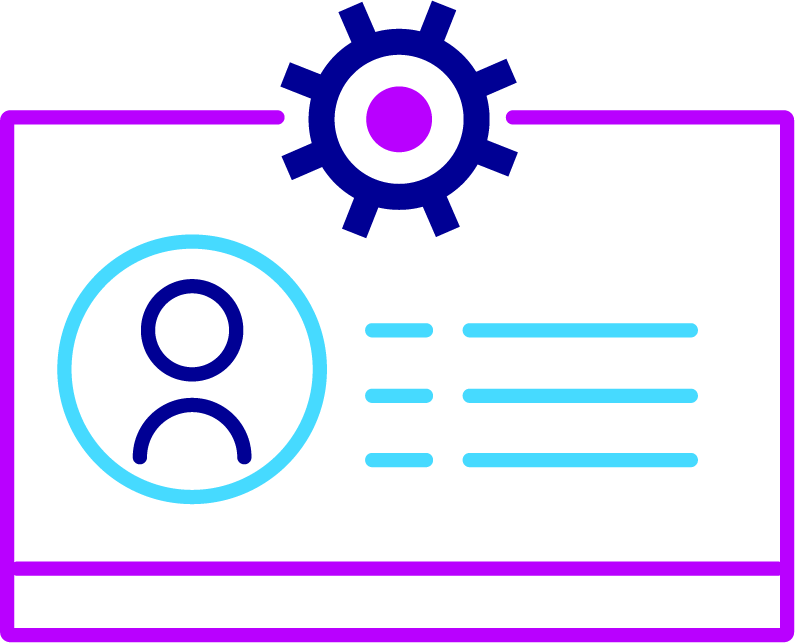
GXFS Personal Credential Manager



User Manual

**Revision table**

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

**Published by**

eco – Association of the Internet Industry (eco – Verband der Internetwirtschaft e.V.)

Lichtstrasse 43h

50825 Cologne, Germany

**Copyright**

© 2023 GAIA-X European Association for Data and Cloud AISBL

**Table of Content**

**Table of Contents**

[1 Overview 4](#__RefHeading___Toc1854_897510659)

[2 Install mobile application 4](#__RefHeading___Toc1899_897510659)

[3 Getting started 5](#__RefHeading___Toc1901_897510659)

[3.1 Onboarding 5](#__RefHeading___Toc1903_897510659)

[3.2 Features 11](#__RefHeading___Toc1905_897510659)

[3.2.1 Connections 11](#__RefHeading___Toc1907_897510659)

[3.2.2 Credentials 15](#__RefHeading___Toc1909_897510659)

[3.2.3 Proof Presentation 18](#__RefHeading___Toc1911_897510659)

[3.2.4 Export/Import wallet 19](#__RefHeading___Toc795_191172049)

[3.2.5 Settings 21](#__RefHeading___Toc421_191172049)

# Overview

The “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 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

# **Install PCM application**

GXF PCM mobile application is available for Android and iOS operation systems and can be downloaded from the respective store

|  |  |  |
| --- | --- | --- |
| **Google Play Store** | Users can search and download the Principal Credential Manager Application from Google Play Store( <https://play.google.com/store/apps/details?id=eu.gaiax.difs.pcm> ) |  |
| **Apple App Store** | Users can search and download the Principal Credential Manager Application from Apple App Store ( <https://apps.apple.com/app/gxfs-pcm/id1662845551> ) |  |

# Getting started

## Onboarding

|  |  |  |
| --- | --- | --- |
| 1 | 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.  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. |  |
| 2 | Legal & Privacy is required in order to keep you informed about the licensing and data protection rules. |  |
| 3 | Set up PIN (6 Digit) and configure Biometric (If the device supports), for wallet authentication. |  |
| 4 | Once the PIN is set up, Users are presented with two options:   * Import Wallet * Initialization |  |
| 5 | **Import Wallet**  If you previously used GXF PCM App and you have the previous wallet exported then import the wallet by clicking the “Import Wallet” button. This redirects you to Import Wallet Screen( [See section 3.2.4](#_toc460)) |  |
|  | **Initialization**  If you want to create a new unique wallet, select “Initialization” button function.  Upon clicking the create wallet button, the App displays a mnemonic and you **must** to copy and store this mnemonic for export and import functions. (mnemonic can also be viewed in setting section of PCM app)  Note: Mnemonic is used as seed to create the wallet. |  |
|  | Once the wallet is successfully created you will be redirected at application dashboard |  |

## Features

### Connections

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. To communicate securely a Trusted Connection between the PCM application and Organizations OCM is required. Over these established Trusted connections only the PCM app can receive credentials and proof requests.

|  |  |  |
| --- | --- | --- |
|  | **Establish Connections**  To establish a connection with an Organization the 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.  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. |  |
|  | **View Connection**  You 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. |  |
|  | **View Connection Details**  By clicking on the connection from the connection list, you can view details with respect to the connection. |  |
|  | **Delete Connection**  If you want to delete a specific connection, from the connection list the select the connection, expand it to view details, and then using the “Delete Connection” button. |  |

### 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 you to hold multiple Verifiable Credentials based on W3C standards. Following is an overview of how a user can interact with credentials.

|  |  |  |
| --- | --- | --- |
|  | **Offered Credentials**  You can view credential offers on the home screen.  You can click on this offer to review it, and “Accept” or “Decline” it.  Once you accepts the credential, it gets stored uniquely in PCM wallet and you can find it in the Credentials List. |  |
|  | **Receiving Credential**  Once you accepts the credential, it gets stored uniquely in PCM wallet and you can find it in the Credentials List. |  |
|  | **View Credentials**  You can view successfully accepted credentials from the ‘Credentials’ tab on the menu bar at the bottom of the app.  This tab facilitates all the credentials held by the PCM App.  By clicking on any credential from the credential list, you can view details with respect to the specific credential. |  |

### 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.

|  |  |  |
| --- | --- | --- |
|  | **Share Verifiable Credentials**  You receive 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. |  |

### Export/Import wallet

|  |  |  |
| --- | --- | --- |
|  | **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. |  |
|  | **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.  The Import wallet function can be initiated during the onboarding process after pin creation.  The user needs to click on “Import Wallet" to initiate the process.  Next the user is expected to upload the wallet file previously exported, and then enter the corresponding mnemonic (save earlier with wallet file).  Once both are provided, the PCM app validates them and restores the wallet on the device. |  |

### **Settings**

The `Settings` menu provide functionalities like Change wallet pin, Set language, View mnemonic, Export wallet, Logout functions and Delete all data. Features are self-explanatory and we develop them in ease of use manner.

|  |  |  |
| --- | --- | --- |
|  | **Remove all data**  Selecting `Remove all Data` button and then confirming the action, all data within your wallet (PCM) will be erased. Such as Connection, Credentials, Settings etc.  The wallet will be reverted in to initial state.  Once data is delete the only way to restore it is to Import it from a backup. The import wallet function is described in the previous section . |  |