KEEPSER COLD WALLET

USER MANUAL

Keepser Cold Wallet - PRO

KEEPSER COLD WALLET - PRO

Our products are engineered to meet the highest standards of quality, functionality, and design.
We hope you thoroughly enjoy your new Keepser Cold Wallet.

Before Use
Please read these user instructions carefully and completely before using the product and retain for future reference.

The Keepser Cold Wallet (Keepser Cold Wallet) solution has 6 components described in this User Manual :

- Keepser Cold Wallet Definition
- Keepser Application (App)
- Data Menu
- Keepser Plugin.
- User Settings Menu
- Administration Menu

Keepser Cold Wallet - PRO Definition

Products

Keepser Cold Wallet, is a black card secure storage device, which is capable of storing your passwords, access codes, credit card information, fidelity card information, crypto-currency and wallet private key, and more that you will discover in this User Manual.

What do I find in the package?

- **Keepser Cold Wallet PRO – Black Card.**

- **QR CODE stickers, one for "MY CARD"**

It is used to connect you new Keepser card to a phone or several phones.

- **QR CODE to access User Manual, FAQ and more.**

The package contains a QR Code printed on a form titled « User Manual, FAQs, and more. Scanning it will allow you to access this User Manual, videos tutorials, and FAQs. You will be able to download these documents as you feel necessary.

Definition terms in the context of Keepser Cold Wallet

KEEPSER APPLICATION

The “Keepser application” or “Keepser App” is a software running on your NFC smartphone, that contains all the features that make you able to use the functionalities from our Keepser Cold Wallet Card.

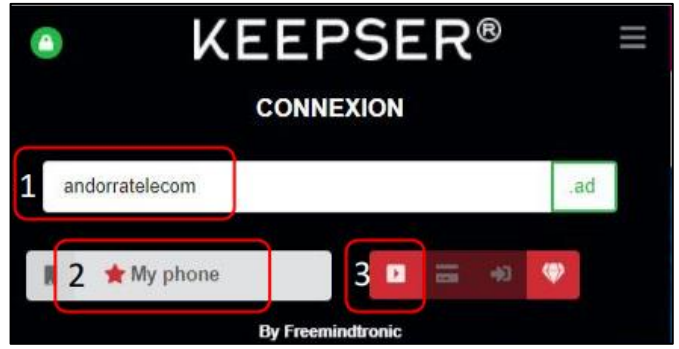
What does the Keepser App do?
The App is the bridge between your Card, you and your computer.

To use your Keepser Application, your phone does not need to be connected to internet, but some functionalities may not be available without Internet connection especially the connection to websites.

KEEPSER PLUGIN

The Keepser Plugin is a smart software module that acts as an add-on to a web browser and gives the browser additional functionality.
The Keepser Plugin can detect which site is visited and allow for the user to perform actions and operations using the Keepser App and the Keepser Card.

The features and capabilities of the Keepser Plugin are described in this manual.



Definition terms in context of Keepser Cold Wallet

- **KEEPS**

This is a very important term to remember.
We call “Keeps" a set of information that you can store in your Keepser Card and that is used to perform various operations such as connection to secure website, e-commerce payment, cryptocurrency operations, and other operations described in this manual. The plural name “Keeps” is used at is often gathers several pieces of data.
For example, (username + password) for accessing your Facebook or Gmail accounts, or (credit card number + expiration date + CVV + card holder), or private key of your crypto-currency wallet.
Each Keeps has a unique name that is assigned by the user of the Keepser Cold Wallet solution.

- **SEED PHRASE**

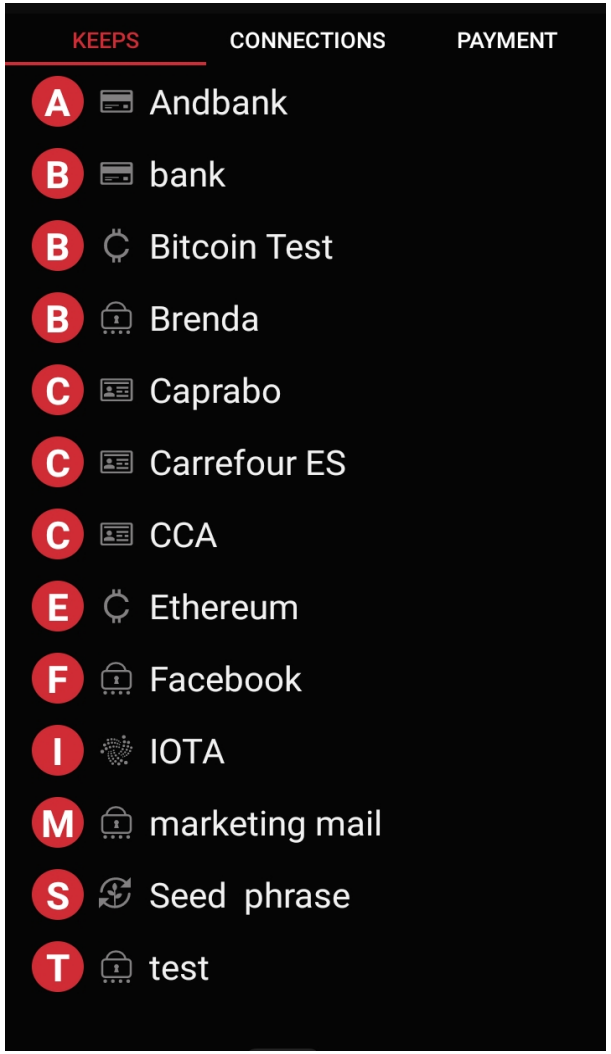
SEED PHRASE, also called Recovery Phrase, or Secret Phrase, is a string of 12 to 24 words generated when you create a new crypto-currency wallet, by yourself or via an exchange platform holding your crypto-currency wallet. It allows you to access all the cryptocurrencies of this wallet and is used to generate keys to perform transactions.
A Keepser Card can contain many SEED PHRASES to manage multiple wallets.

- **RSA 4096 KEY**

RSA-4096 is standardized encryption. It is one of the best encryption systems that you can use to protect your data in transmission. The Keepser Cold Wallet solution allows you to generate and store your own private RSA-4096 keys in the Keepser Card and generate the corresponding public key from it. You can then use it to securely send or share the "Keeps” or establish end-to-end secured communication channels.

- **IOTA**

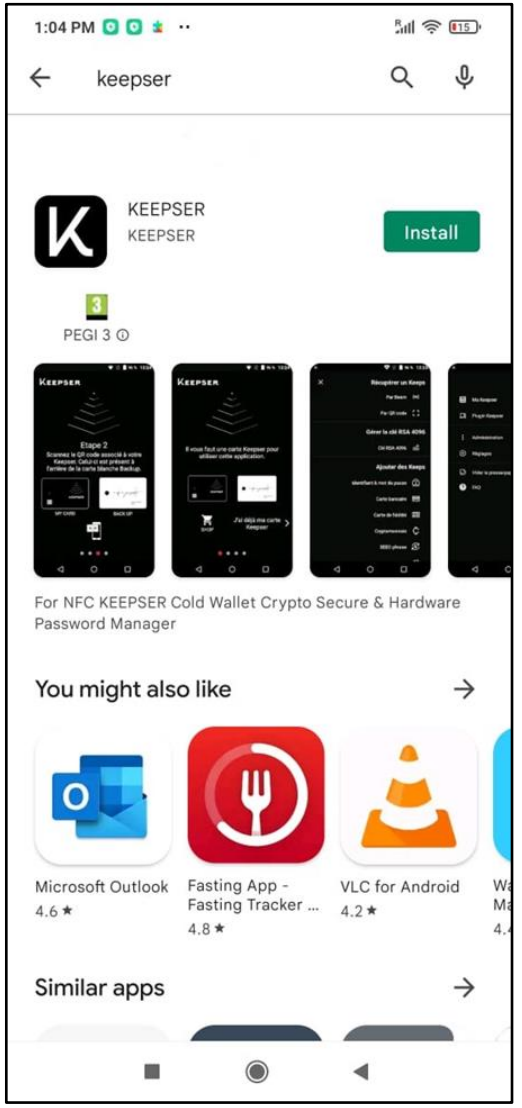
IOTA is an open-source distributed data registry technology. It is not based on blockchain technology but on another technology called Tangle. Iota tokens are like cryptocurrencies, tailored for microtransactions. It aims to securely exchange information and value between Internet of things (IoT) objects.



Before using your Keepser Cold Wallet

WARNING:
In order to use the Keepser Cold Wallet, you need a smartphone with:
1. Android OS – version 6 or above.
2. Support for Near Field Communication (NFC).

An update of this User Manual will be issued when the support for iOS phones (iPhone) will be released.



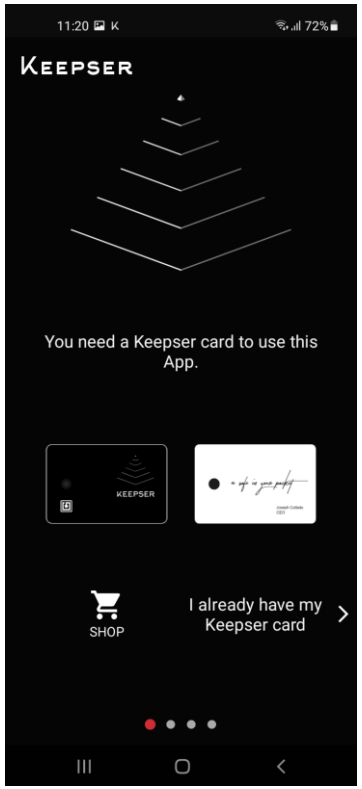
Steps:

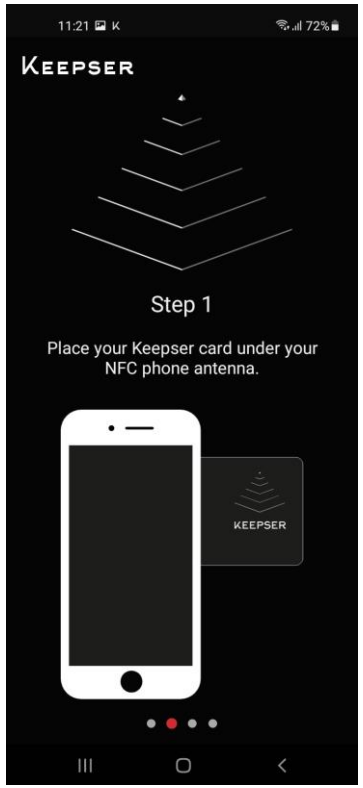
1. Search for the "KEEPSER" Application on Google Play.
(if you do not see the KEEPSER application on Google Play, this means your smartphone is not compatible with the Keepser Cold Wallet solution (no NFC support for example).

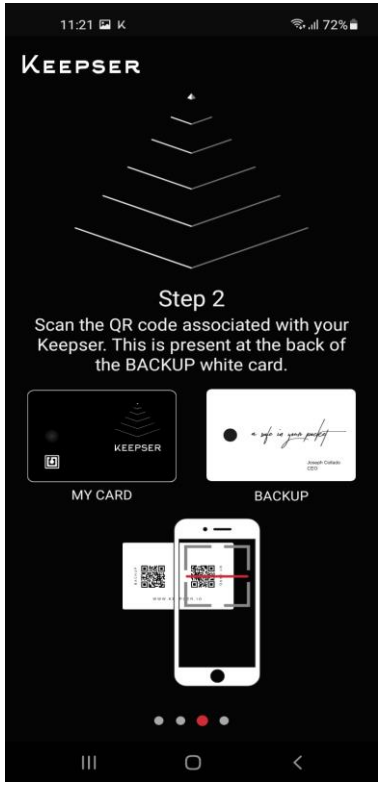
2.- Download and install the application on your smartphone.

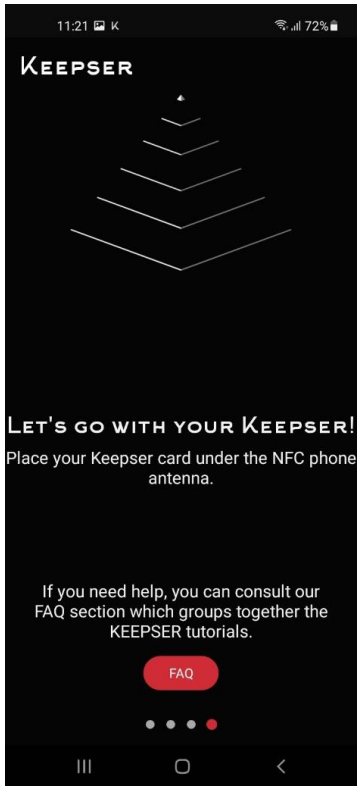
Connecting your Keepser Cold Wallet Card (1/2)

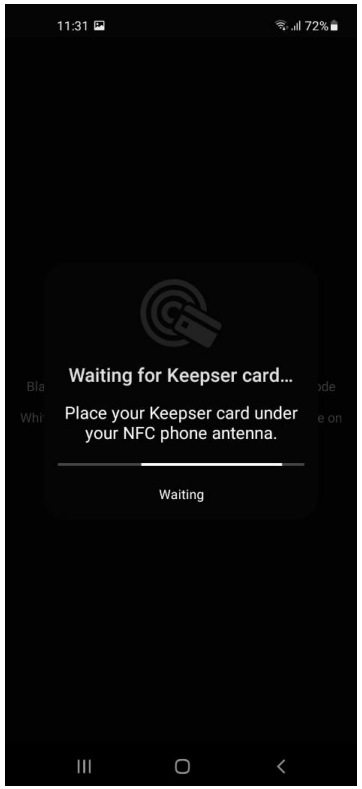
When the Keepser App is installed on your phone, open the Keepser App and read the displayed instructions to connect your Keepser Card and connect it with this phone. Note that you can connect several cards per phones and several phones can be connecting a single card.
(if you do not have a Keepser Card yet or wish to buy a new one, you can tap on the “SHOP” button. It will bring you to the www.keepser.com, e-commerce website where you can finalize your purchases.











(*) About NFC connection.

- Important information:

  - The KEEPSER CARD is very sensitive. You do not need to bring the card in full contact of the back of the smartphone to trigger the NFC connection.

  For best efficiency, it is recommended to let about 1 cm space (a finger width) between the Keepser Card and the phone.

  - When a Keepser Card is approached to NFC phone, you will hear a « bip » sound when the NFC connection is activated.

  - The Keepser Card should be kept within NFC range (few cm), for the duration of the data share between the Card and the Application. Depending upon the operation you will want to do, the amount of data to be shared may vary from few milliseconds to few seconds, and you should wait for a confirmation message before moving the Keepser Card beyond NFC range.

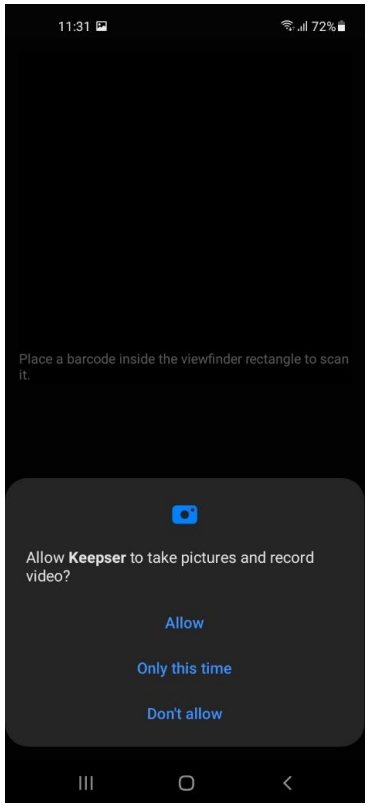
  - NFC antennas of smartphones are usually located on the upper portion of the back, below the cameras. But some phone may have it at another place.

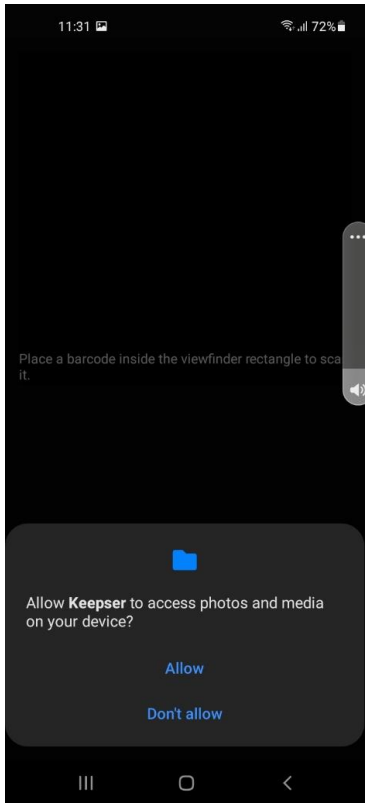
  - If you do not easily manage to pair the NFC Keepser Card with your NFC phone, you should try placing the Keepser Card at different places or consult the technical characteristics of your phone to locate the NFC antenna.

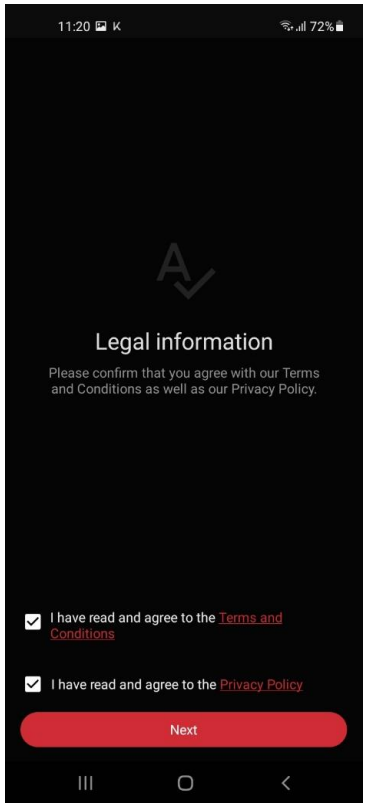
Connecting your Keepser Cold Wallet Card (2/2)

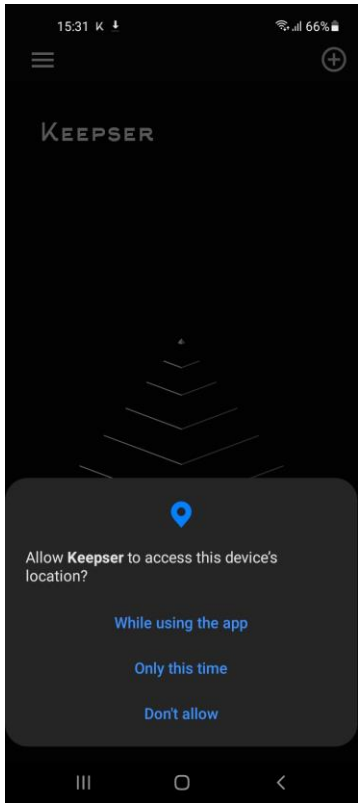
Allow the Keepser App to use the camera (take picture and record video) and to use the photos and media of your device. Then Scan the QR code labelled “MY CARD”.

Put your Keepser Cold Wallet black card under your phone, nearby the NFC antenna, and wait until the “Legal Information” message appears, then accept the legal information (Terms & Conditions , Privacy Policy) and click “next”. You will then be asked to allow for the Keepser Application to access your location. We recommend you allow for it in order to benefit from the geofencing features.







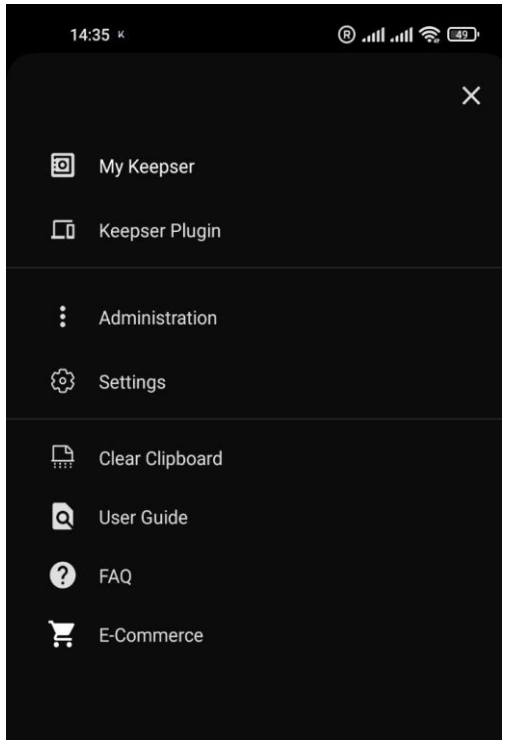


KEEPSER APPLICATION
(App)

Keepser Application /Front Page

Main Menu / Data Menu

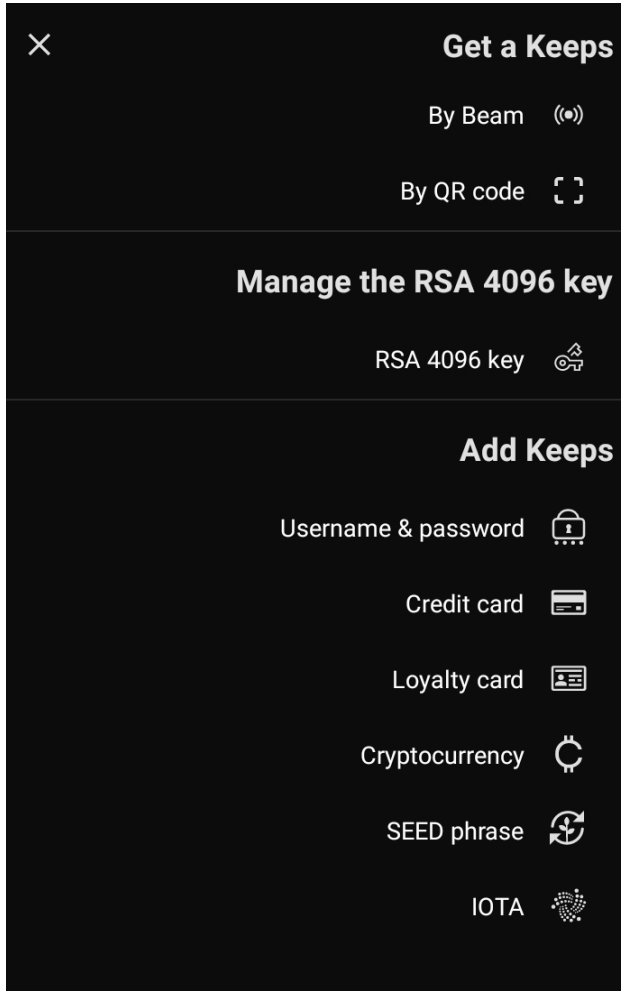
MAIN MENU



A

B

DATA MENU

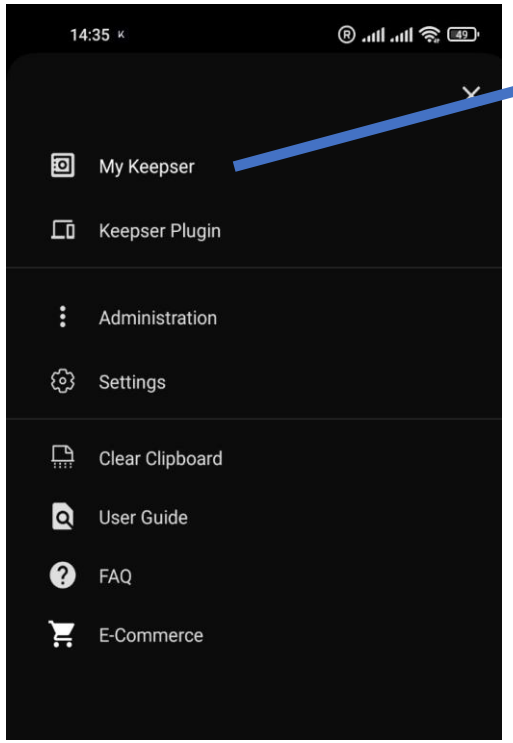


C D E

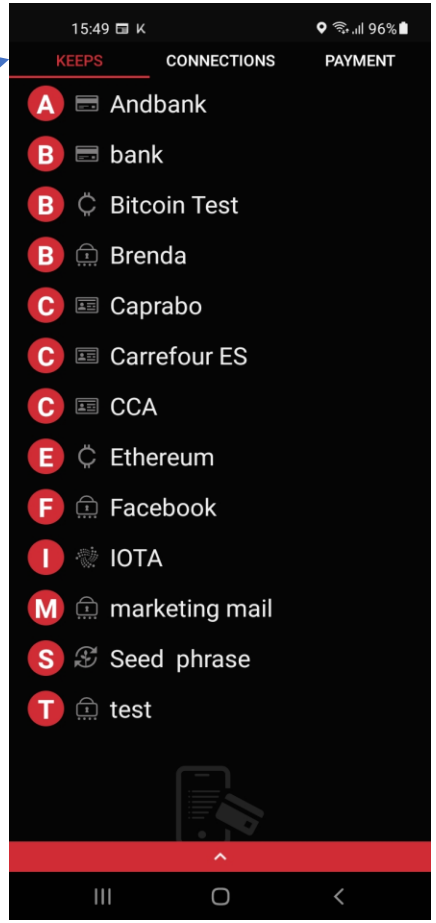
A. Access to the Main Menu
B. Access to the Data Menu
C. Minimize (same as Android phone)
D. Close (same as Android phone)
E. Go back (same as Android phone)

Keepser Application

Main Menu – My Keepser

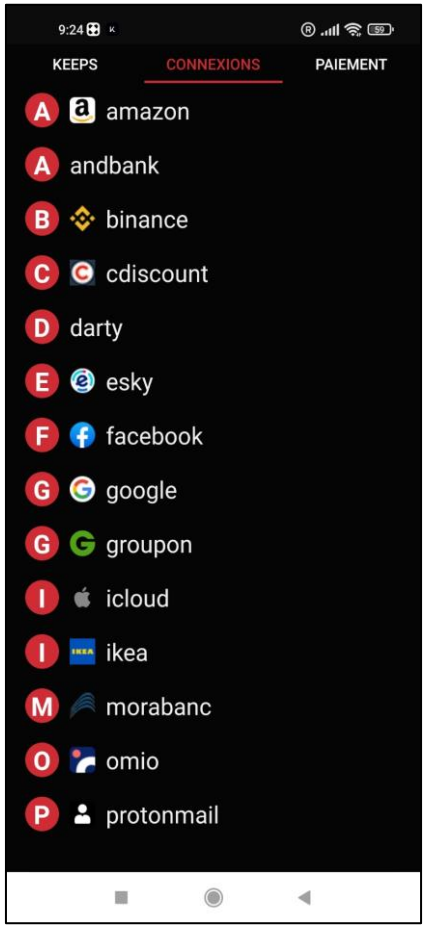


Keeps



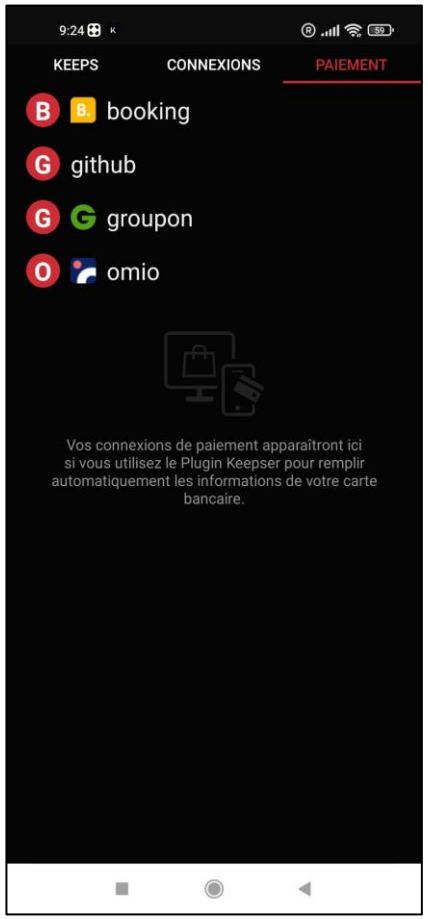
A

Connections



B

Payments

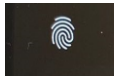


C

A.- See the list of all the Keeps stored in your Keepser Card, with their names sorted by alphabetical order.
B.- The list of the websites you connected to automatically, using the Keepser Plugin
C.- The list of the e-commerce sites where you triggered the payment auto-fill , using the Keepser Plugin

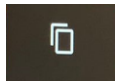
(*) Touch Features

When touching a specific Keeps for more than 2 seconds, you will see 4 icons appear:



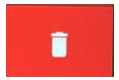
Fingerprint Icon:
If you have added a password (additional security) and set the fingerprint feature (see next page for details), instead of typing the password, you can access to the KEEPS information by using your fingerprint.

(*) Very important: to enable the fingerprint icon/feature in the Keeper App, first of all, you will need to set up and allow the fingerprint feature of your phone (go to your phone´s settings).

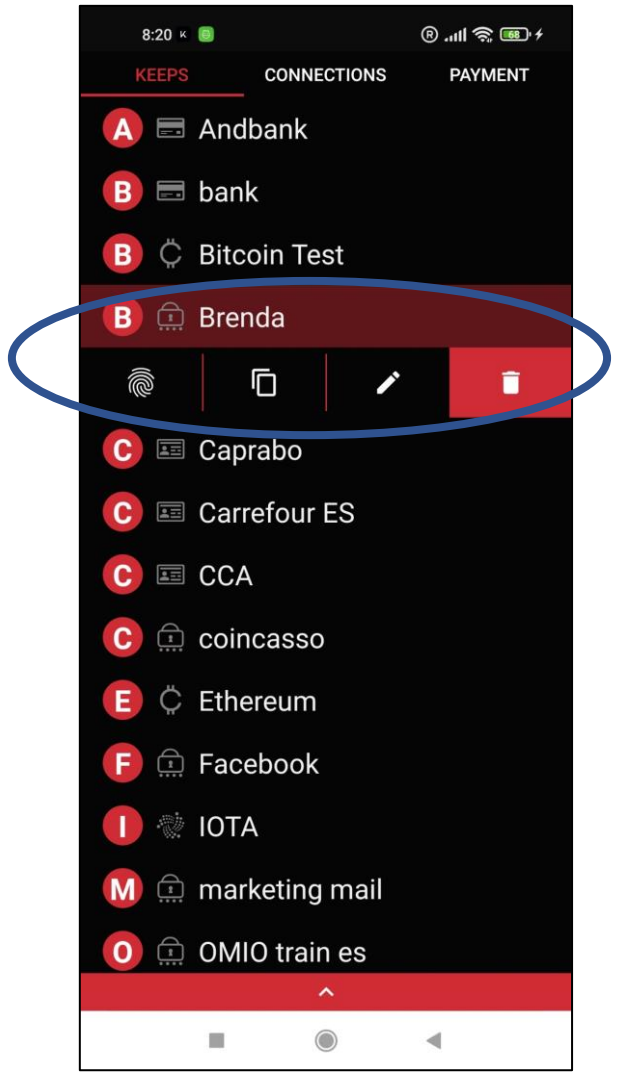


Copy Icon:
This allows you to copy a KEEPS and paste it to another Keepser Card that is connected to this phone.

Edit Icon:
Create a new KEEPS without deleting the original one, and allow you to edit the new one, including adding more or different trust criteria. This is the method to be used when you wish to add trust criteria after a KEEPS has been connected.



Trash Icon:
Allows you to delete the selected KEEPS



(*) Touch Features.

Fingerprint Icon

How to setup the fingerprint icon in your Keepser App.

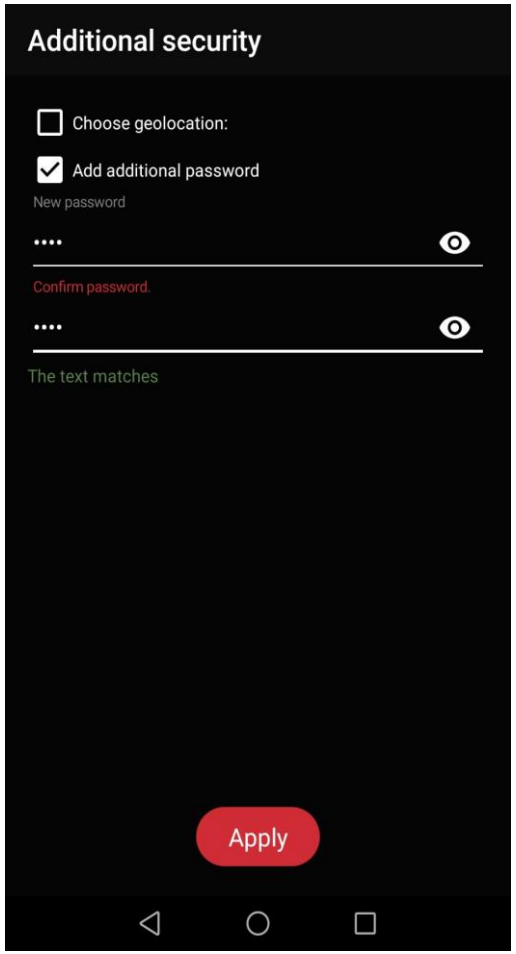
(*) *Important: this is requiring you previously set up the fingerprint recognition on your phone.*

First Step:

When you enter the information to “Add a Keeps”, you have to click on the “Additional Security” button.

This will bring you to the “Additional security” page.

Toggle the switch on top of the page, to “Customized”

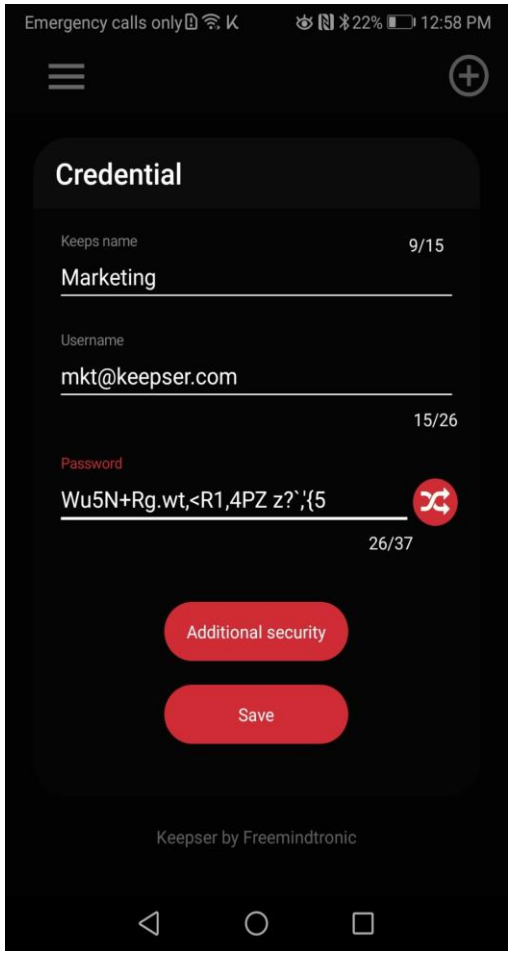


Second Step:

When shown the pages on the right, select the option "Add additional password“.

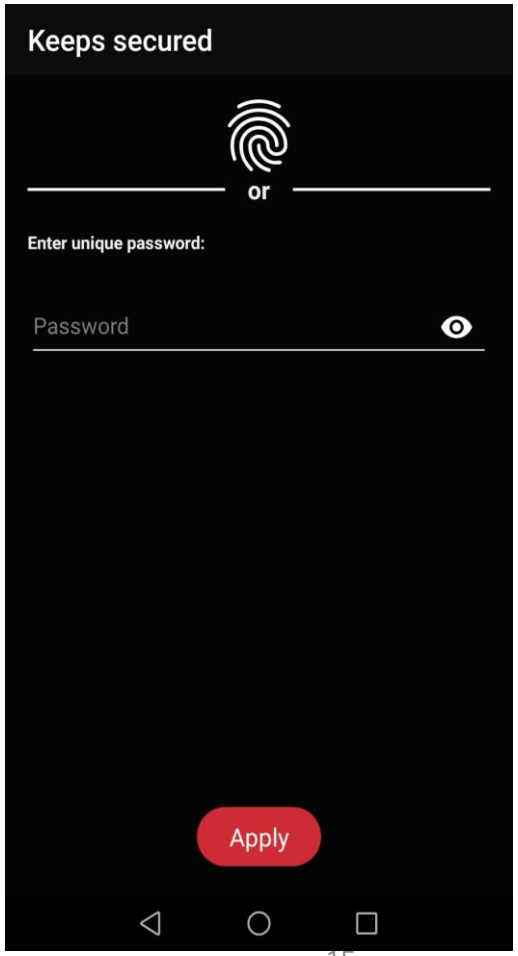
Write a password and validate by clicking on the “Apply” button.

Now the setup is complete.

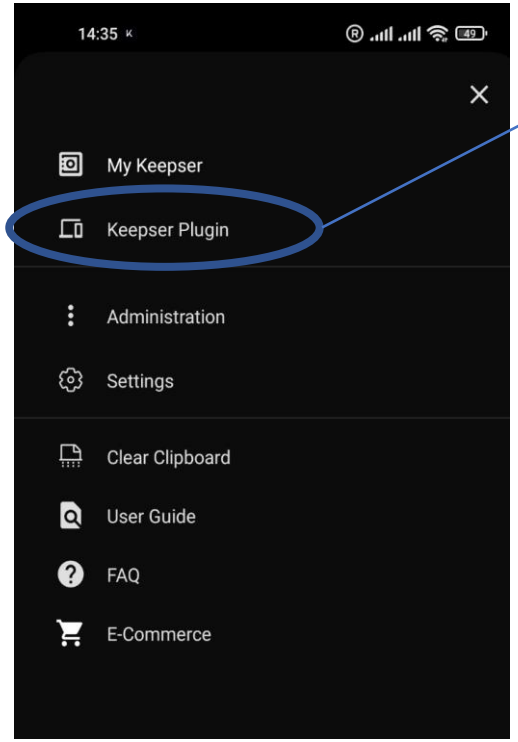


Third Step:

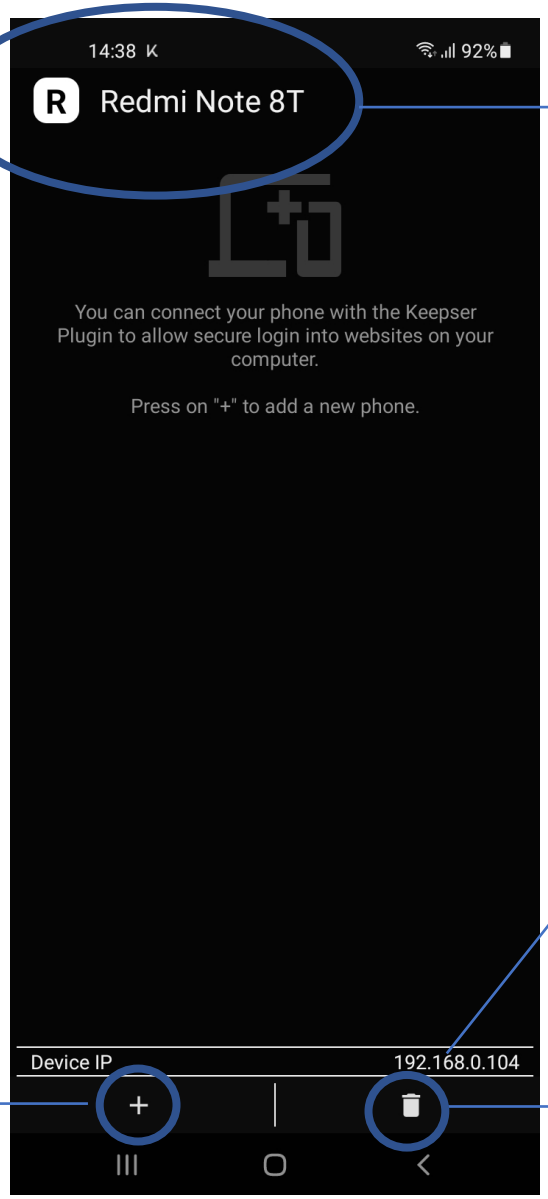
When you want to read the information of a KEEPS, in the “My Keepser” page, the App will now ask either for the password or the fingerprint (if you have set it up on your phone).



Keepser Application



Keepser Plugin page.
Allows you to link this phone in a Keepser Plugin.

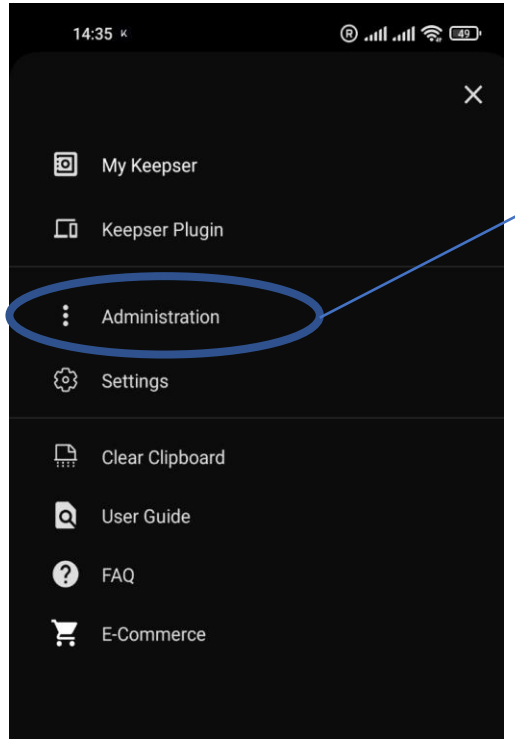


Name of your phone called “connection key” in this user guide.
This name can be edited as you wish (see “User Settings – Plugin” section) . A long pressure on the name of this phone will show a trash icon, allowing you to delete this phone from the Plugin registration.

Device IP
This shows the IP address of your phone.

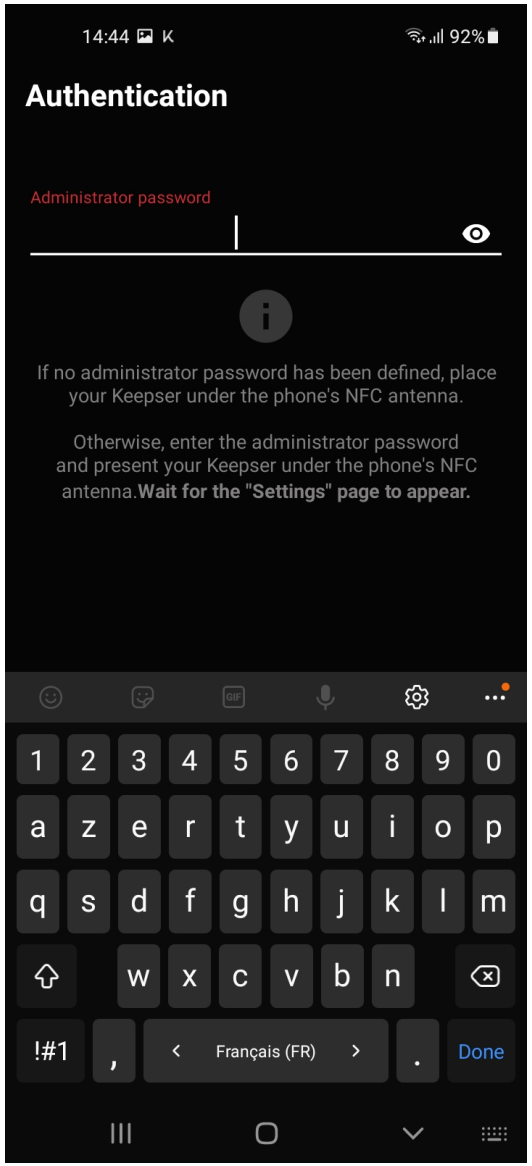
Click on the “trash icon” to delete all stored “connection keys” from the Keepser Card.

Click on the “+” sign to add this phone to the Plugin:
This will open the camera to scan the QR Code generated by the Keepser Plugin and displayed on your computer (see details in the Plugin section)



Setting an administrator password is not mandatory for using the Keepser Cold Wallet solution.

The Administrator can be different from the User and can hide the Keepser from the user.

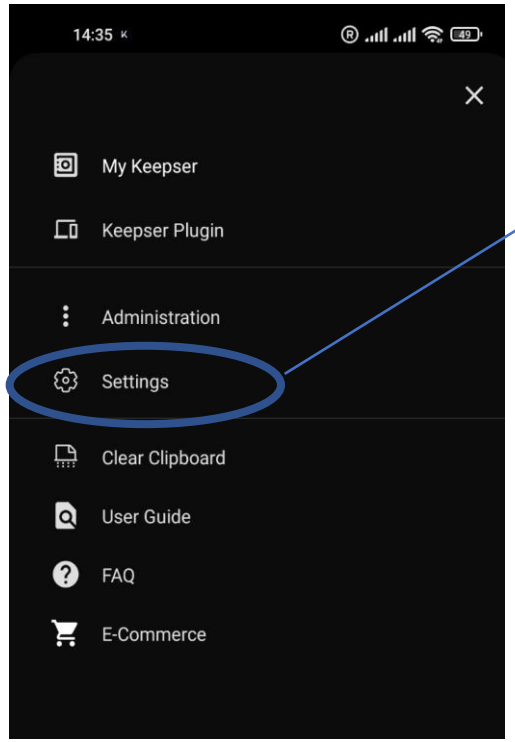


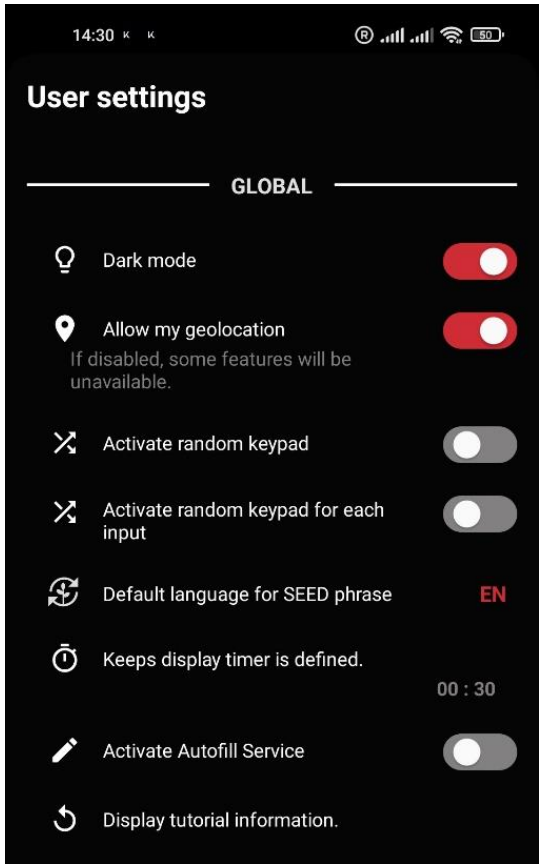
WARNING:
ONLY YOU KNOW THE ADMINISTRATOR password. MAKE SURE YOU REMEMBER IT OR HAVE A WAY TO RETRIEVE IT.

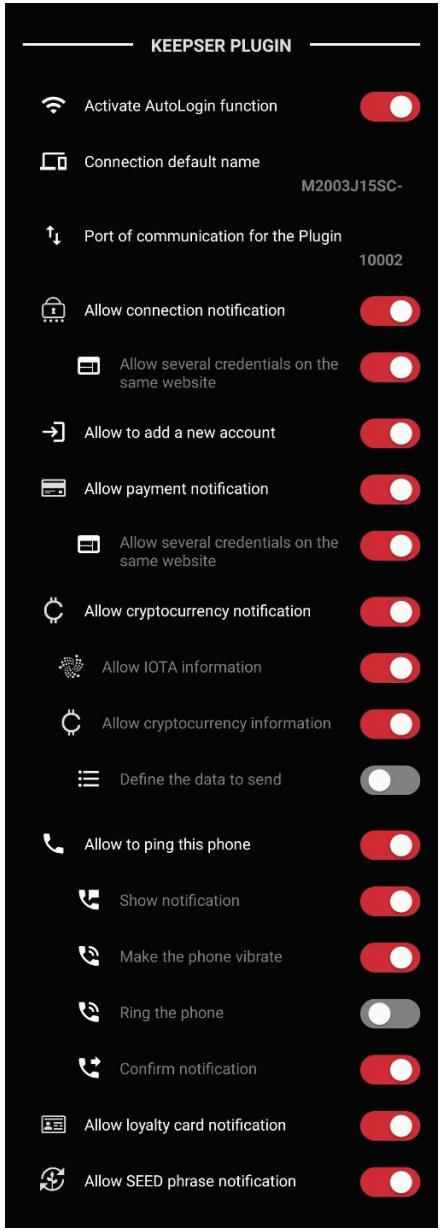
The Administrator password allows you to access the Administrator parameters and manage the different functions. It also allows to unlock some preset parameters in the User Setting menu.

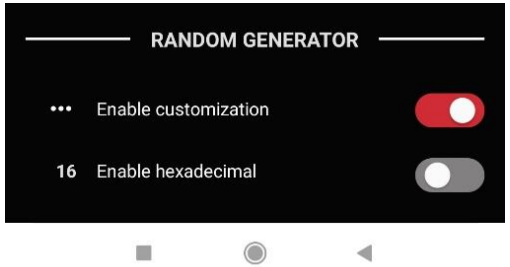
You can enter a password between 1 and 16 characters. The number of attempts to enter the Administrator password is set at 3.
After 3 failed attempts, for security reasons, the Keepser App will ask you to scan the “MY CARD” QR Code to connect again the Keepser card

You can then continue to use the Keepser Card, without accessing the Administration menu, until you enter the proposer Administrator password.









User Settings:
In this section, user will find different actions to configure the Keepser App and its interaction with the Keepser Card.
Details are provided in the next pages

Keepser Application

Main Menu / Settings / Activate Autofill Service

AUTOFILL SERVICE allows to autofill credentials when you connect to websites using your smartphone

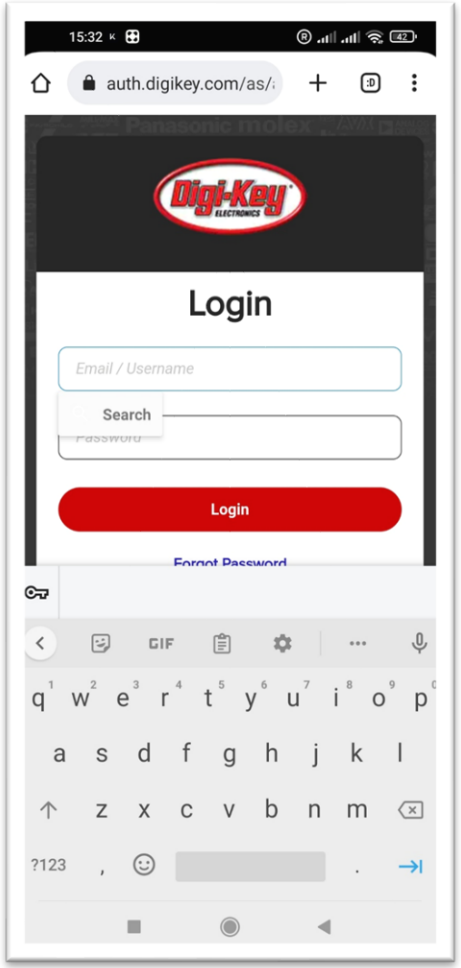
How Autofill Service works for credentials
In the user settings click to activate the Autofill Service

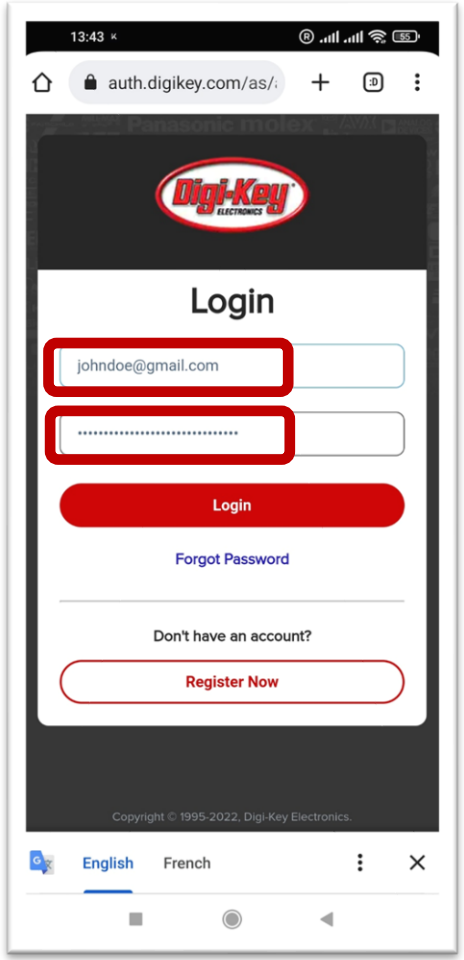
On your phone open a website (here Digikey) and go to the login page.

When clicking in the username field there is a « Search » button which appears. If the button doesn't appear, the website it's not compatible

Click on it a follow the instructions.
The username and password will automatically be autofilled.

This function doesn't work on all websites. Sometimes it is available for the password ONLY.





Keepser Application

Main Menu / Settings / Activate Autofill Service

AUTOFILL SERVICE allows to autofill crypto public address when you connect to websites using your smartphone

How Autofill Service works for crypto
In the user settings click to activate the Autofill Service.

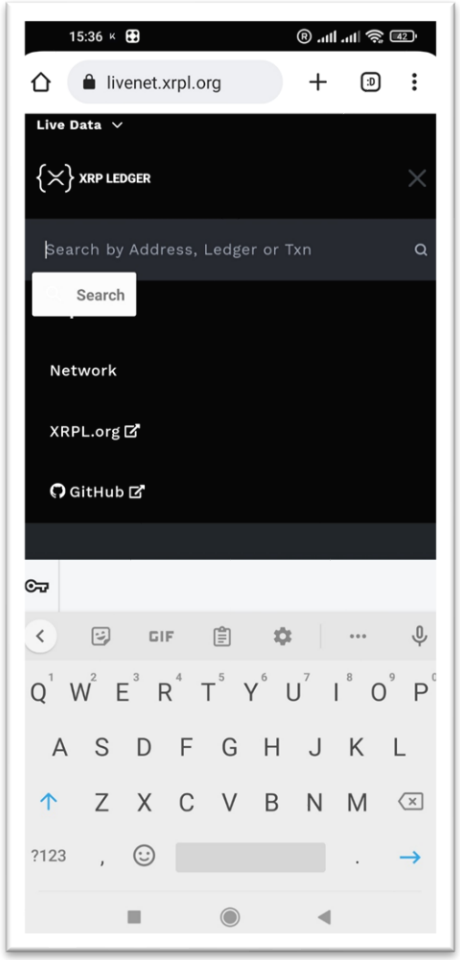
On your phone open a website (here Digikeylivenet.xrpl) and go to the field to search by address

When clicking in the field there is a « Search » button which appears. If the button doesn't appear, the website it's not compatible.

Click on it an follow the instructions.

The public address will automatically be autofilled.

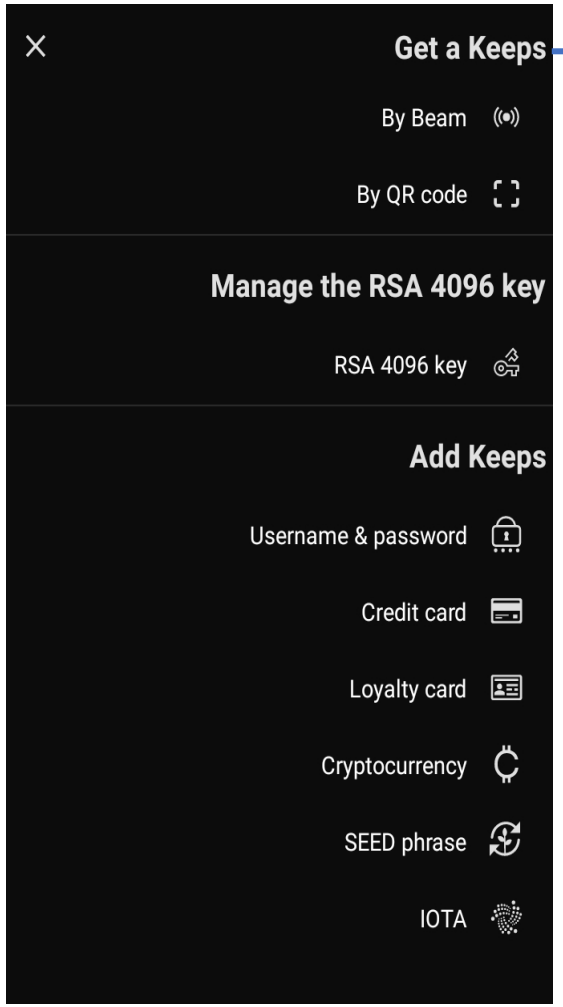
This function doesn't work on all cryptocurrency websites.



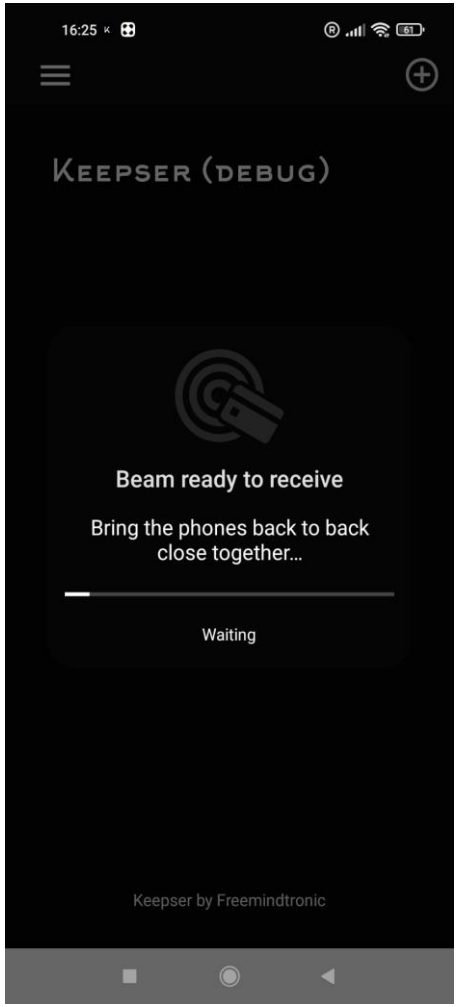
DATA MENU

Keepser Application

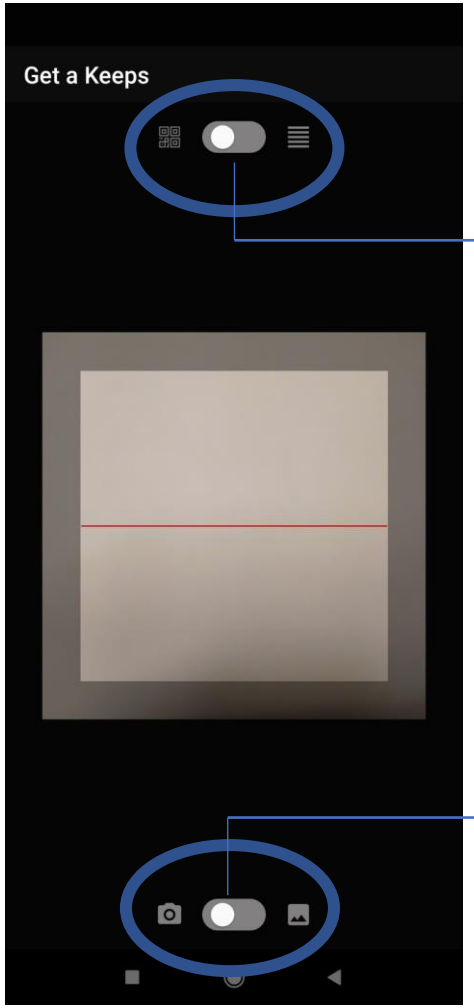
Data Menu / Get a Keeps / By Beam / By QR Code



1. By Beam



2. By QR Code

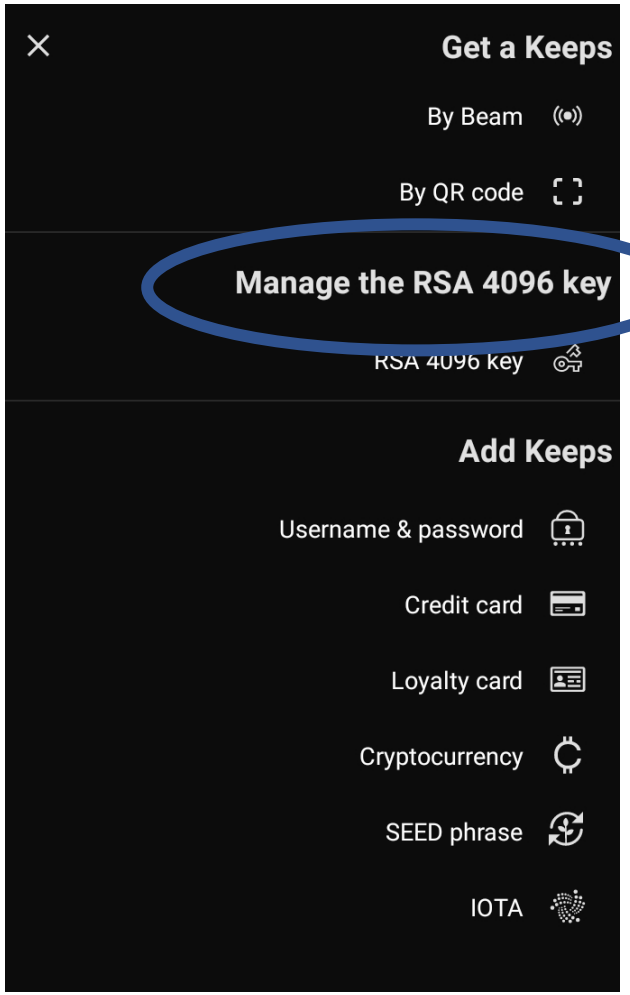


This switch allows to toggle between getting a Keeps via a QR code The Keeps you received was encrypted with your RSA public key
First copy the string of characters the 3rd party sent you and click on the lines icon. Automatically the characters are copied. Place your Keepser card under the phone to store the Keeps.

This switch allows to toggle between “Scan QR code” or get a QR Code from the phone photo gallery.

1.- By Beam: Exchange Keeps putting two NFC phones back-to-back. See the specific tutorial for this feature.
2.- By QR Code: This opens the camera or the photo gallery to scan the QR Code of a Keeps, generated from another Keepser card.

Data Menu – Manage the RSA 4096 key - RSA 4096 key



The RSA 4096 key is an asymmetric key = private key and public key.

Click on RSA 4096 key: you can either generate (or generate again) a new RSA 4096 key or load (generate) the corresponding public key from your existing RSA 4096 private key.

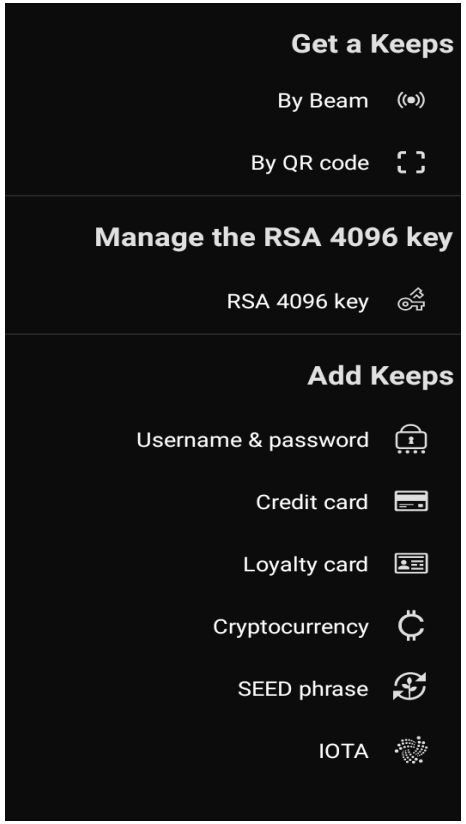
The corresponding QR Code is displayed and can be shared. (see slide 20)

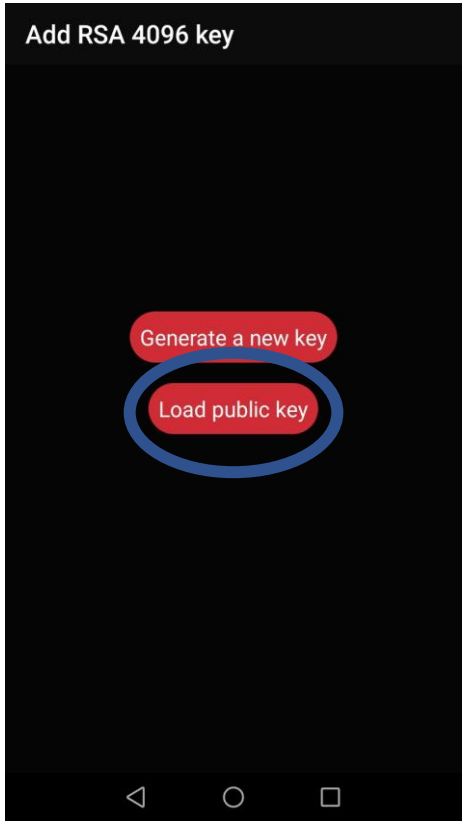
It's always and ONLY the public key which is displayed. NEVER the private key.

WARNING – if you create a new RSA key, the previous one will be erased, and all data cyphered with the previous key will not be abled to be deciphered.

Data Menu – Manage the RSA 4096 key - RSA 4096 key (1/3)

- This generates the Public RSA 4096 Key from the RSA 4096 Private key stored in the Keepser Card, in QR Code format.
- This QR Code can then be stored on your phone for further use or shared via various medias.





Generate the Public Key from the Private Key stored into the Keepser Card.

The public key is displayed, you can share it.

Click on one of these icons to send the RSA 4096 public key via various channels (email, SMS, Whatsapp,….)

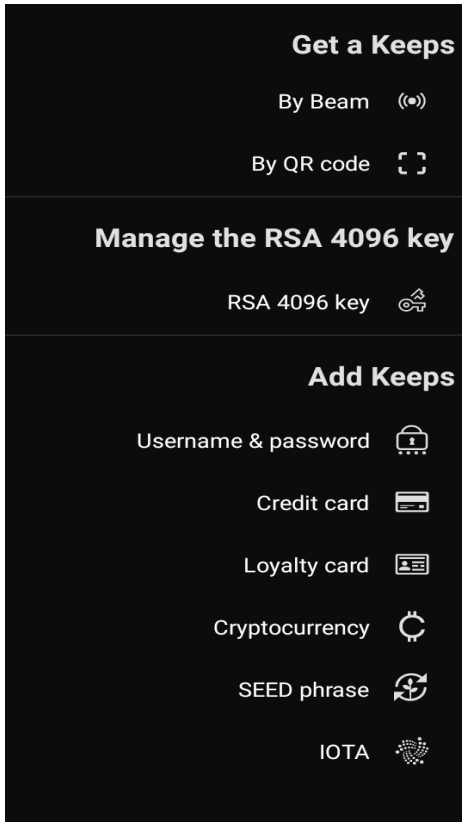
If you click on the « share » icon, you will send the Qrcode and the character string of the public key

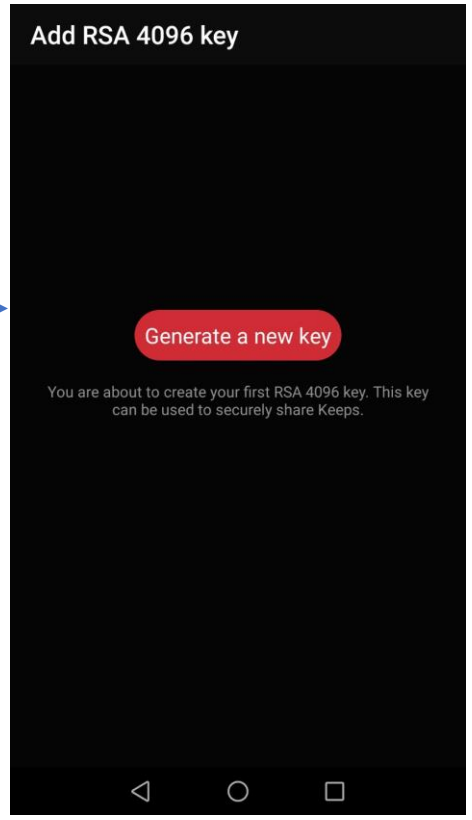
If you click on the « picture » icon, you will send only the Qrcode of the public key

Keepser Application

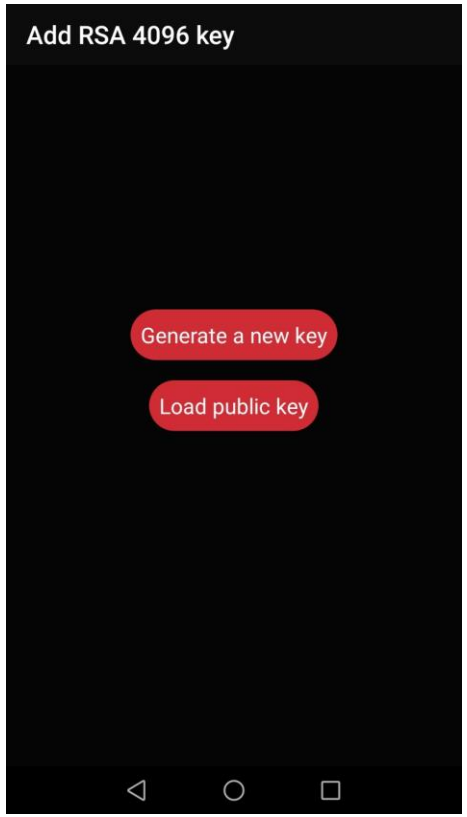
Data Menu – Manage the RSA 4096 key - RSA 4096 key (2/3)

- Generate a New Key: This generates a new RSA 4096 key. The private key is stored on your card
- This QR Code can then be stored on your phone for further use or shared via various medias.

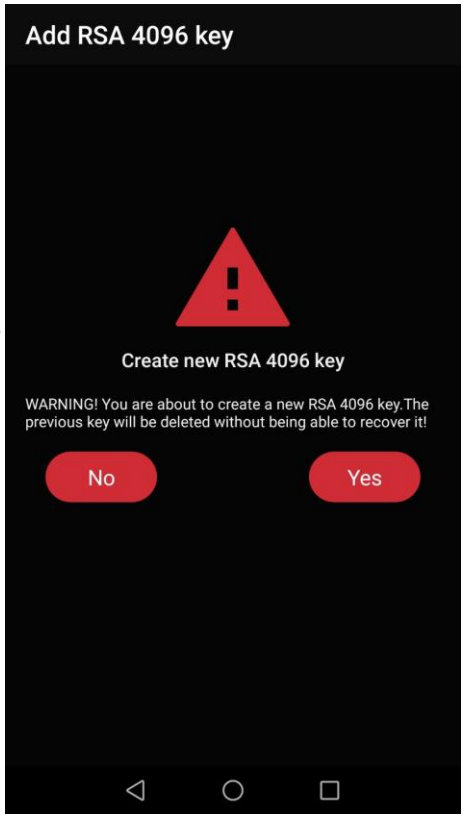




Generate New RSA Key the first time



Generate New RSA Key (Displayed if a RSA Key has been generated before)



Read carefully the message before to click on YES

The public key is displayed, you can share it.

Data Menu – Manage the RSA 4096 key - RSA 4096 key (3/3)

How to share the RSA 4096 public key.

Click on the share icon, you will send the QRcode and the alphanumerical code/string of the public key.

Click on the picture icon, you will send only the QRcode of the public key.

Keepser Application

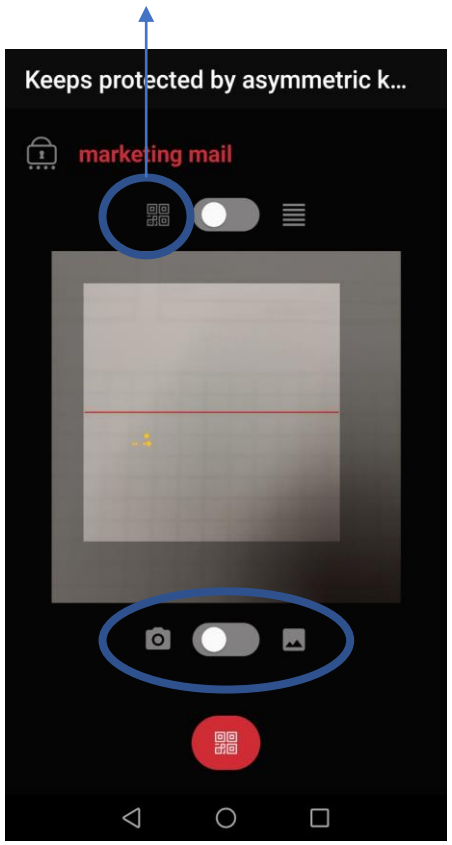
How to securely share a Keeps with a 3rd party using RSA encryption

- Main menu – My Keepser
- Click on the Keeps you want to share and display its information
- Click on the « QR Code button » - This generates the QR Code of the Keeps and brings you to the following page

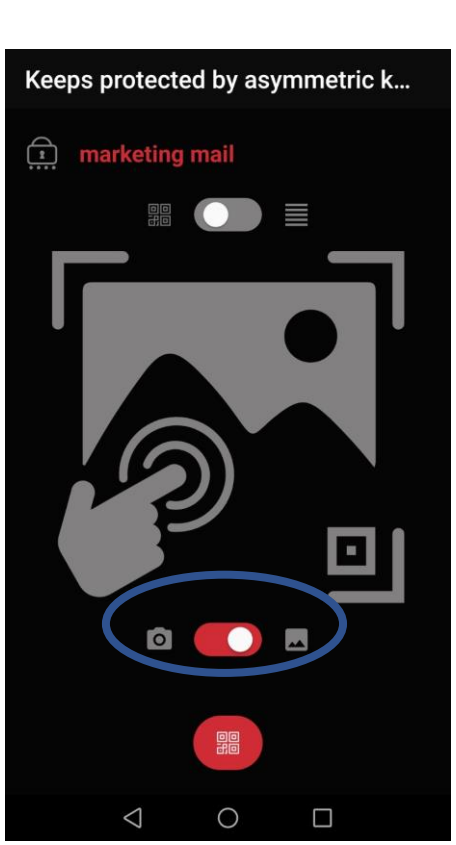
Name of the Keeps.

Clicking on the « Key » symbol will allow to start the RSA secure transmission protocol.

The 3rd party RSA key Is a QR Code

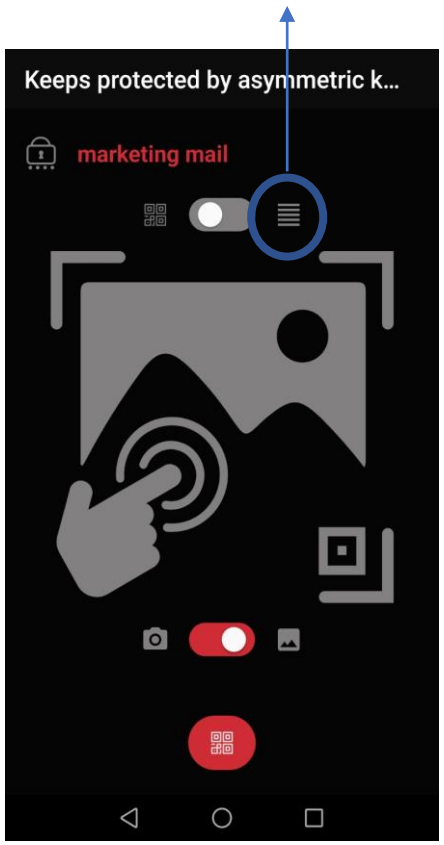


Picture icon opens the scanner. You should scan the QR Code of the public RSA key provided by a 3rd party.

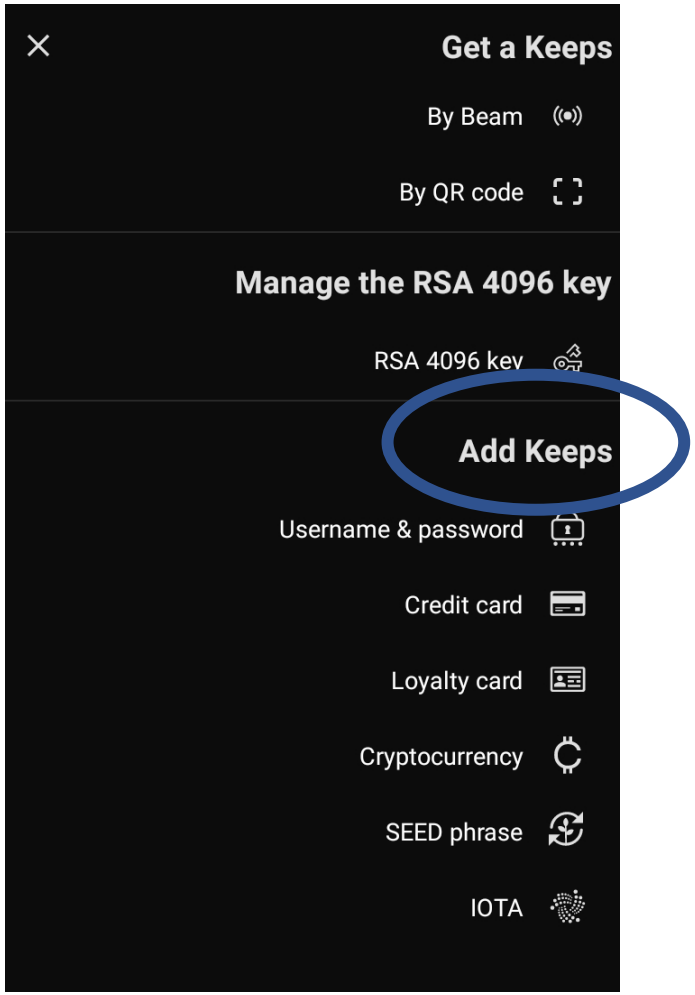


Galery icon allows you to access the QR Code of a 3rd party RSA public key you have stored on your phone.

Use this icon if the 3rd party RSA key is a text string. See slide 18



In case the 3rd party is sending you its RSA public key in the form of a string of characters (via email, SMS or other), you have first to copy them and click on the lines icon.



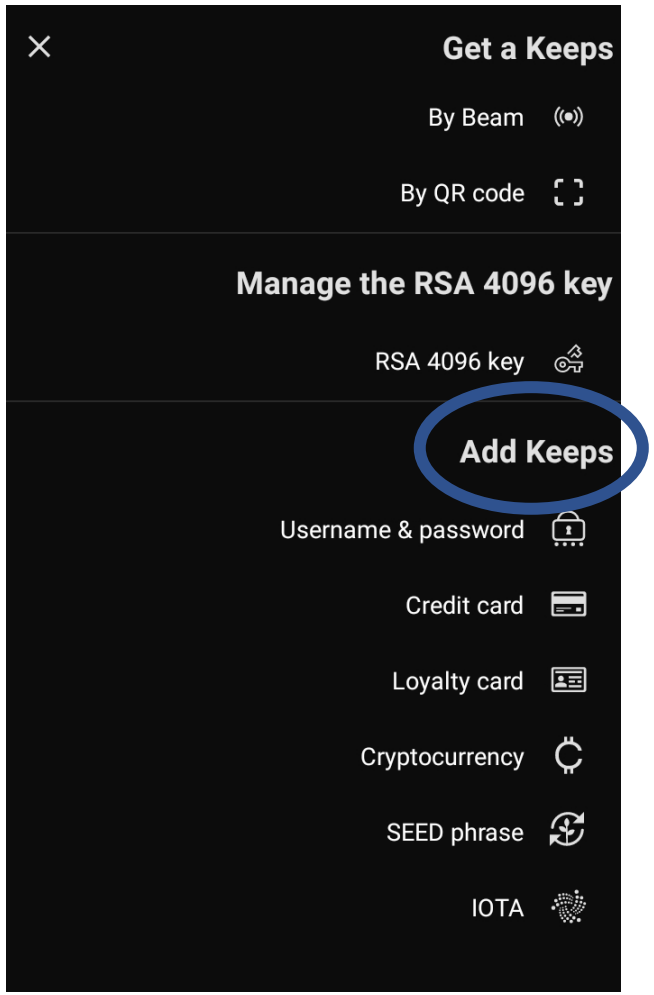
In this section you will be able to enter and securely save the Keeps information into your Keepser Card for various types of Keeps:

- User & password (credentials) for web accounts
- Loyalty cards for account connection & rewards
- Credit cards for e-commerce payment
- Cryptocurrency key and wallet keys
- SEED phrase
- IOTA Token information

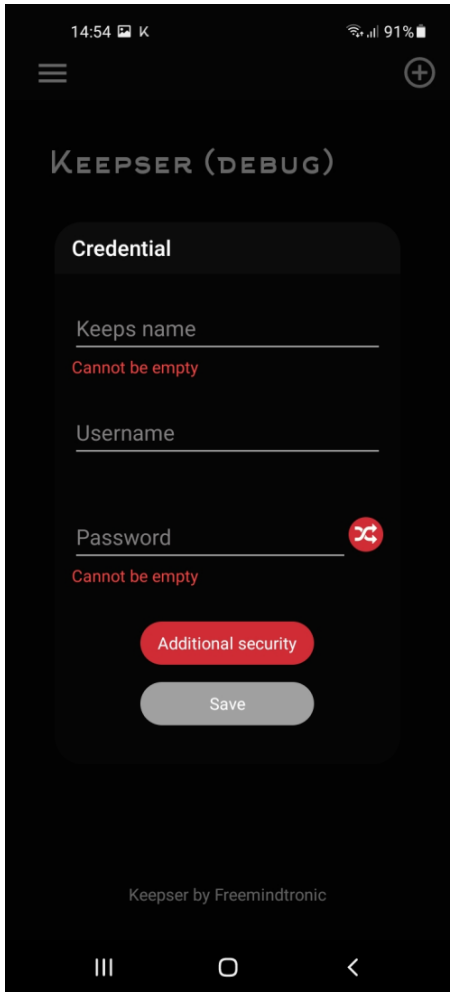
You can add various trust criteria and conditions of access for each of the Keeps.

Keepser Application

Data Menu / Add Keeps – username & password / loyalty card / credit card

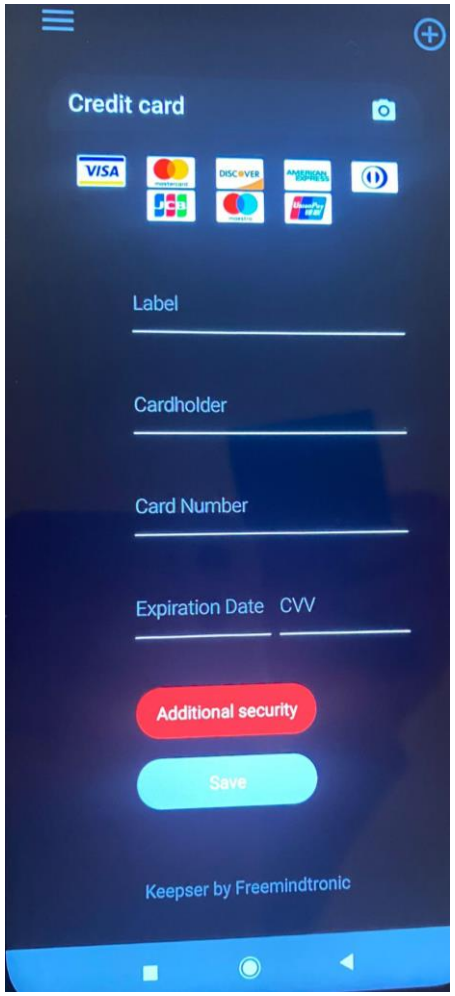


Username & password



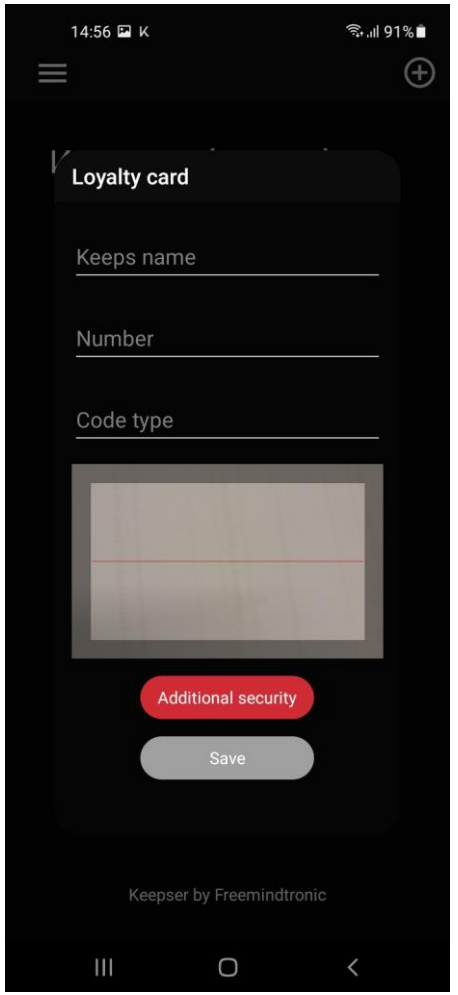
Enter user name (Identifier) and password for access to a web account or an application

Credit Card



Enter credit card information to be used for e-commerce.

Loyalty Card

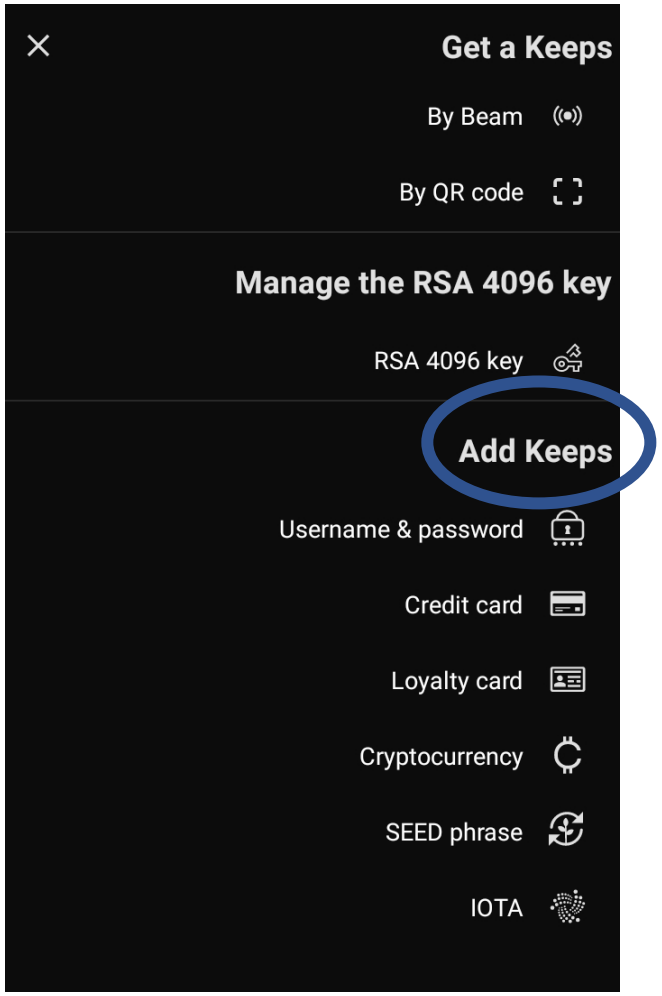


Scan the bar code of the card.

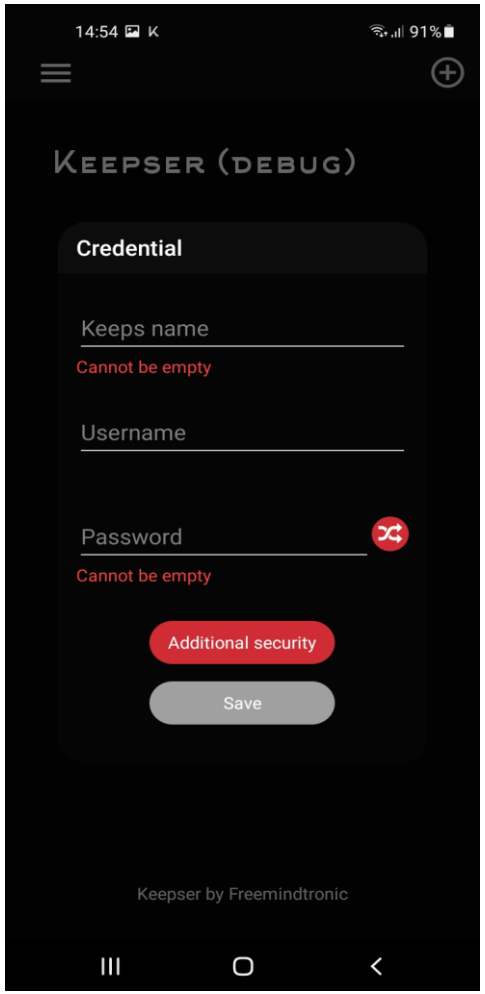
Keepser Application

Data Menu / Add Keeps / Username & password / Additional security

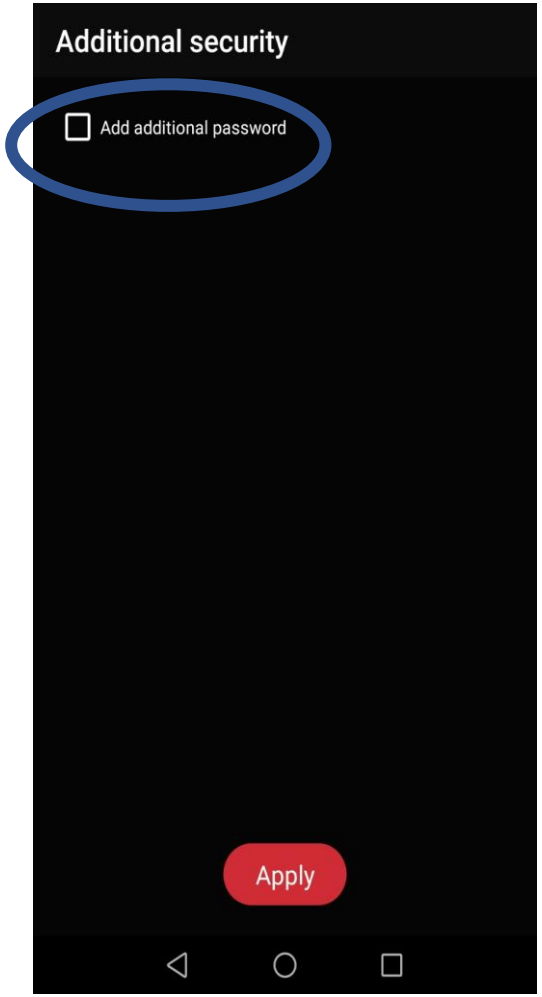
An example to add additional security for Keepser PRO when entering a new username & password Keeps.



Username & password



Keepser PRO



KEEPSER PLUGIN

About the main Keepser Plugin window (1/6)

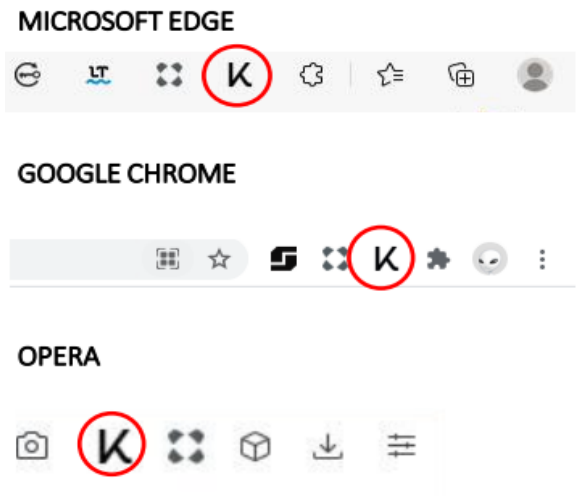
How to set up the Keepser Plugin in your computer.

1.- Download and install.

Download Keepser Plugin then install it.

- MICROSOFT EDGE : microsoftedge.microsoft.com/addons
- CHROME : chrome web store
- OPERA : addons.opera.com
- FIREFOX : addons.mozilla.org

Once the App is installed, the Keepser icon appears at the top right of your browser window, on the right of the address bar.



Important: For the Keepser Plugin and the Keepser App to work properly, YOUR COMPUTER AND YOUR SMARTPHONE MUST BE CONNECTED TO THE SAME WIFI NETWORK.

In the Keepser App “User Settings – Global”, YOU MUST TURN-ON THE “Activate Autologin function” switch.

Easy access to Keepser tutorials and e-commerce site :

After installing the Keepser Plugin in a browser, if you open the browser and click on the Keepser Plugin icon without entering a website URL, you will be sent to a page where you can directly access the tutorials for the Keepser Cold Wallet (Keepser Cold Wallet) solution, and access the Keepser e-commerce web-site.

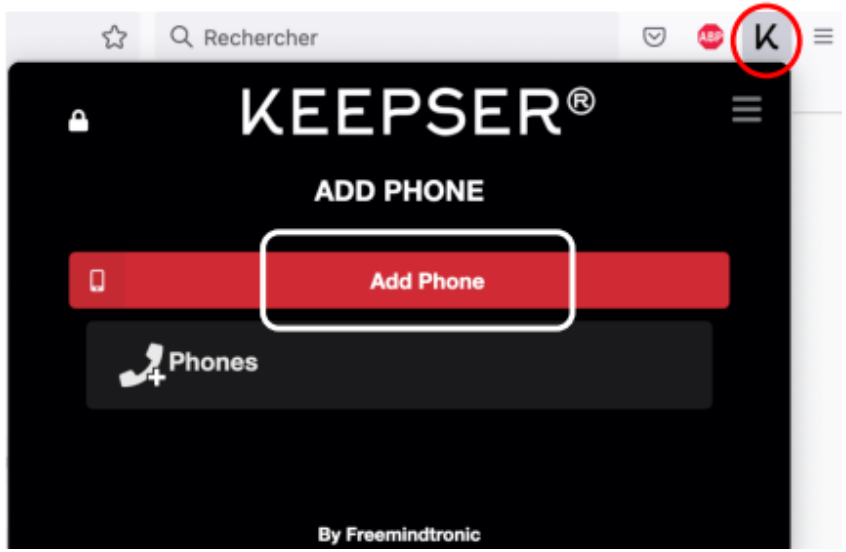
About the main Keepser Plugin window (2/6)

How to connect a phone in the Keepser Plugin.

Turn on your computer and open a browser for which you have installed the Keepser PlugIn onto.

Click on the KEEPSER Plugin icon.

When you use the Keepser Plugin for the first time, the window below opens and suggests you “add a phone.”
You can add (connect) a large number of phones.

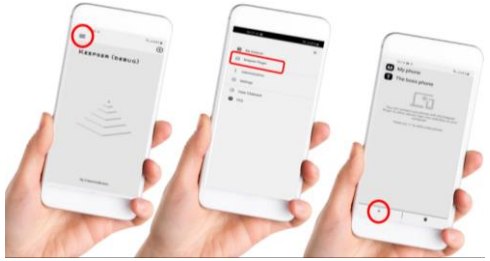


How to connect (add) a phone :

1 – Open your browser and click on the Keepser Plugin icon. Get to the “Add phone” page (automatic for the first phone; through the menu for additional phones).

2. Open the Keepser Application on your phone and click on the icon at the top left of the screen (to open Main menu)

3. Then press on “Keepser Plugin”.



4. Click on the icon “+” at the bottom of the page – This will open the QR Code scanner.

5 - Click on “Add a phone" button in the Keepser Plugin window .
This will generate a QR Code displayed on your computer.

6 – Scan the QR Code with your smartphone. A 4-digit verification code will then display. If the same message is read on you Keepser Plugin, you will be able to add the phone.

Note that you may want first to change the name of your phone. To do so, please refer to the “User Settings – Plugin section” of this manual

About the main Keepser Plugin window (3/6)

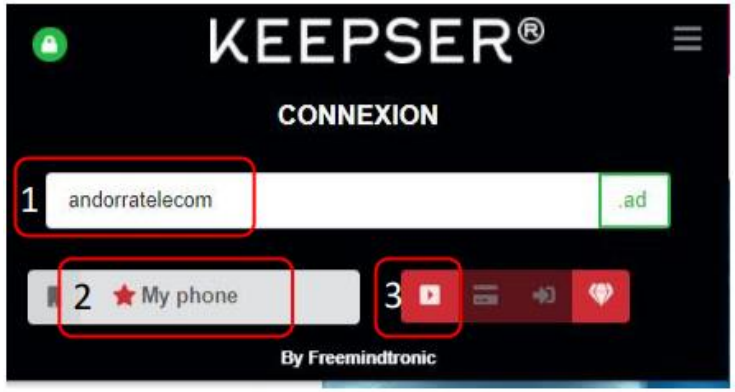
Using the Keepser Plugin for secure automatic website account connection:

1. Open your browser and connect to a web site on which you want to login. Then click on the icon of the Keepser Plugin .

- A window opens, and the URL of the website you connect to is displayed
- Select the phone you want to use for the automatic connection (where your Keepser Card is connect ed onto, and your Keepser Card contains the username (ID) and password to access your account on this web site).
- Click on the Red “Play” (connection) button.

A Notification is sent to the phone (you have to have authorized the notifications from the Keepser Plugin (see User Settings)
You must click on the notification and follow the displayed instructions, asking you to pair your Keepser Card.

You will then be automatically be logged in with your username (ID) and password retrieved and securely transmitted from the Keepser Card.

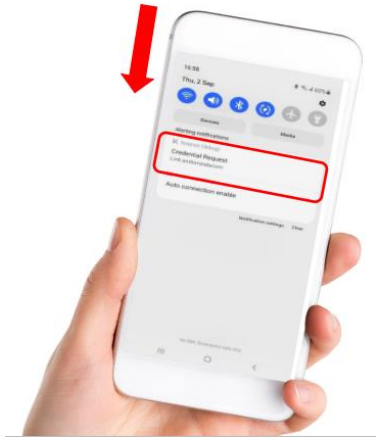


Information about automatic secure web connection

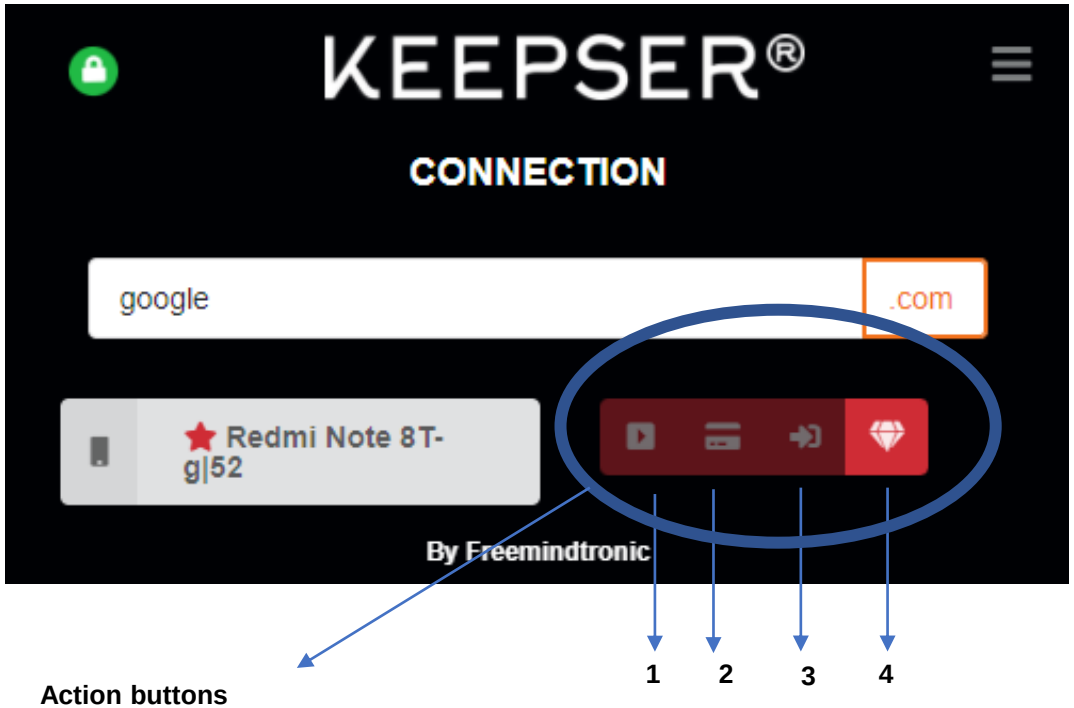
When connecting to a website for the first time, you must associate the username stored in the card that corresponds to the site.
During subsequent visits to this same site, the connection will be automatic, the username having already been associated.
It is possible to associate several usernames on the same site (example: professional and personal account). Click on the "+" icon to add a new username.
If you have added several usernames, click on the icon to open the list of usernames already associated with this site and choose one.

Note: Disapearing notification:

After 6 seconds, or if you touch the smartphone screen, the notification received from the Keepser Plugin may disappear.
Like any other notification received by your phone, you can see it by scrolling down your finger from the top of the screen.
You can then click on the notification



About the main Keepser Plugin window (4/6)

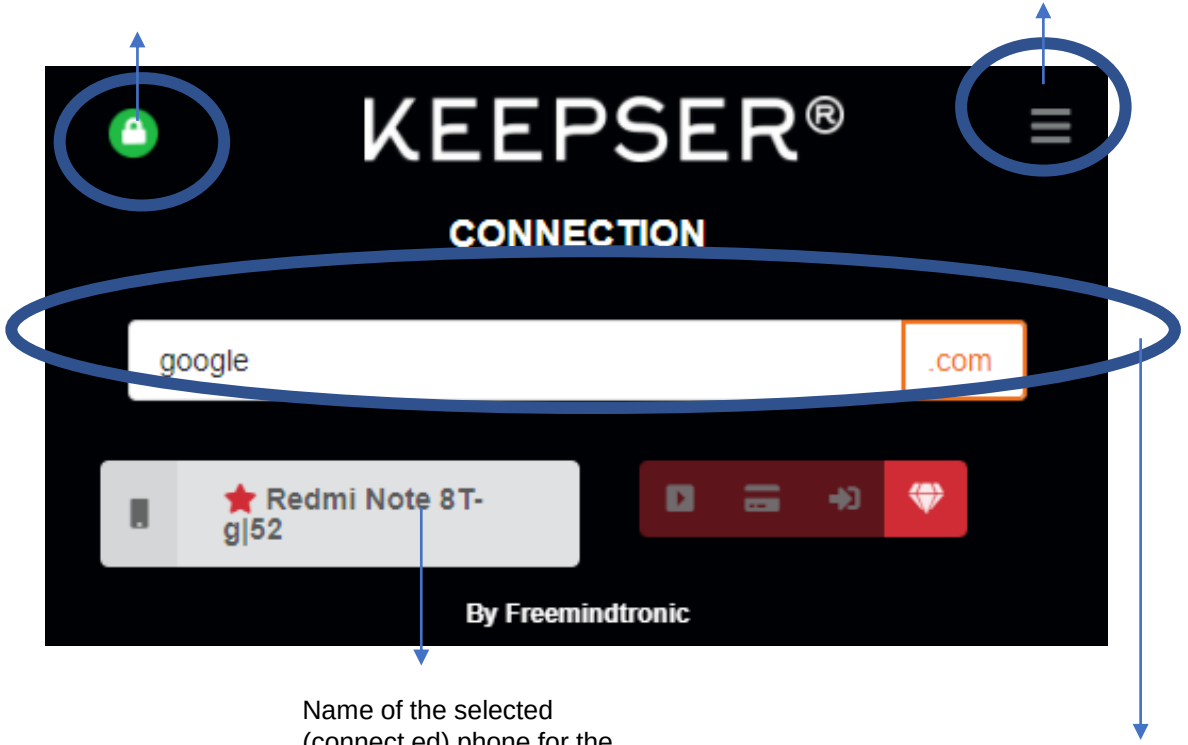


Action buttons

1. “Play” (connection) button: to securely autologin to you account on a website, with the Keeps stored in your Keepser Card.
2. “Credit Card” button : to autofill the credit card information on a e-commerce payment page, with the Keeps stored in your Keepser Card
3. “Right Arrow” button: to create a new account in a website.
4. “Diamond” button: to securely autofill cryptocurrency public address with the Keeps stored in your Keepser Card.

Green lock = https (encrypted connexion)
Red lock = http (non-encrypted connexion)

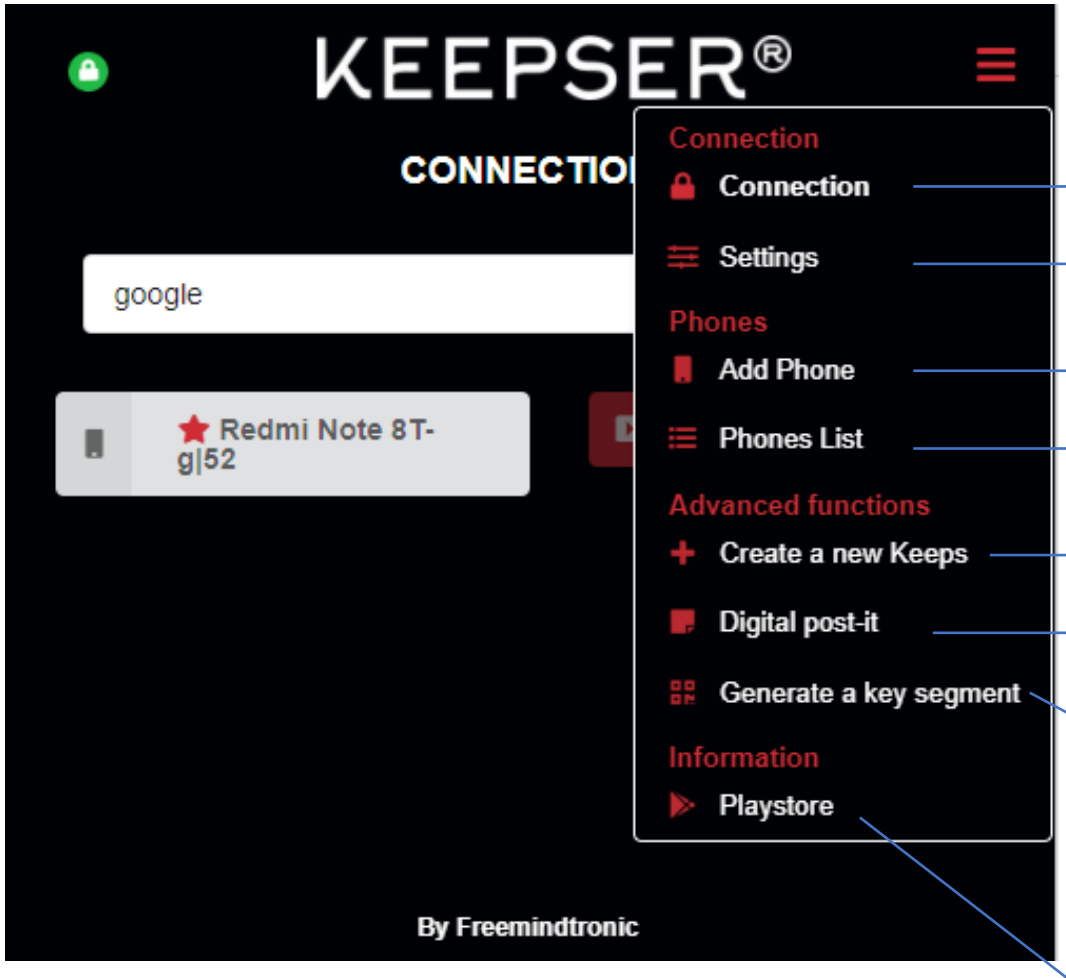
Keepser Plugin Main menu



Name of the selected (connect ed) phone for the action/transaction

Name of the visited web site, automatically detected by the Keepser Plugin.

About the main Keepser Plugin window (5/6)



Open the « Connection » window

Access a suite of options and settings (see next pages for details)

Open the « Add Phone » window (you can add as many phones as you want)

Access and edit the list of connect ed phones (see next pages for details)

Enter a new Keeps (credit card; SEED phrase and generate a QR Code) to share and save it in your Keepser Card (see next pages for details)

Allows to securely share the information of a Keeps to your computer, so you can copy/paste it and connect manually, in case the automatic connection is not working. (this could happen sometimes on few websites with unusual login or payment page sequences)

Generate a QR code that you can use as a trust criteria for a Keeps. You can also print the QR Code for later use. (only available for PRO+ models)

In the Keepser App: Data menu – Add Keeps – Additional Security – Add QR Code or barcode nearby you

Generates a QR Code that will bring you to the Keepser Application in Google Play Store, where you can download it from, if you did not do it yet.

.

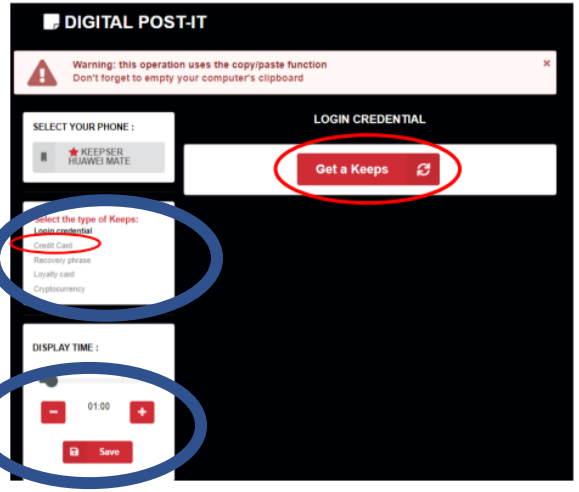
About the main Keepser Plugin window (6/6)

Main menu - Digital Post-it

Use it when autologin to websites or autofill in payment forms is not possible. This could happen sometimes on websites or payment pages with unusual sequences.

Securely display the information of a Keeps from your Keepser Card through the Keepser Plugin, so you can copy/paste it in the various fields to populate.

Cliking on « Digital Post-it » in the Plugin Main menu, will open a new tab in your browser.



1 – Select the type of Keeps you want to display from your Keepser Card

2 – Select the time the Keeps information will remain displayed on your computer (after this time, all information is erased)

3 – Click on the « Get a Keeps" button.

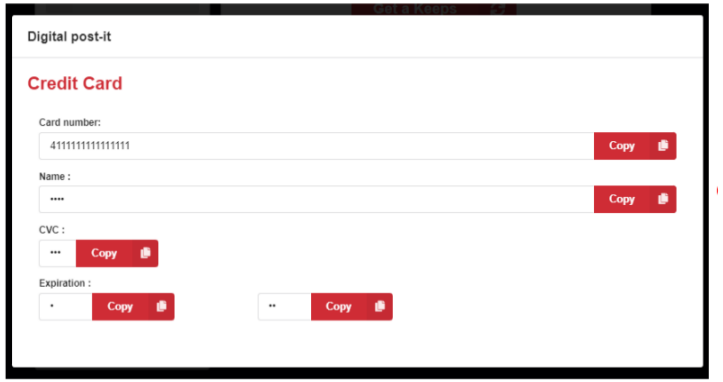
4 - This will send a notification to the selected phone.

5 - Click on the notification received on your phone

The list of all the stored Keeps from the selected Keeps type is displayed.

5 - Select the Keeps you want to display

Digital Post-it with the Keeps information securely retrieved from the Keepser Card



Each piece of information of the Keeps has a « Copy » button besides it.

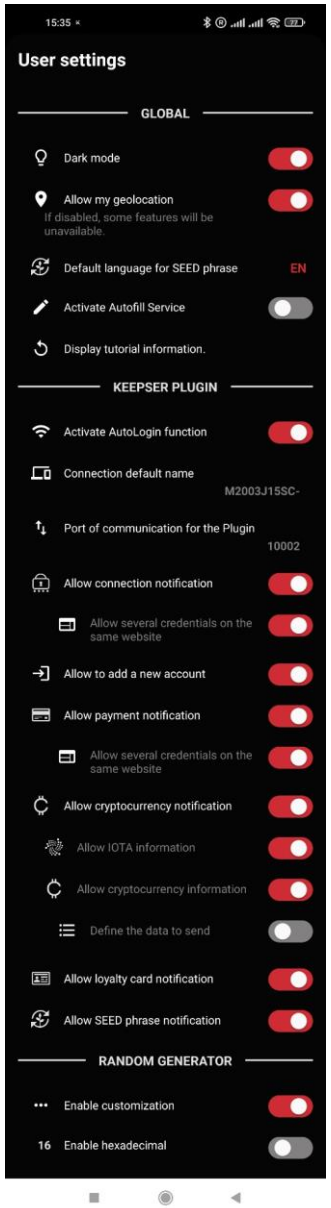
When clicking on a « Copy » button, the content of the corresponding field is copied into the clipboard of your computer. You can then paste it where you need to.

After pasting one piece of information, you can come back to the Keepser Digital Post-it tab, and copy another piece of information. You should repeat this operation until all the pieces of information you need are properly populated to perform the targeted transaction.

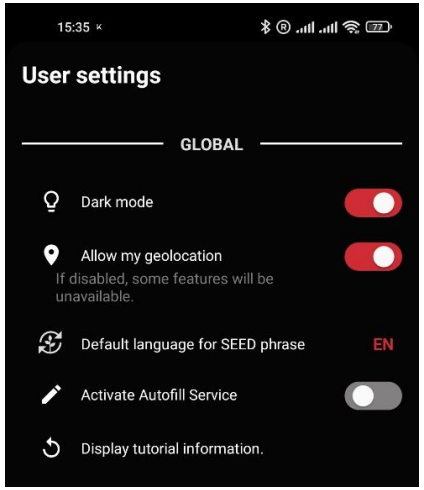
DO NOT FORGET TO ERASE THE CLIPBOARD AFTER THE LAST COPY/PASTE

USER SETTINGS MENU

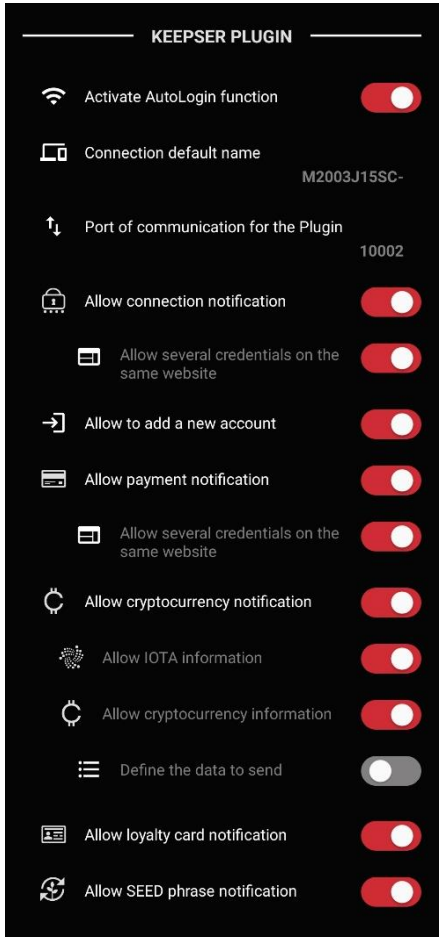
Main Menu – Settings - User settings – Global section (1/2)



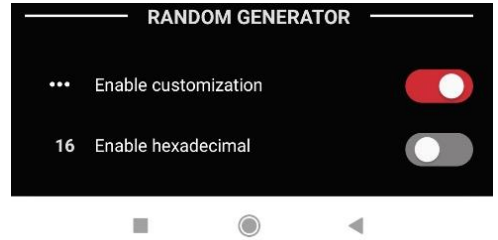
Global settings



Keepser Plugin settings



Random generator



Main Menu – Settings - User settings – Global section (2/2)

The Global section is providing a set of options that the user can choose from the selection is made by toggling a switch, or by touching the grey or red text.

Note that, depending on the Keepser Cold Wallet model, some parameters may be fixed and cannot be changed by the user. Some can be changed by the administrator.

1. **Dark Mode**: Allows you to change the background of the Keepser App pages. Black background with white text is the default setup. It can be changed to a white background with black text.

2. **Allow my geolocation (If disabled some features will be unavailable):** This feature needs to be enabled to allow for the geofencing feature (see "additional security" section, when entering a new Keeps.

3. **Activate random keypad**: Used for the USER PIN.
You can use this function only IF you have defined a User PIN (See administration menu for details). When set, this User Pin is required to view and access the list of Keeps stored in the Keepser Card, and a key pad is displayed.
When the "Activate random keypad" is configured, the numbers of the key pad will be shuffled to add an additional level of security.

4. **Activate random keypad for each input:** Used for the USER PIN.
When activated, this option is reshuffling the key pad numbers, every time the user is entering a number.

5. **Default language for SEED Phrase** – Choose which language you want to use to store the words of the SEED phrase. By touching the language symbol, this opens a list of available languages you can choose from.

6. **Keeps display timer is defined:** This defines the time for which the information of a KEEPS remains displayed on the Keepser App ("My Keeps" page). After this time, the information disappears and the display goes back to the list of KEEPS ("My Keeps" page). The timer is set at 30 seconds by default. When reading & displaying the information of a KEEPS on your smartphone, a circle appears on the right, which is progressively decaying as time goes. When the full circle is gone, the information disappears and is not keeped in the phone for security reasons. Changing this parameter is possible through the administration parameters.

7. AUTOFILL SERVICE allows to autofill credentials when you connect to websites using your smartphone.

8. **Display tutorial information:** you can activate these tutorials. Go and See the slide 7.

Activate Autologin function: Allow the notifications from the Keepser Plugin Autoconnection with your Wi-Fi

1.- Connection default name: This is the name of your phone, that will be used for the registration of your phone in the Keepser Plugin. The default name is the one given by the phone manufacturer, but you can change it. To edit it, you can click on the name, and type a new name of your choice. For security reasons, 4 random characters are automatically added by default to the name you choose. However, you can delete or edit these characters before registration with the Plugin.

2.- Port of communication for the Plugin: indication If you click you can change it

It is possible to change the communication port between your phone and the Wifi network. However, in order for the Keepser App and the Keepser Plugin to properly communicate and interact, both your phone and your computer shall use the same port. **The default port is 10002**.

3**.- Allow connection notification**

This authorizes the Plugin to send notification for the autologin function to your phone. If you turn this off, you will not be able to automatically connect to secure websites.

3.1 **Allow several credentials on the same website**

This switch is authorizing or not for several KEEPS to be used on a web site connection. For example, if you have several accounts on the same website, and you want to be able to select which one to use for login. You can select the account to connect to by default. Not activating this feature will not allow for several accounts on the same website or application.

4.- **Allow to add new account**

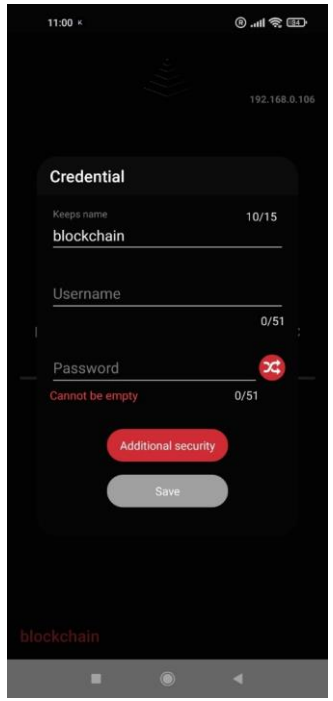
This function allows you to create a new account on a web site, directly from the Keepser App and connect the credentials in the Keepser Card. It requires to click on the “Create new account” button in the Plugin.

5.- Allow payment notification.

This authorizes the Plugin to send notifications for the credit card autofill function to your phone. If you turn this off, you will not be able to automatically perform payment on e-commerce websites.

5.1 Allow several credentials on the same website: This switch is authorizing or not for several KEEPS to be used on an e-commerce payment page. For example, if you have several credit cards and you want to be able to select which one to use for a payment. You can select the credit card Keeps to use by default. Not activating this feature will not allow for several credit cards to be used on the same website or application.

CREATE A NEW ACCOUNT
(with the Keepser Plugin)



When clicking on the « Create new account » button is showing in the Keepser Plugin window, a notification is sent to the phone.

When clicking on the notification, this window opens, the name of the visited website is appearing.

You can then follow the usual procedure to connect a new Keeps.

Main Menu – User settings – Random Generator section (1/4)

1.- Enable customization:

This function enables the user to generate random complex passwords. When this switch is turned ON, a “shuffle” icon is shown when asked to enter a new password in various places in the Keepser Application. See next page for more details.

The complex password is using ASCII characters from the following list:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!"#$%&'()*+,-./:;<=>?@[\]^_{|}~`

2.- Enable Hexadecimal:

This function enables the user to generate random complex passwords using hexadecimal characters. When this switch is turned ON, a “shuffle” icon is shown when asked to enter a new password in various places in the Keepser Application. See next page for more details.

The complex password is using characters from the following list (upper-case or lower-case)

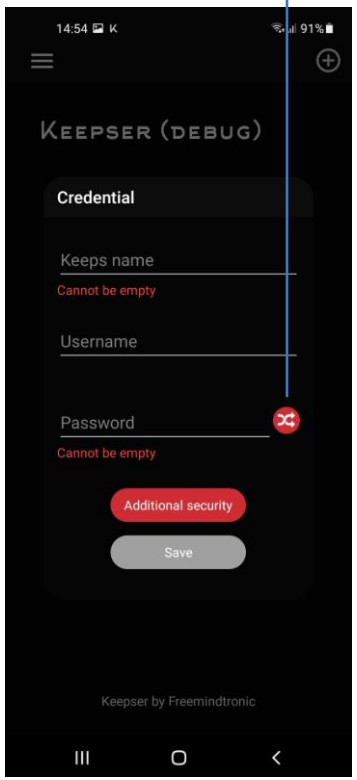
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E et F

Keepser Application

Main Menu – User settings – Random Generator section (2/4)

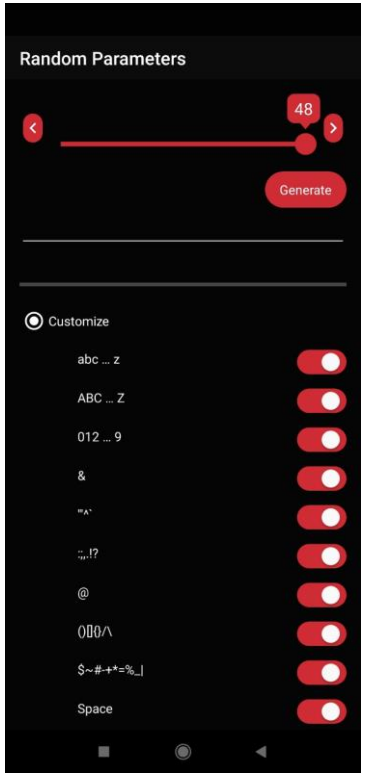
Using and configuring the Random Complex password Generator (ASCII characters).
(When recording a new credential: Data Menu ➔ Add Keeps ➔ User name & password).

Shuffle Icon

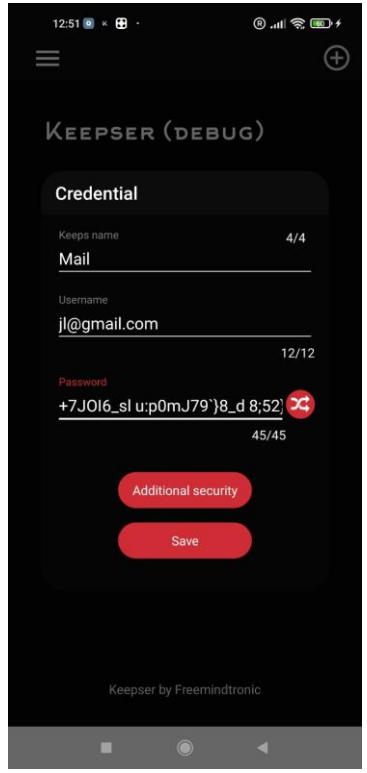


A short click on the « Shuffle » icon automatically generates a complex password (up to 48 characters)

Note: the cummulative total number of characters from the Keeps name, Username and the password fields is 61 characters. Keeps name is limited to 15 characters.



A long click on the « shuffle » icon opens a menu to configure the random generator.
Length of the password can be configured.
The« customize » mode allows to select a subset of the character portfolio.
Click on « Generate » to generate the password and verify the configuration.



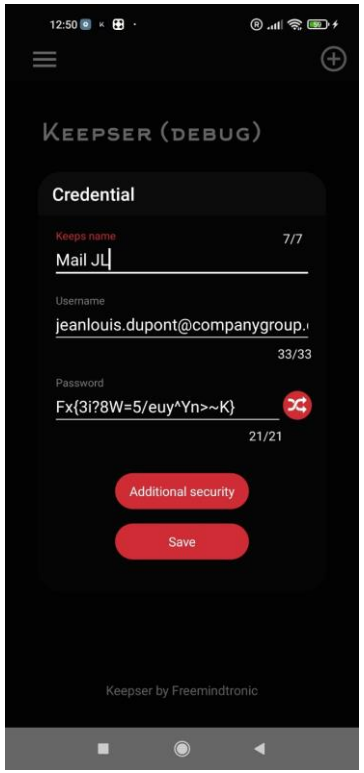
Example for short Keeps name and Username.
The generate password has 45 characters.

Note: the number of available characters for each field is automatically calculated and displayed

Keepser Application

Main Menu – User settings – Random Generator section (3/4)

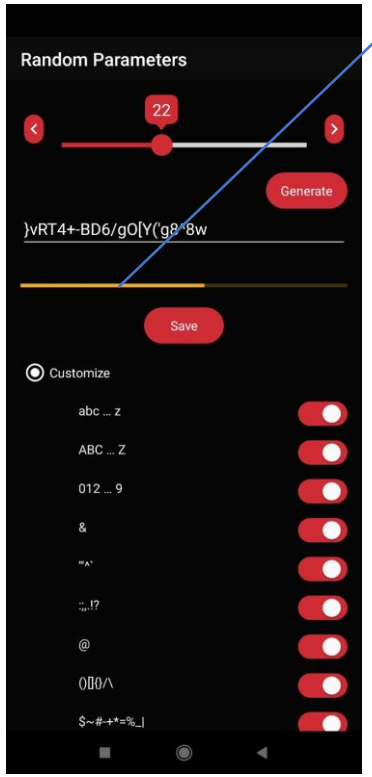
Using and configuring the Random Complex password Generator (ASCII characters).
(When recording a new credential: Data Menu ➔ Add Keeps ➔ User name & password).



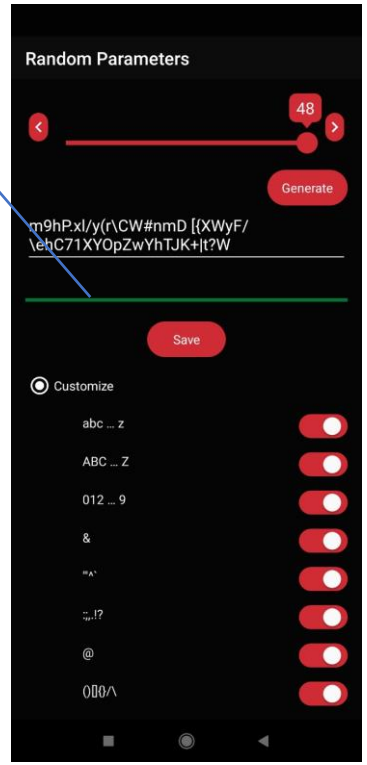
Example for long Keeps name and Username.
The generated password has 21 characters.

(The password length could have been configured higher than 21 characters)

Entropy bar



When configuring the password length, and « Entropy bar » appears with colors to provide an estimate of the robustness of the generated password.
Orange color = average entropy and password robustness.

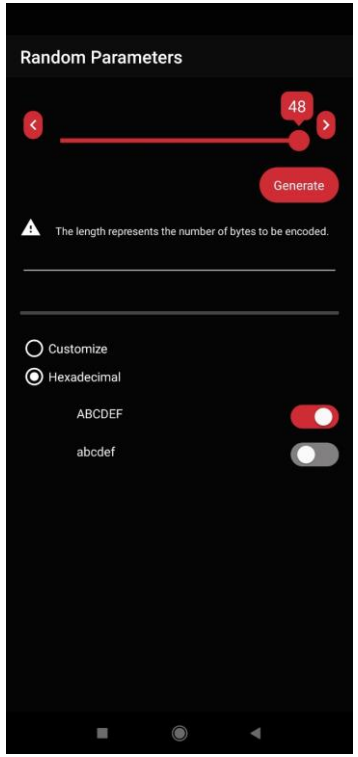


Green color = strong entropy and password robustness.

Keepser Application

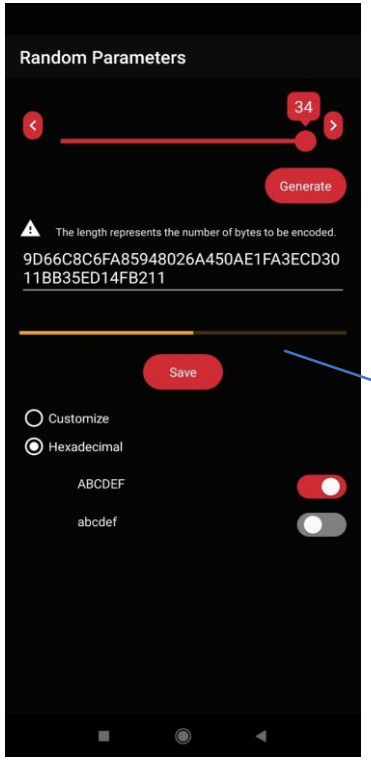
Main Menu – User settings – Random Generator section (4/4)

Using and configuring the Random Complex password Generator (ASCII characters).
(When recording a new credential: Data Menu ➔ Add Keeps ➔ User name & password).



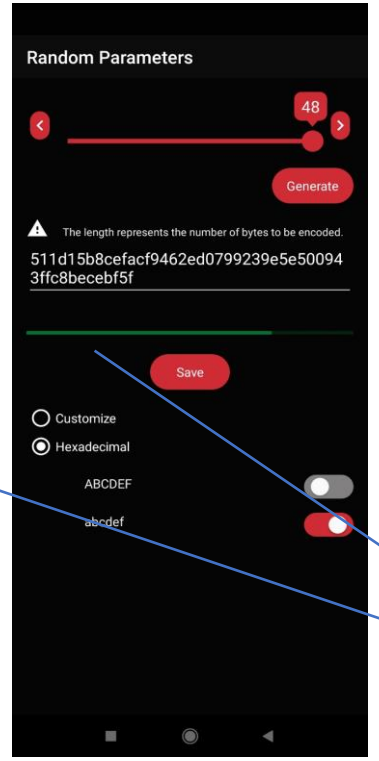
If the Hexadecimal option is turned ON in the Random Generator section, a long click on the « shuffle » icon is opening the above menu.

You can then select upper-case or lower-case characters.



When configuring the password length, an « Entropy bar » appears with colors to provide an estimate of the robustness of the generated password.

Orange color = average entropy and password robustness.



Entropy bar

Green color = strong entropy and password robustness.

Main Menu – Settings - User settings – Clear Clipboard

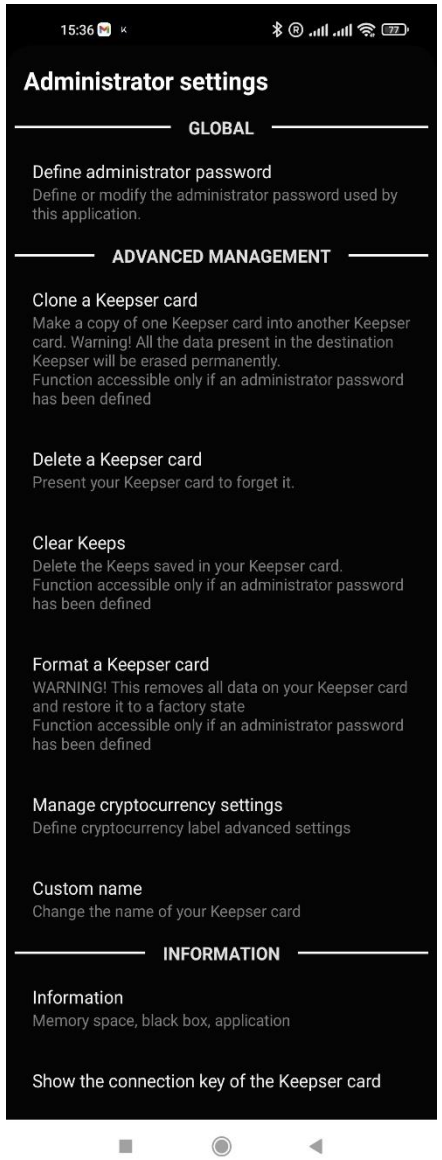
Some of the Keepser App functions allow you to copy information or QR Codes into the Clipboard of the phone. Click on « Clear Clipboard » to permanently erase it.

For security reasons, it is recommended to erase the Clipboard regularly.

Main Menu – Settings - User settings – FAQ

Clicking on « FAQ » will bring you to the Frequently Asked Questions posted on **www.Keepser.com website.**

ADMINISTRATION MENU



GLOBAL SECTION:

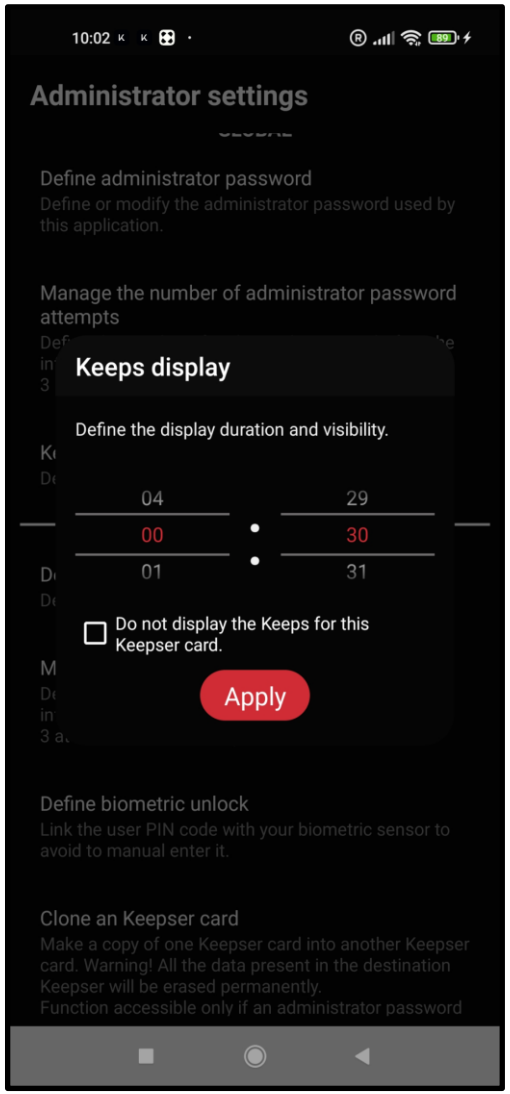
Define Administrator password:
This allows you to change your administrator password. Between 1 and 16 characters.

Manage the number of administrator password attempts:
This is set at 3 attempts by default.
It could be changed between 1 and 15 attempts.

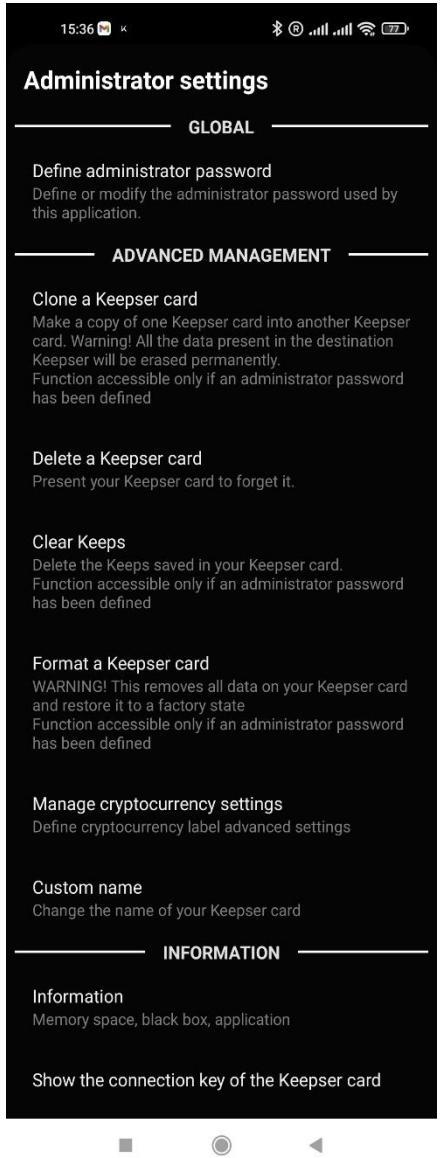
Keeps display:
This feature allow you to define the time for which the information of a Keeps is displayed. 30 seconds is set by default. It can be configured between 5 seconds and 5 minutes.

IMPORTANT: by selecting the “Do not display the Keeps” check box, the user will not be able to see the information of the Keeps. It can only see the list of Keeps and use the Keeps without knowing its content. This is very convenient when the administrator is different from the user (company & employee for example).

If a user tries to display the information of a Keeps hidden by the administrator, a “operation unavailable” message will be displayed.



Main Menu – Administration Settings - ADVANCED MANAGEMENT (1/4)



- **Define User PIN code: see slide 50**

If this User PIN code is defined, it will be required when a user wish to access the Keeps list.
(Main Menu → My Keepser)
The PIN code shall have 4 digits minimum and 8 digits maximum. See next page for details.

- **Manage PIN attempts: see slide 50**

Set to 3 attempts by default. Could be configured between 1 and 15.

- **Define biometric unlock: see slide 50**

You will be able to use the fingerprint recognition capability of your phone, instead of typing the User PIN. See next page for details.

- **Clone a Keepser Card: see slide 51**

This function allows you to clone (replicate) your Keepser Card and copy all the information, configurations and settings into the “Safe Clone” back-up card, or another Keepser Card.

To perform this operation, you will be asked to enter the Administrator password. The content of your Keepser Card will be temporarily copied into the volatile memory of the phone (encrypted of course), will be copied into the 2nd card, then erased from the phone memory.

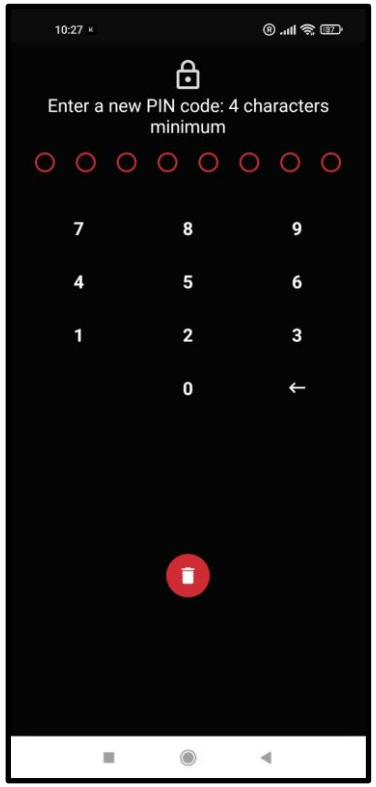
You have to keep the cards close to the phone during the entire operation. Depending upon the number of Keeps stored in your card, this could take from 30 seconds up to 4 minutes.

- **Delete a Keepser Card:**

This function cancel the connection of the Keepser Card with the phone using the Keepser App. All data and settings are kept in the card.

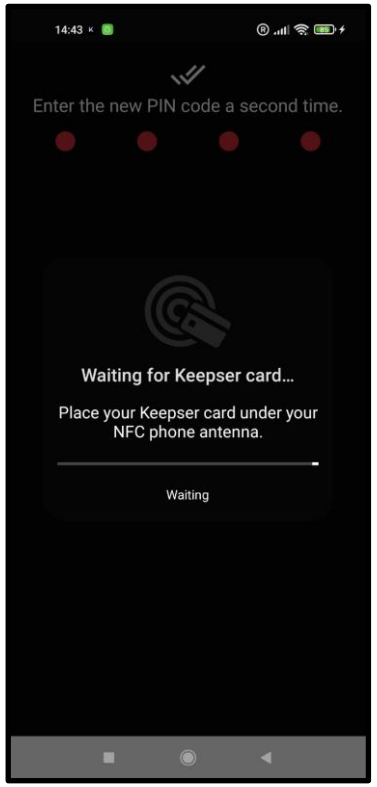
• Setting up a User PIN and the biometric feature

Main Menu ➔ Administration ➔ Advanced Management



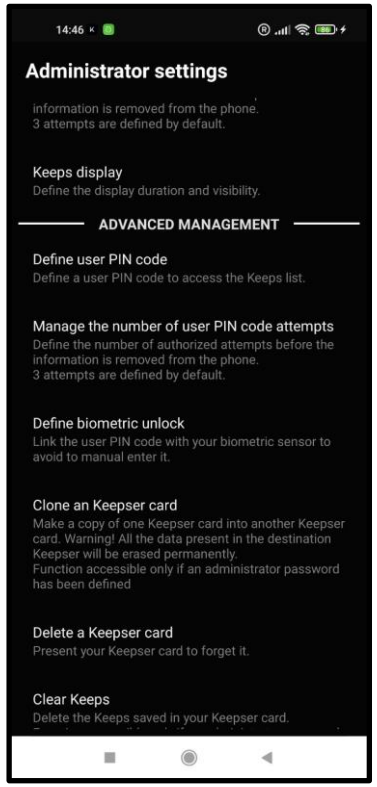
Step 1:

Define the User PIN by typing at least 4 digits and maximum of 8 digits.



Step 2:

Confirm the User PIN and record/save it in the Keepser Card



Step 3:

If you wish to set up fingerprint recognition, click on « biometric unlock » and follow the instructions on the screen.

• Using User PIN and Fingerprint

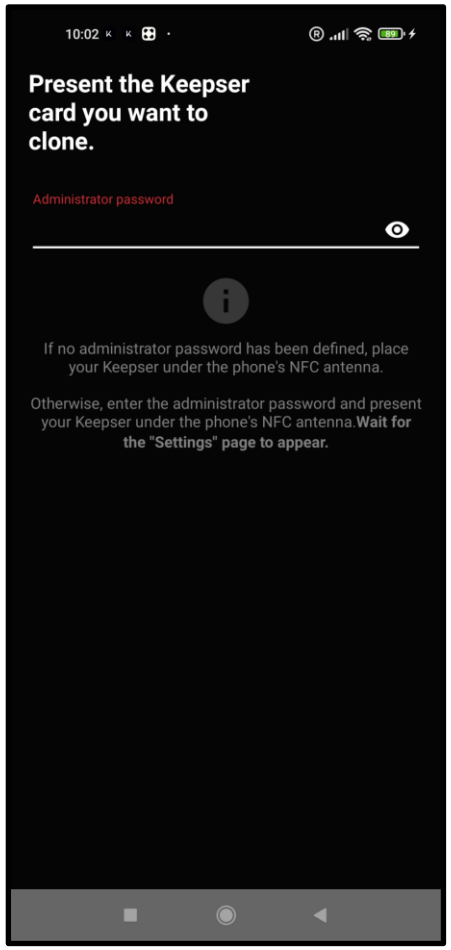
Main Menu ➔ My Keepser

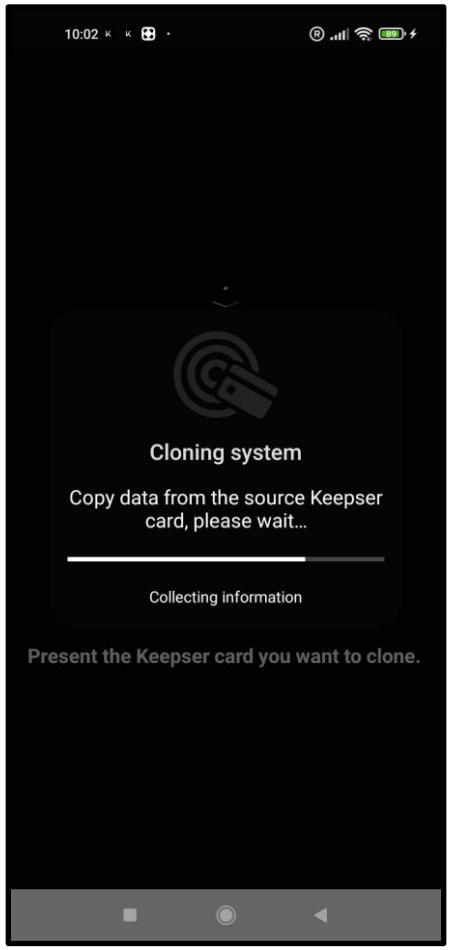
When accessing « My Keepser » this window opens.

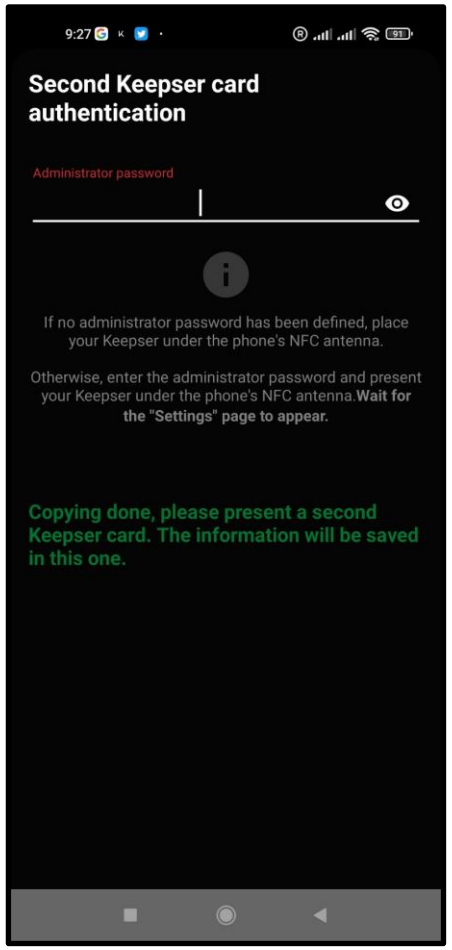
To display the Keeps list, the user should enter the User PIN or put his finger on the biometric sensor of your phone.

If the « Random Keyboard » option has been set in the User Settings, the numbers of the key pad are shuffled.

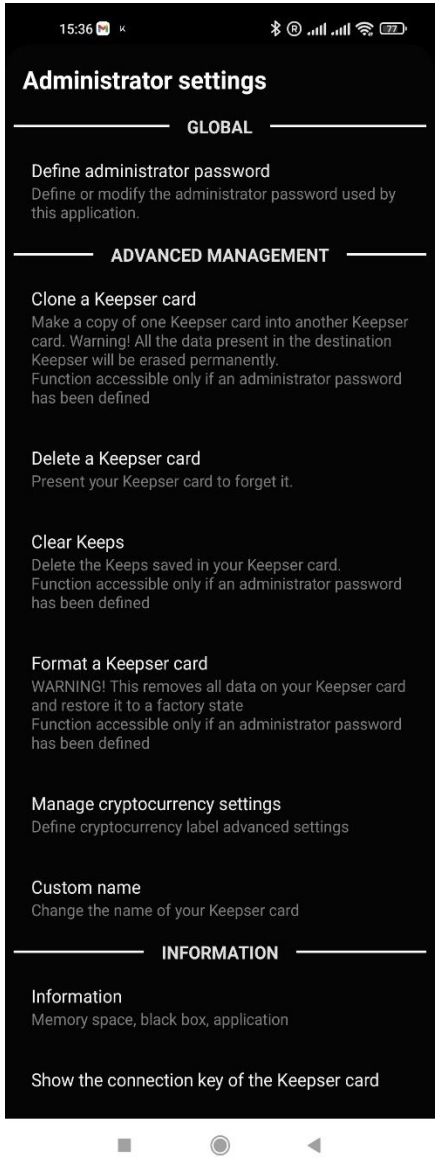
Main Menu – Administration Settings - ADVANCED MANAGEMENT (3/4)







Main Menu – Administration Settings - ADVANCED MANAGEMENT (4/4)



- **Clear Keeps:**

Delete all the Keeps from the Keepser Card. Configurations and set-ups are remaining intact.

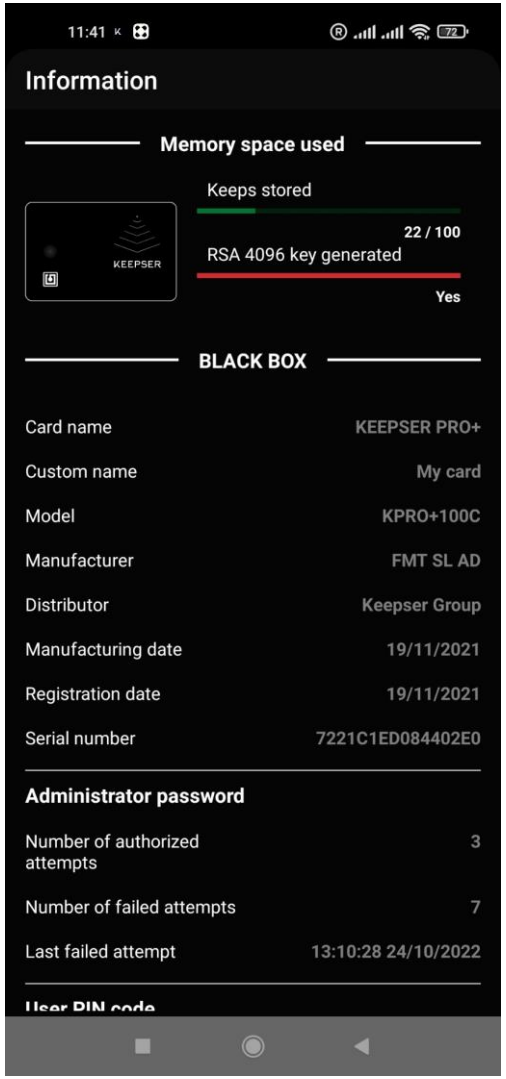
- **Format a Keepser Card:**

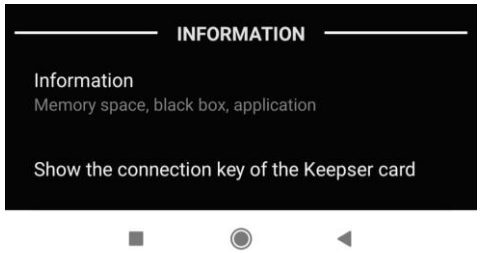
Allows the administrator to reset the Keepser Card to the factory state.

- **Custom Name:**

This allows you to give a custom name to your card.

Main Menu – Administration Settings - INFORMATION





This section provide a set of information related to your Keepser Card and the Keepser App. There is no optional configuration.

- **Memory Space used:**

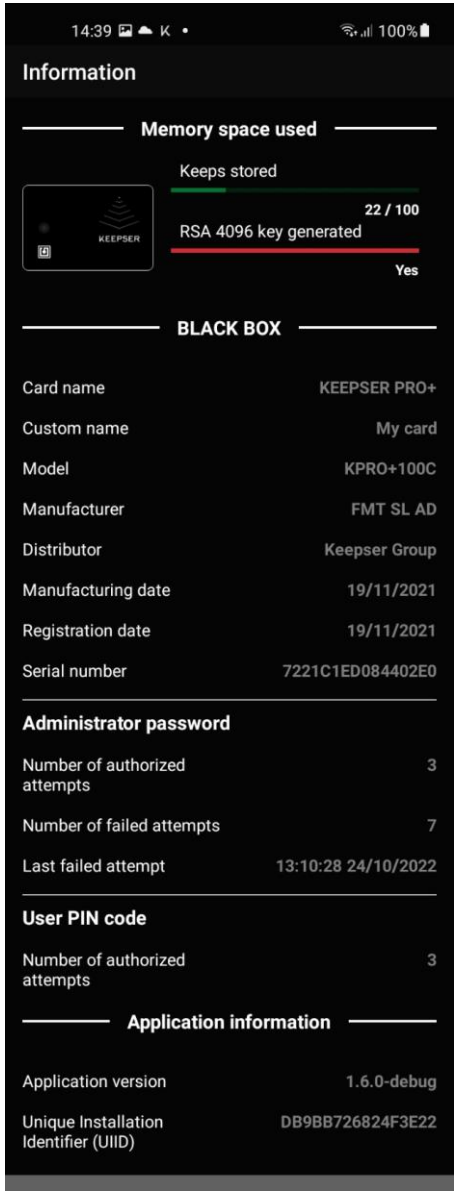
Provides the number of Keeps stored in the Keepser Card with a visualization of the space taken by the Keeps. It also tells you if a RSA 4096 has been generated and stored in the card.

BLACK BOX SECTION

- **Card Name** : The Keepser Card model
- **Custom name:** Provide the Custom Name of the card the administrator may have defined
- **Model:** Internal Keepser code
- **Manufacturer:** Provide traceability on the hardware manufacturing line.
- **Distributor**: Keepser Group
- **Manufacturing Date:** Provide traceability on the manufacturing date
- **Registration Date:** Date on which the card has been first connected
- **Serial number:** This is the unique serial number of the Keepser Card.

This number will show on your invoice, and will be required to order a stand-alone “Safe Clone” card, without buying a Keepser Card.

Main Menu – Administration Settings - INFORMATION



This section provide a set of information related to your Keepser Card and the Keepser App. There is no optional configuration.

- **Administrator password:**

  -- Number of authorized attempts : as set up in the administration menu.

  -- Number of failed attempts : Number of incorrect administrator passwords entered since the first use.

  -- Last failed attempt: traceability on the time of the last failed attempt.

- **User PIN code:** as set up in the administration menu
- **Application information:** Provide the revision of the installed Keepser Application
- **Unique Installation Identifier:** created when installing the App.
- **Show the connection key of the Keepser Card:**

This function generates the QR Code of the key used for NFC secured connection between the Keepser Card and the Keepser Application.