

První certifikační autorita, a.s.



User Manual

I.CA RemoteSign Mobile Application

datum vytvoření:	30.9.2019
datum změny:	8.11.2021
verze:	1.4
počet stran:	22

CONTENTS

CONTENTS	2
1. INTRODUCTION	3
2. INSTALLATION	3
3. INITIAL APPLICATION LAUNCH	4
4. DEVICE ACTIVATION	5
4.1 PASSWORD SETTING, BIOMETRICS ACTIVATION	6
4.2 ACTIVATION COMPLETED, SIGNING OF THE AGREEMENT	7
5. APPLICATION LOGIN	8
5.1 LOGIN – BIOMETRICS	8
5.2 LOGIN – PASSWORD	8
5.3 LOGIN – INCORRECT PASSWORD ENTERED	8
6. PASSWORD RESET	9
6.1 NEW PASSWORD SETTING	9
7. TRANSACTIONS	9
7.1 TRANSACTION LIST	10
7.2 TRANSACTION DETAIL	12
8. SETTINGS	16
8.1 SETTINGS – MAIN SCREEN	16
9. PASSWORD CHANGE	17
9.1 PASSWORD CHANGE.....	18
10. DEVICE	18
10.1 DEVICE LIST	18
10.2 ADD A DEVICE	19
10.3 DEVICE DETAILS	20
11. SUBSEQUENT CERTIFICATE	22
12. APPLICATION FAILURE REPORT	22
13. PUSH NOTIFICATION	22
14. DEVICE ACTIVATION FROM BACKUP	22

1. INTRODUCTION

I.CA RemoteSign (hereinafter "RemoteSign") is an application for the Google Android and Apple iOS platforms, forming the client part of the RemoteSign system designed for electronic signing on mobile devices.

Mobile device requirements:

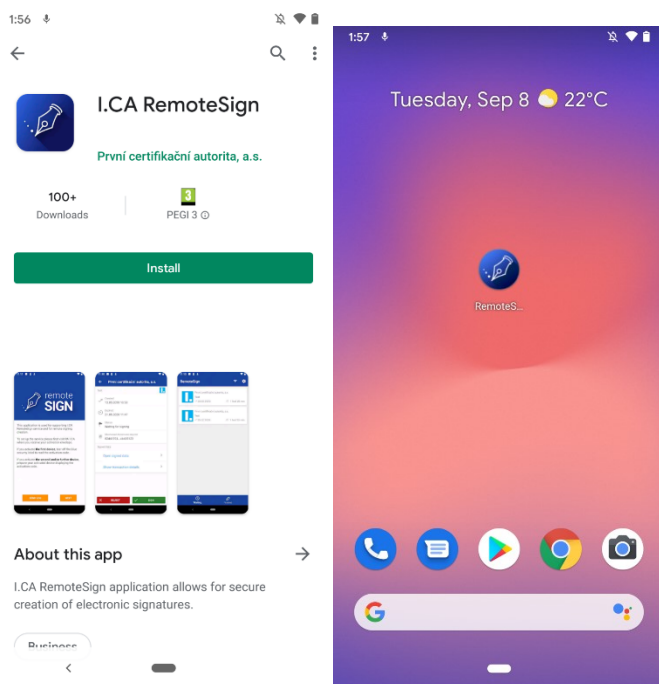
- mobile phone or tablet with operating system Android version 6.0 and higher or iOS 10.0 and higher
- mobile phone must not be rooted or jailbroken and must not contain any software installation from untrusted sources
- minimum free 100 MB of phone internal memory (the application cannot be stored in an external storage)
- internet connection

Other prerequisites for activation of the application:

- signed agreement on issuance of qualified certificate
- activation envelope

2. INSTALLATION

The application can be downloaded and installed for free from Google Play (Android) or App Store (iOS) under the name „I.CA RemoteSign“. A new application launch icon will be added during the installation.

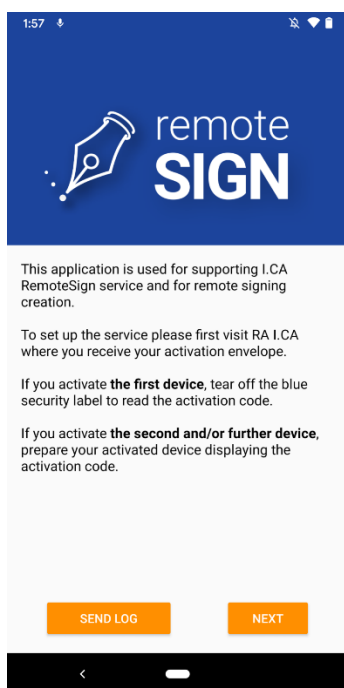


Once the application has been installed, its activation must be done first, followed by signing the Agreement on using I.CA RemoteSign service (applicable only for electronic issuing, otherwise the agreement in printed/paper form will be signed). All these steps must be done beforehand the application could be fully used.

3. INITIAL APPLICATION LAUNCH

Initial launch of the application is followed by the screen displaying basic information on how to proceed. Activation of the service is done at První certifikační autorita, a.s. sales points or by service providers operating activation service points. Here, the identity of user (service applicant) is verified, user is registered and then the agreement on issuance of a certificate is signed (applicable for printed/paper form of the agreement). Once registered, a user is provided with activation documents (activation envelope).

User must then scratch security label placed on activation envelope and proceed to application activation in their device.



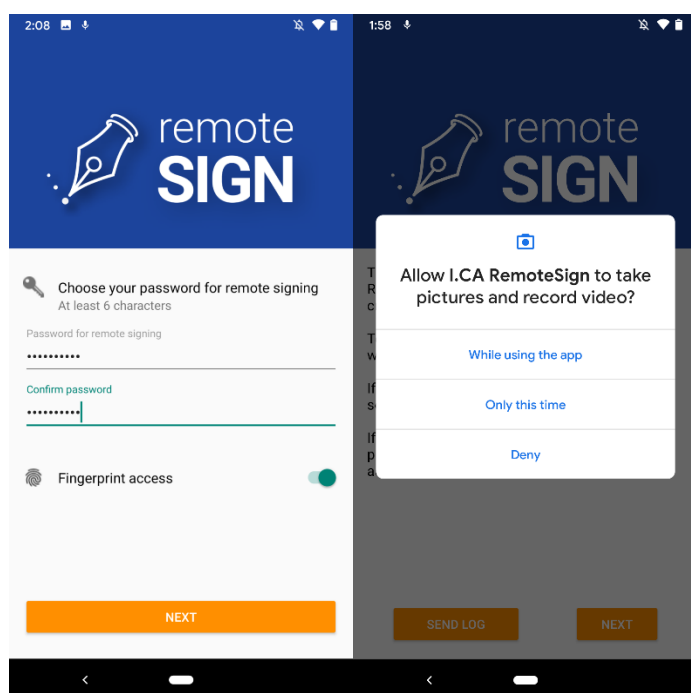
Important information:

Please retain your activation envelope for further use, e.g. password reset or device activation from backup.

4. DEVICE ACTIVATION

Mobile application activation follows these steps:

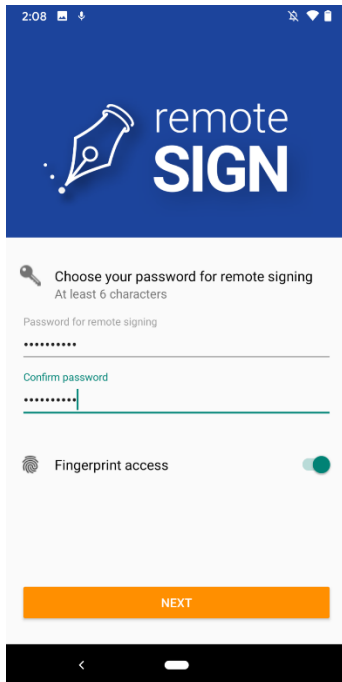
1. Scanning activation code (2D barcode) placed on activation envelope. Scanner integrated in the application is used for this scanning (access to camera must be granted to the application).
2. Choosing and entering password for future signing and authentication to the application, activation of biometrics.
3. Electronic signing of the Agreement on using I.CA RemoteSign Service (applicable for electronic documentation).



4.1 Password setting, biometrics activation

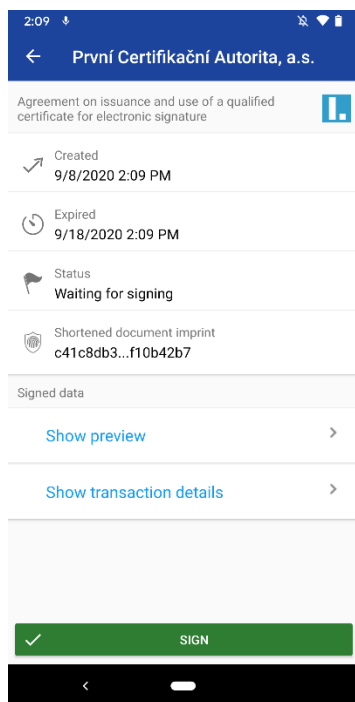
Password must be entered twice (to confirm it) and its length is at least 6 alphanumeric characters (A-Z, 0-9) and must contain one letter at least (case sensitive).

Once the password has been entered, biometrics can be activated (on supported devices). Biometrics is not available on unsupported devices.



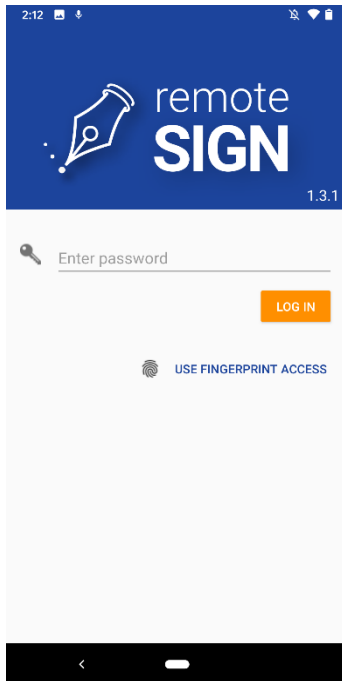
4.2 Activation completed, signing of the agreement

To start using the application for documents signing, activation must be completed by signing the Agreement on using I.CA RemoteSign service (unless documentation in printed/paper form has been signed at a sales point). Signing of the agreement is equal to signing of standard document/transaction with the only difference – signing of the agreement must not be rejected so that the application/device could be used. Successful activation is confirmed by displaying of the relevant screen.



5. APPLICATION LOGIN

To log in to the application and view transactions (signing requests), the user can choose between password authentication and biometrics (if supported by the device).



Types of the application launch:

- **Standard** (using an icon) - having logged in, the transaction list screen will be displayed
- **From push notification** – having logged in, the detail of particular transaction will be displayed

5.1 Login – biometrics

If the user enabled biometrics login, they log in by putting their finger on the fingerprint reader or by using *faceID*.

5.2 Login – password

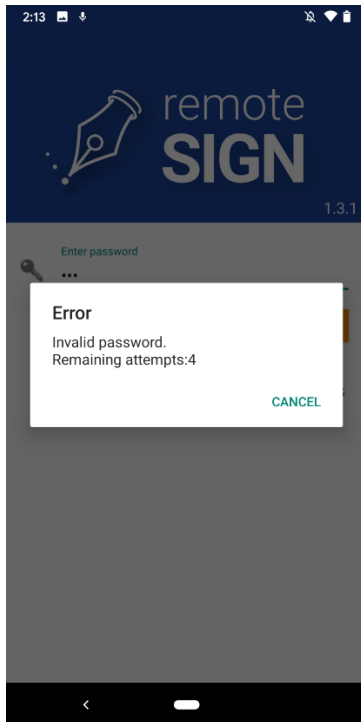
If biometrics login is not enabled, the user must log in using their password.

5.3 Login – incorrect password entered

5.3.1 Remaining „n“ attempts

The user has 5 attempts to enter correct password

If the user enters incorrect password, they will see information about the incorrect password and the number of attempts remaining.



5.3.2 Blocked password, password reset option

If the user has used up all attempts (forgotten the password), a screen will be displayed in which they can select the option to reset the password.

6. PASSWORD RESET

If the user has forgotten their password, the option to reset it is available. The activation code (2D barcode) from activation envelope must be scanned again to reset the password.

6.1 New password setting

If the activation code has been successfully retrieved, continue to set a new password.

6.1.1 Invalid password

If entered passwords do not match (entered twice for checking) or do not meet security requirements, the information is displayed that the password has not been accepted (must be entered correctly).

7. TRANSACTIONS

Each request for signing, certificate renewal, etc. is called a transaction.

For users, individual transactions will look similar to emails. From the user's point of view, each transaction will have:

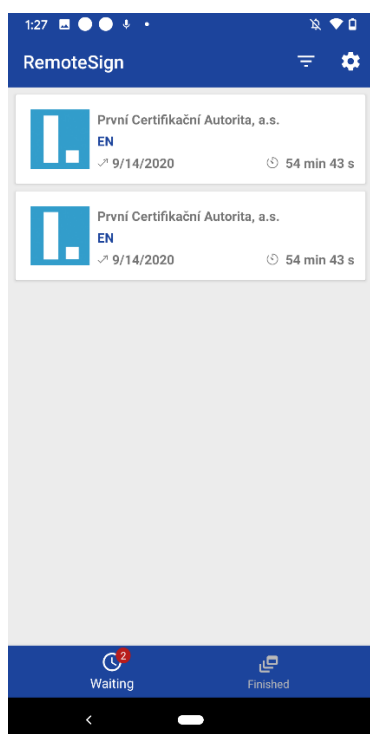
- its (verified) originator (service provider)
- date and time of creation

- validity
- subject of the transaction
- preview or download link for all signed data (encrypted)
- hash (imprint) of signed data
- status (unread/read/signed/rejected/expired)

The user can mark each individual transaction as read/unread and, after viewing the transaction details, sign or reject it.

7.1 Transaction list

On the transaction list screen, transactions are divided into waiting and finished/completed. To switch between these lists, click on the appropriate option at the bottom of the screen. For waiting transactions, the number of unread transactions is indicated.



7.1.1 Displayed transactions

For each transaction, the logo of its originator (service provider), the name of the originator, the subject of the transaction, the creation date of the transaction and the time remaining until the expiration of the transaction are displayed.

An unread transaction is shown in bold and displays the number of unread transactions for the "waiting" option. The list of waiting transactions is sorted by the date and time of the transaction's expiration from the nearest (top) to the latest (bottom) expiration date.

The list of finished transactions is sorted by date and time of completion (i.e. signing, rejection or expiration of the transaction) from the most recently finished (top) to the oldest (bottom) finished transactions.

The history of transactions is maintained for at least 1 month.

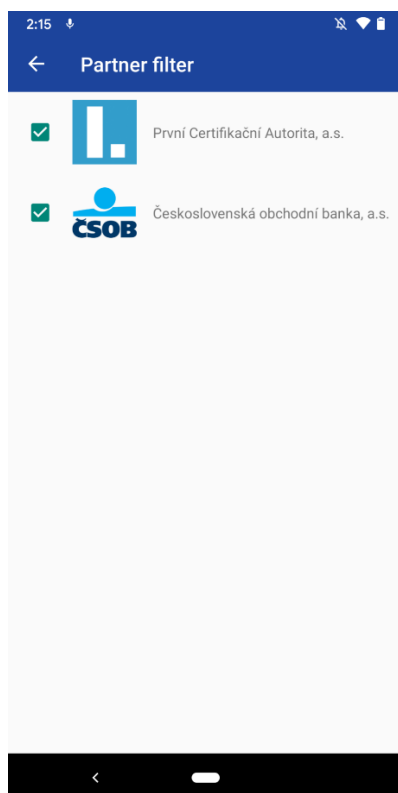
The list of transactions can be restored (reloaded from the server) by "swiping" the list down. When scrolling the list upwards (i.e. by scrolling the list downwards), in case of a larger number of transactions in the list, further transactions are gradually loaded from the server. In this case, if other transactions are waiting to be downloaded from the server for display, the information "Loading, please wait" is displayed at the end of the list while waiting. This information is replaced by the relevant transaction after downloading the information about such transaction.

After clicking on a specific transaction, its detail will be displayed.

7.1.2 Filter setting in the transaction list

It is possible to filter by partners (I.CA, ČSOB) in the list of transactions.

By default, the filter is set to display everything. Other filter settings are valid only for the given session. It is not saved when the application is closed.



7.2 Transaction detail

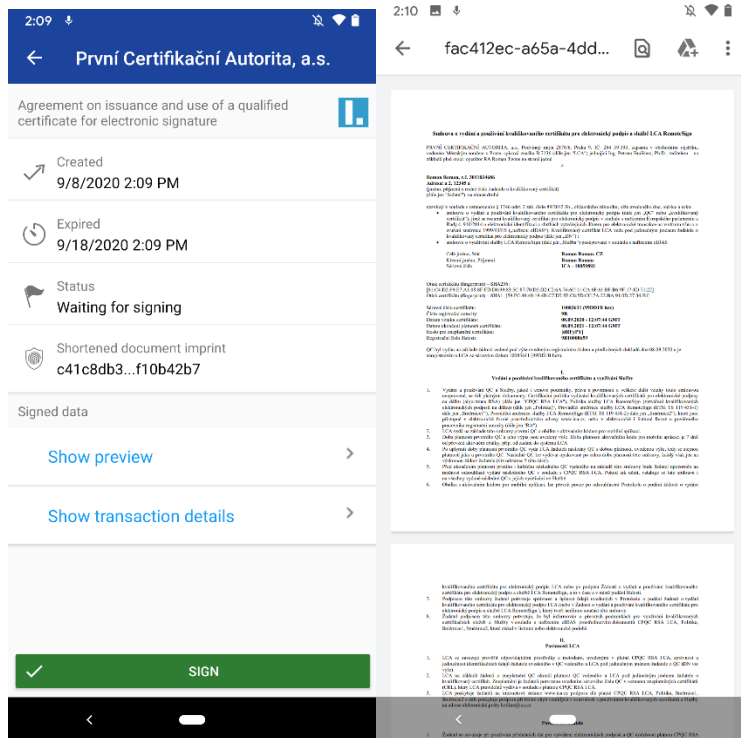
In the transaction detail, the transaction can be signed or rejected. The "Reject" button can be inactive for specific transactions (e.g. for signing an agreement on using I.CA RemoteSign service).

The transaction detail contains an option to preview the signed data or to download and display the signed data in the associated application.

Detailed information is available for each transaction, which the user can display, if interested, by selecting the option "Show transaction detail", the complete hash (imprint) of the document and the transaction ID are shown here.

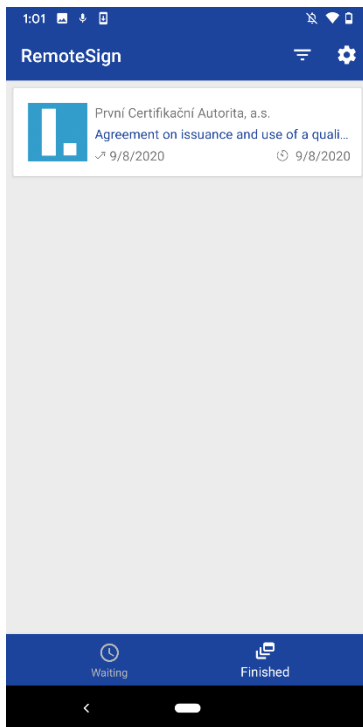
After clicking on the "Sign" button, it is necessary to authorize the operation:

- First signature in a row - password required.
- Next signature in a row - biometrics can be used (if active)



7.2.1 Finished transactions

The user can view the list of finished/completed transactions here.



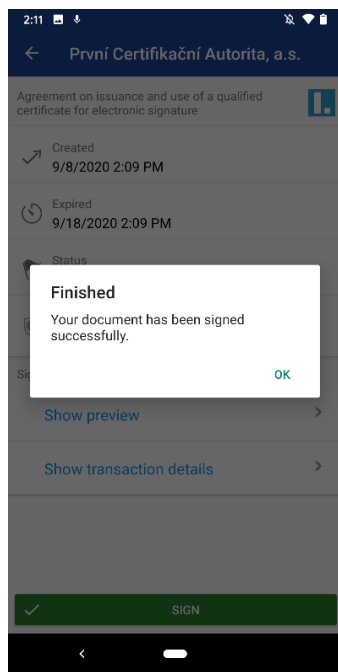
7.2.2 Transaction cannot be signed on the given device

The screen with this information is displayed in cases where, for technical reasons, it is not possible to sign a particular transaction on a specific device (e.g. when the transaction occurred before the activation (cloning) of the mobile application).

The user is redirected back to the list of transactions.

7.2.3 Signed successfully

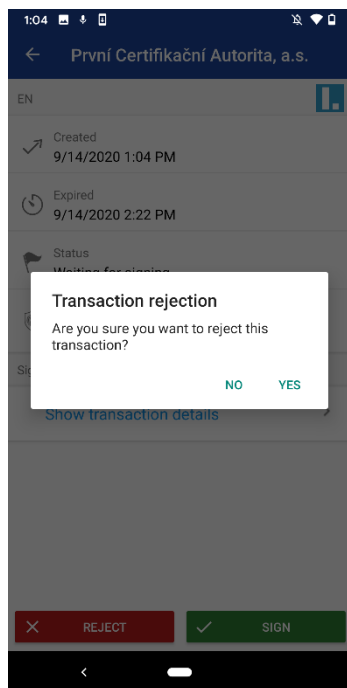
The user is informed about the successful completion of the transaction signing by a pop-up window, after clicking on it the user is returned to the list of waiting transactions.



7.2.4 Reject transaction

The transaction is rejected by pressing the "Reject" button, then a pop-up window is displayed asking if the user really wishes to reject the transaction.

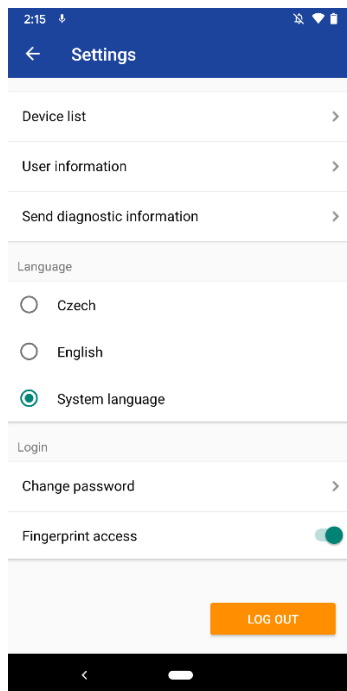
Rejection of a transaction cannot be undone.



7.2.5 Expired transaction

When a transaction has been expired, the relevant information is displayed and such transaction cannot be signed anymore.

8. SETTINGS

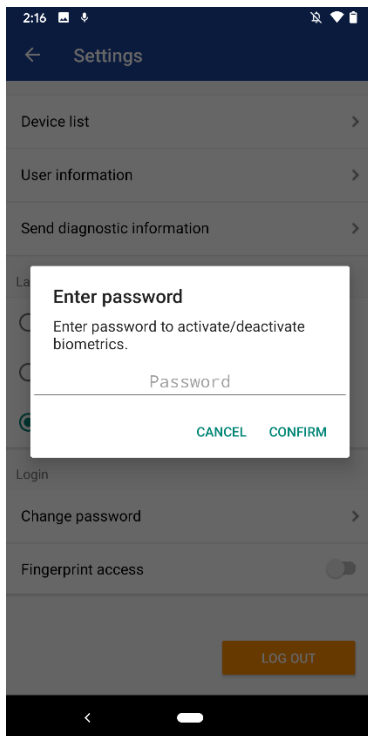


8.1 Settings – main screen

Main application settings screen in which you can select one of the actions:

- view user and device information
- change password
- activate biometrics
- deactivate biometrics (deactivation of biometrics is done immediately without asking for a password)
- send diagnostic information
- display a list of devices

8.1.1 Biometrics activation – entering password



Changing the status of the biometrics activation switch will display a new window for entering the password for biometrics activation authorization.

8.1.2 User and device information

The application displays information about the user and the device.

This screen is rather intended for diagnostic purposes in the event of troubleshooting.

8.1.3 Send diagnostic information

Through this screen, diagnostic information can be sent ad hoc to I.CA Technical Support (HelpDesk).

The diagnostic information does not contain any sensitive data, such as passwords, keys, signed data, signed data preview, link, or authentication headers for signed data. The diagnostic information is encrypted before sending to keep the transmitted logs between the mobile application and the I.CA secret.

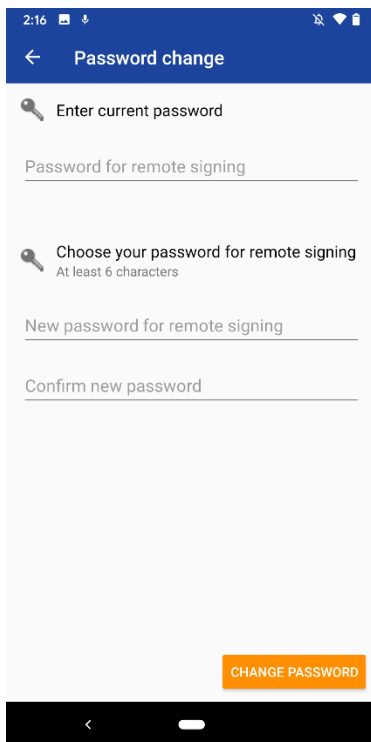
9. PASSWORD CHANGE

The user can choose to change the password on the setting screen.

If the user forgets the password, password reset functionality is available. To reset the password, the user must retrieve the activation code (2D barcode) from the activation envelope.

The password must be at least 6 alphanumeric characters long (A-z, 0-9) and contain one letter at least. The password is case sensitive.

9.1 Password change



The screenshot shows a mobile application interface for changing a password. At the top, there is a blue header with a back arrow, the text "Password change", and a plus icon. Below the header, there are three sections, each starting with a key icon:

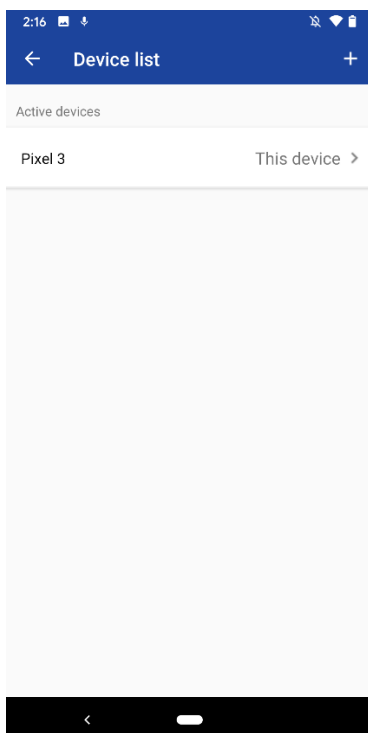
- Enter current password**: A text input field labeled "Password for remote signing".
- Choose your password for remote signing**: A text input field labeled "New password for remote signing" with a sub-label "At least 6 characters".
- Confirm new password**: A text input field labeled "Confirm new password".

At the bottom right of the form area, there is an orange button labeled "CHANGE PASSWORD". The bottom of the screen shows a black navigation bar with a back arrow and a home indicator.

On this screen the original password and the new password must be entered (twice for checking).

10. DEVICE

10.1 Device list



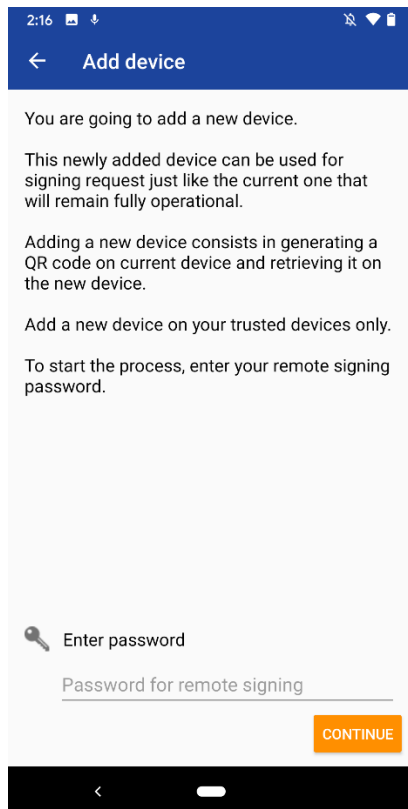
The screenshot shows a mobile application interface for the device list. At the top, there is a blue header with a back arrow, the text "Device list", and a plus icon. Below the header, there is a section titled "Active devices". Under this section, there is a list item for "Pixel 3" with a right-pointing arrow and the text "This device >". The rest of the screen is empty. The bottom of the screen shows a black navigation bar with a back arrow and a home indicator.

Device list can be found in Settings.

It displays a list of previously activated devices (active, blocked (even for a specified period of time), cancelled).

It allows the user to add another device or view the details of a specific device.

10.2 Add a device



The option to add devices is available in the device list.

It informs about the way and consequences of cloning a device with the option to enter a password to continue.

10.2.1 Activation QR-code for a new device

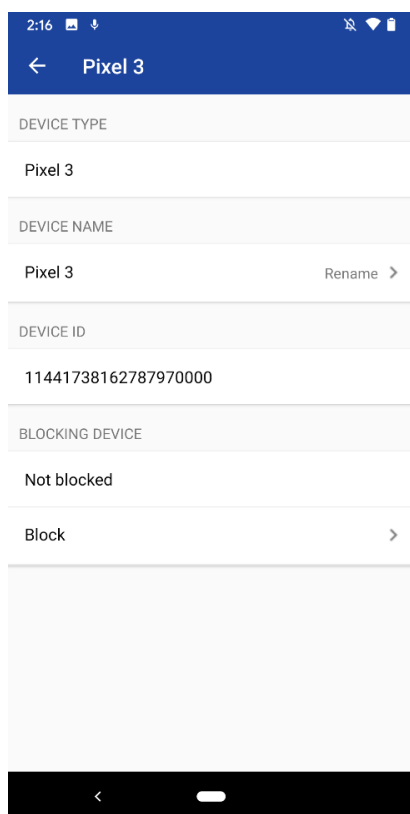
The application generates an activation QR-code for activation of another device.

10.2.2 Warning – attempt to cancel unfinished cloning

If the user attempts to cancel an incomplete cloning, a consequences warning is displayed asking if the cloning should actually be cancelled:

- YES - cloning will be cancelled
- NO - cloning continues

10.3 Device details



This screen displays the device details:

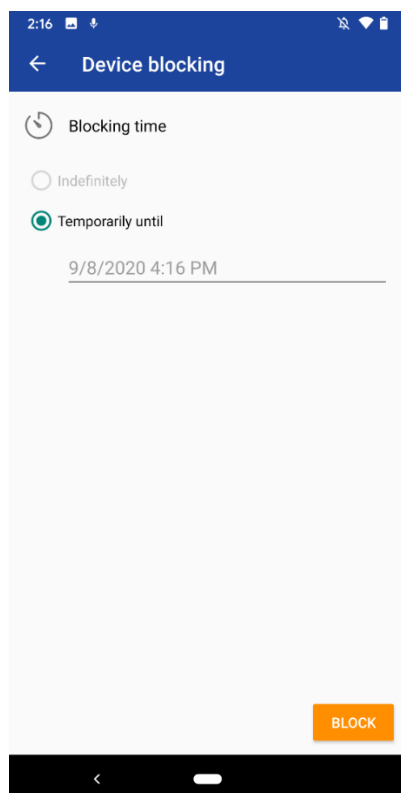
- *Device type*
- *Device name*
- *Device ID*
- *Device status*

Following options can be chosen:

- Rename device
- Block device:
 - block temporarily (for specified period)
 - block indefinitely
 - block permanently
 - unblock

10.3.1 Block device

The device can be blocked for a specified time or indefinitely. In the case of blocking for a specified time, the user enters the date and time until which the device should be blocked. After this time, the device will be unblocked automatically.



10.3.2 Block device – blocked successfully

This screen informs about the successful blocking of the device (the time until which the device is blocked is displayed here, if it is a block for a specified time).

10.3.3 Revoke

This screen shows the effects of cancelling the device and is also used to enter the password required to cancel the device. Device cancellation is only possible in case of two (or more) activated devices, otherwise this option is deactivated and the device can only be blocked via the mobile application.

11. SUBSEQUENT CERTIFICATE

60 days before the certificate expires, the device will request a "RemoteSign Certificate Renewal Request". After signing this request, a request for the issuance of a subsequent certificate will be sent. Once the subsequent certificate is issued, it is then automatically used for further signing, there is no need for the client to do anything else.

If the request is not signed immediately, the application will not allow the signing of a transaction other than the request for the subsequent certificate 30 days (and less) before the expiration of the RemoteSign certificate.

12. APPLICATION FAILURE REPORT

This screen offers the option to send diagnostic data to technical support (HelpDesk I.CA/ČSOB).

13. PUSH NOTIFICATION

After the transaction has been created by the originator (service provider), push notifications will be received on all active devices of the given account. Push notification informs about a new transaction to be signed and, regardless of the service provider (originator), appears under the RemoteSign icon. "Clicking" push notification opens the RemoteSign application login page, after logging in, the details of a specific transaction are displayed.

After the transaction is completed and marked on the RemoteSign server as "Finalized", a push notification will be sent informing the user that the signing was successfully completed.

14. DEVICE ACTIVATION FROM BACKUP

Reactivation of the device (e.g. after a reset to factory settings) is only possible if the user account is backed up. OS resources ensure the transfer of selected data of installed applications to the new device. RemoteSign application will not work immediately because no secret security keys have been transmitted. It is necessary to use the original activation code (envelope) to put the application into operation.