Android Application Demo

Blockchain Security 2Go Starter Kit

www.infineon.com

Android Application Demo

Blockchain Security 2Go Starter Kit

About this document

Intended audience

The target readers of this document are Blockchain developers that want to test the blockchain security 2go starter kit with an android phone. When reading this document, you should have

- the Blockchain Security 2Go starter kit,
- an android smart phone such as a google Pixle2 or Samsung Galaxy S8 with NFC capability
- the installed Coinfinity Blockchain Security 2Go example app

1 Introduction

The Android application demonstrator was developed by Coinfinity GmbH and demonstrates an application example for the Blockchain Security 2Go starter kit V1.0 in combination with an NFC-capable Android smart phone. The example application interacts with the Blockchain Security 2Go starter kit V1.0 via NFC and the Ethereum blockchain. The following three signing examples are demonstrated:

- sending and receiving Ethereum tokens (ETH)
- sending and receiving ERC-20 tokens
- Interacting with an example smart contract (based on a voting demonstration) deployed on the Ethereum blockchain.

There are two ways to download the android application example to your smartphone.

- Via google playstore [2]
- Via android studio and the available source code [8]

1.1 How the app works

The app is communicating with the card via NFC to generate new private/public keys, read the public keys and sign transactions. To interact with the Ethereum blockchain, the Web3j library [1] is used to build transactions. Brodacasting of transactions to the Ethereum network is done via the infura.io API [3]. The conversion of ETH balance to EUR is done via Coinfinity rate API and displayed inside the app.

To be able to use the QR code scanning and displaying functionality the app expects the `com.google.zxing.client.android` QR code scanner to be installed via google play store [4]. As the time of writing the app was removed from the appstore, thus the “Barcode Scanner+” from Sean Owen is used [5].

1.2 Android development - Getting started

- Install Android Studio [8]
- Import the project into Intellij or Android Studio, use project type "Gradle"
- Try to build it
- Make sure to install Zxing barcode scanner plus app on device to be able to scan QR codes
- Add an android run/debug configuration in Intellij/Android Studio
- Run/debug app via Intellij/Android Studio

1.3 Android Device requirements

Do not use an Android emulator for testing purposes because NFC is required to interact with Infineon Card.

- minSdkVersion 24
- targetSdkVersion 27
- NFC enabled device
- internet connection
- camera for QR code scanning

1.4 Smart Contract example

The example smart contract is located in a separate folder outside the app project called "Smart Contract". It contains Solidity code for the contract and a truffle suite for testing. [Voting.sol](Smart%20Contract/contracts/Voting.sol) contains the main code of the contract and imports other common ".sol" files. See the Solidity language documentation [5] on further information on how to write Smart Contracts in Solidity. [voting.js](Smart%20Contract/test/voting.js) is the main truffle test file written in JavaScript to quickly test the contract without deploying it on mainnet or testnet. See the truffle documentation [7] on further information on how to write tests for Solidity contracts.

2 Get Tokens

Certainly, in order to try out the signing features and in order to send some ETH, ethereum tokens are needed. Therefore you have to send ETH to the ethereum address of the particular key-index. For developers we suggest to use the testnet first.

A very convenient way to acquire ETH testnet tokens is via metamask [11]. Metamask ist a google chrome, firefox, opera or brave browser extension which enables a wallet option directly in your browser. By having this very efficient ethereum software wallet, testnet tokens can be claimed using the “MetaMask Ether Faucet”. Here you can request 1 ether from the faucet which is then directly transferred to your MetaMask wallet. Having a testnet ether tokens, they can be transferred to the blockchain security 2go starter kit cards.

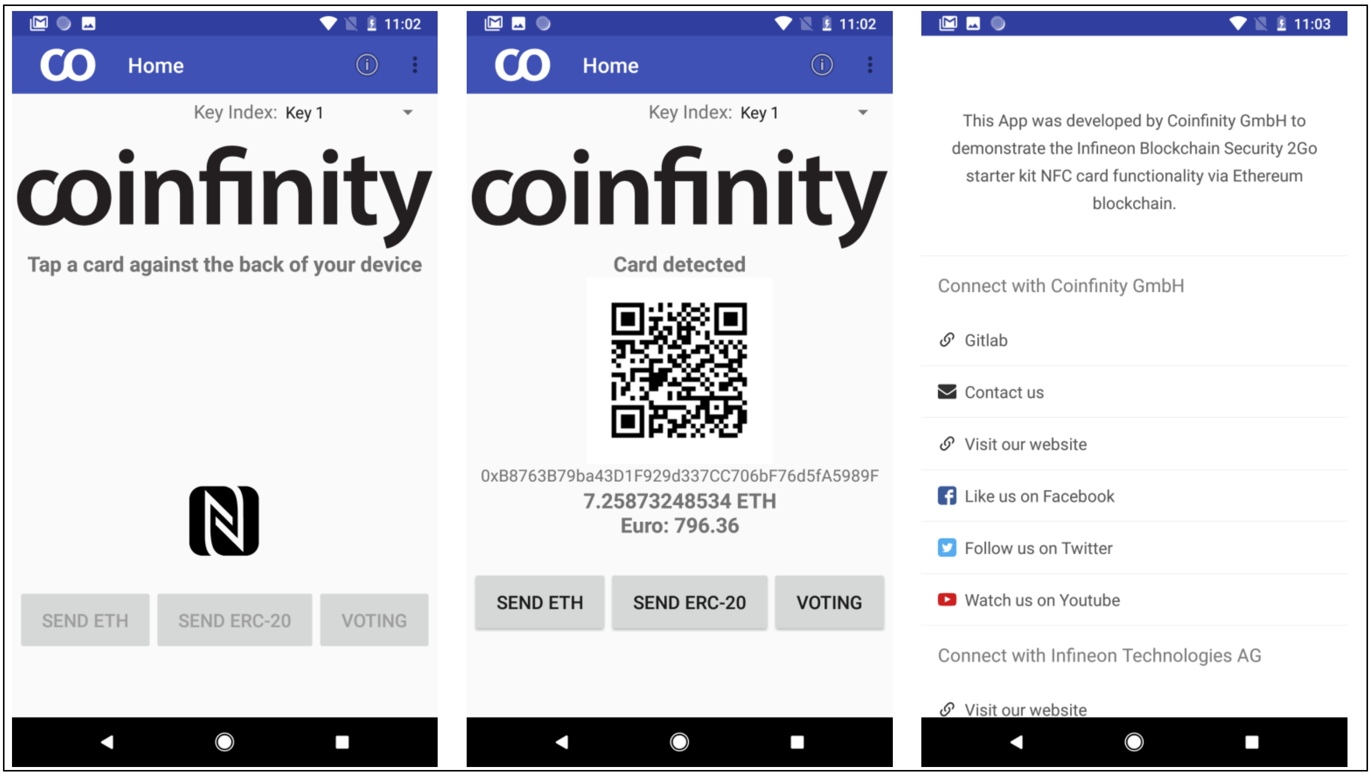
Certainly, mainnet tokens can be also used in the demo application and “real” value can be stored and transferred using the blockchain security 2go starter kit. In order to aquire mainnet ETH, please contact Coinfinity [10].

3 Android App Usage

In the following the functionality of the application example is illustrated and described. Therefore screenshots were taken to showcase all possible options. The language of the app is related to configuration of your device.

3.1 Homescreen

By opening the app you will be asked to present the Blockchain Security 2Go starter kit card on the back of your smart phone where the NFC antenna of your phone is located. The buttons of the three signing applications are grayed out until you present the card. By approaching the card by default the first public key (key index 1) is read out and displayed as an Ethereum address on the screen. Moreover a QR code is shown, which is also representing the Ethereum account. The app automatically performs a query to the Blockchain API in order to display the amount of available tokens which are corresponding to the shown Ethereum address. The value of the available Ethereum tokens is also interpreted as Euro by estimation based on the coinfinity API. By pressing on the info icon in the right corner of the app, Information about Coinfinity is displayed.



Tap a card against the back of your device

Card detected

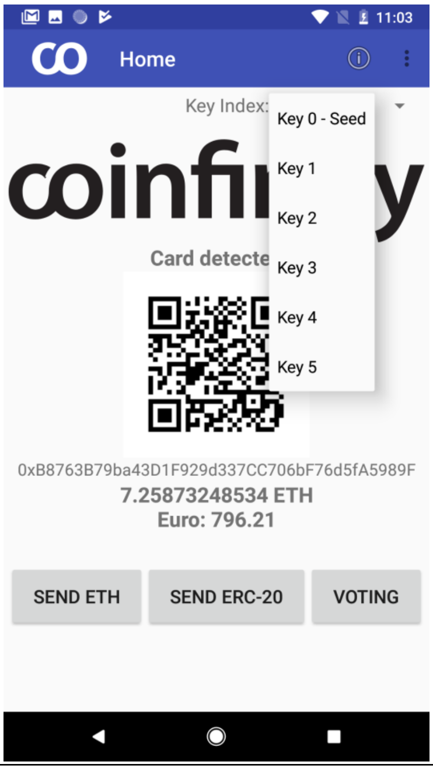
0xB8763B79ba43D1F929d337CC706bF76d5fA5989F
7.25873248534 ETH
Euro: 796.36

This App was developed by Coinfinity GmbH to demonstrate the Infineon Blockchain Security 2Go starter kit NFC card functionality via Ethereum blockchain.

Figure 1 Homescreen: By presenting the Blockchain Security 2Go starter kit card at the NFC interface of the smartphone, the public key is read out and represented as an Ethereum address. This address is also illustrated as a QR code.

3.2 Key Index

The app automatically triggers the generation of 5 keys on the blockchain security 2go card if the particular key is chosen. By default the Key index 1 is read out, and visualized as Ethereum address on the display. In order to change the key which should be represented, the key index option can be changed in the drop down menu. This allows the usage of other keys which can be further used for the signing demonstrators such as sending ETH, ERC20 or the voting demo. Again the Ethereum token amount as well as an Euro estimation is illustrated automatically.



0xB8763B79ba43D1F929d337CC706bF76d5fA5989F
7.25873248534 ETH
Euro: 796.21

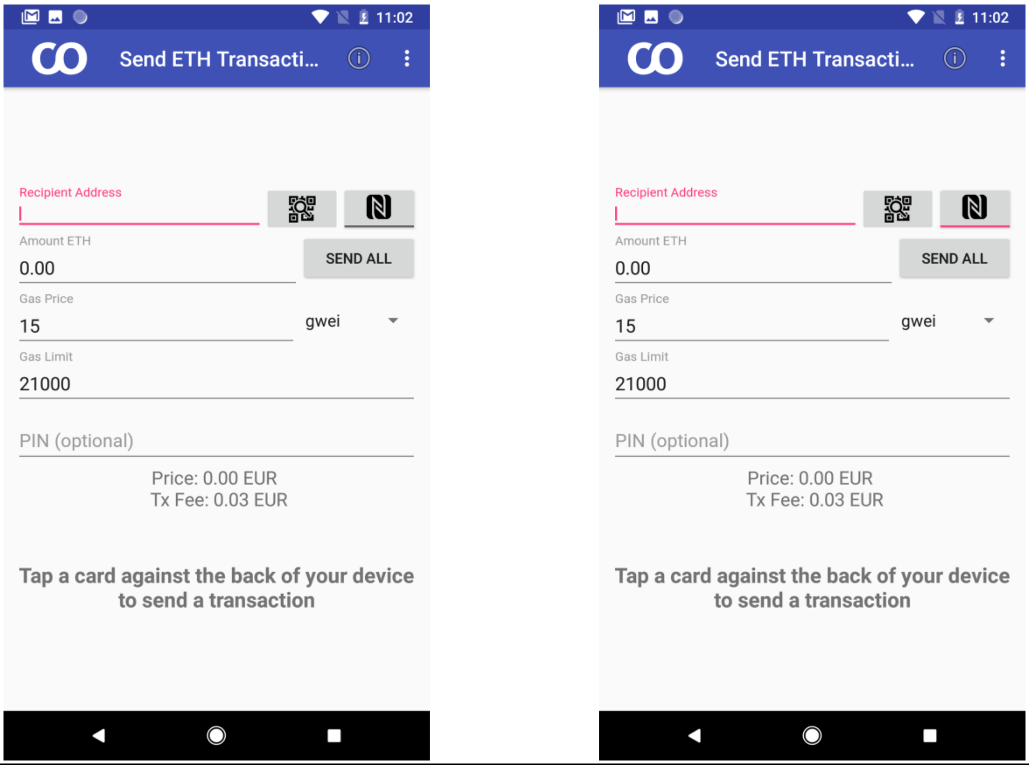
Figure 2 Key Index: To change the key which shall be used in the application example the drop down menu can be use.

3.1 Send ETH and ERC-20

The send ETH option is triggered by pressing the send ETH button when a Blockchain Security 2Go card is available at the NFC interface. Within this option Ethereum tokens (IF AVAILABLE) can be sent to other Ethereum addresses. Therefore a valid recipient address should be specified. This address can be filled out via text (or simple copy function), with the QR code scanning option (QR icon) but also via the NFC read option. The NFC icon represents the option to read out the key index 1 of another Blockchain Security 2Go card. If this option is activated, it will be underlined (see Figure 3). After that you can present the recipient card at the NFC interface and the card Ethereum address is copied into the field.

In order to send Ethereum tokens the amount of ether, the gas price, the gas limit and the pin (if it was configured) have to be specified. To trigger the transaction, the card has to be presented again at the NFC interface of the smart phone in order to sign the generated transaction message.

The same procedure is used in the ERC20 option.



Recipient Address:

Amount ETH: 0.00

Gas Price: 15 gwei

Gas Limit: 21000

PIN (optional)

Price: 0.00 EUR
Tx Fee: 0.03 EUR

Tap a card against the back of your device to send a transaction

Recipient Address:

Amount ETH: 0.00

Gas Price: 15 gwei

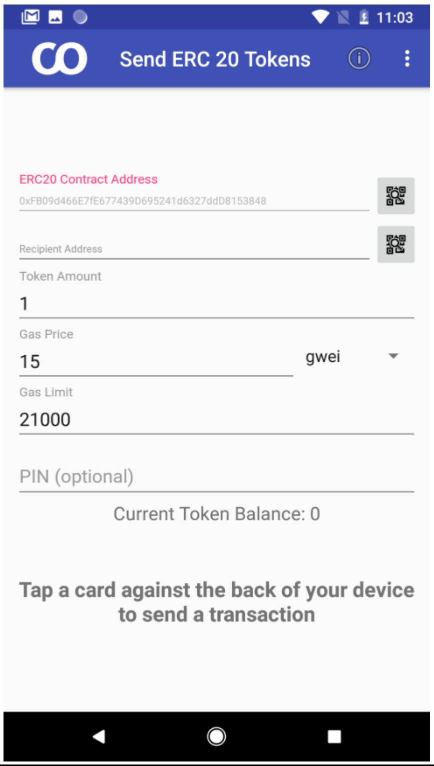
Gas Limit: 21000

PIN (optional)

Price: 0.00 EUR
Tx Fee: 0.03 EUR

Tap a card against the back of your device to send a transaction

Figure 3 **Send ETH: The recipient address can be specified with text, QR code scanner but also NFC. In order to trigger a transaction the card has to be presented at the NFC interface ones more to complete the transaction with the signing process for the generated transaction message.**



ERC20 Contract Address: 0xFB09d466E7fE677439D695241d6327ddD8153848

Recipient Address:

Token Amount: 1

Gas Price: 15 gwei

Gas Limit: 21000

PIN (optional)

Current Token Balance: 0

Tap a card against the back of your device to send a transaction

Figure 4 **Send ERC20: The ERC20 send option is similar to the ETH example. A recipient address has to be specified, as well as the token amount, gas and gas limit.**

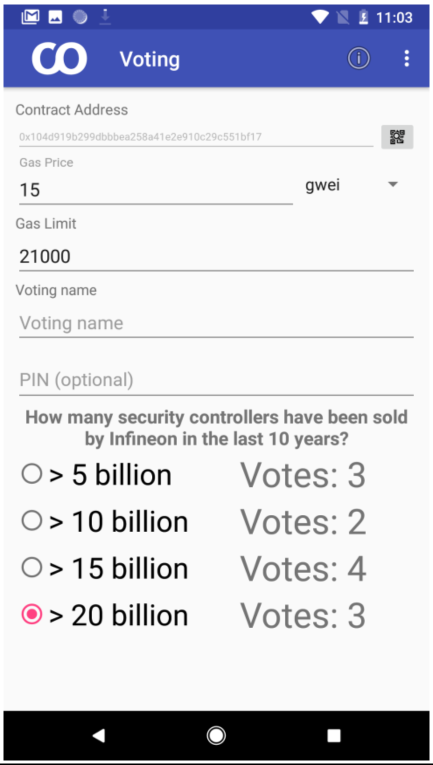
3.1 Voting

The voting application demonstrator illustrates an example of how to use the Blockchain Security 2Go starter kit in combination with smart contracts. Therefore an example contract is used that showcase a decentralized voting demonstrator. Any card can be used in order to cast a vote. Certainly a small amount of ETH is necessary in order to interact with the contract. Within this example a question is asked: "How many security controllers have been sold by Infineon in the last 10years?"

Four answer options are possible: >5billion, >10billion, >15billion, >20billion

Certainly the correct answer would be the biggest number: >20billion.

In order to cast a vote, the card should be represented on the NFC interface. The smart contract example is open source and has the mainnet contract address [9]: 0x2C680955cd340eaE72703e6886957bf8465F9583. It is also hosted on the ethereum ropsten testnet: 0x104d919b299dbbbea258a41e2e910c29c551bf17



Contract Address
0x104d919b299dbbbea258a41e2e910c29c551bf17
Gas Price
15 gwei
Gas Limit
21000
Voting name
Voting name
PIN (optional)

How many security controllers have been sold by Infineon in the last 10 years?

○ > 5 billion Votes: 3
○ > 10 billion Votes: 2
○ > 15 billion Votes: 4
● > 20 billion Votes: 3

Figure 5 Voting option: An example smart contract interaction with the blockchain security 2go card is demonstrated.

3.1 Drop-down menu

By opening the drop-down menu in the Homescreen, all necessary other features are demonstrated.

3.1.1 Refresh balance

As the name suggests, the refresh balance option refreshes the amount of tokens which are related to the particular key index. Thus a new query to the Blockchain is made and the value is refreshed below the Ethereum address. As illustrated in Figure 6, the procedure is also indicated.

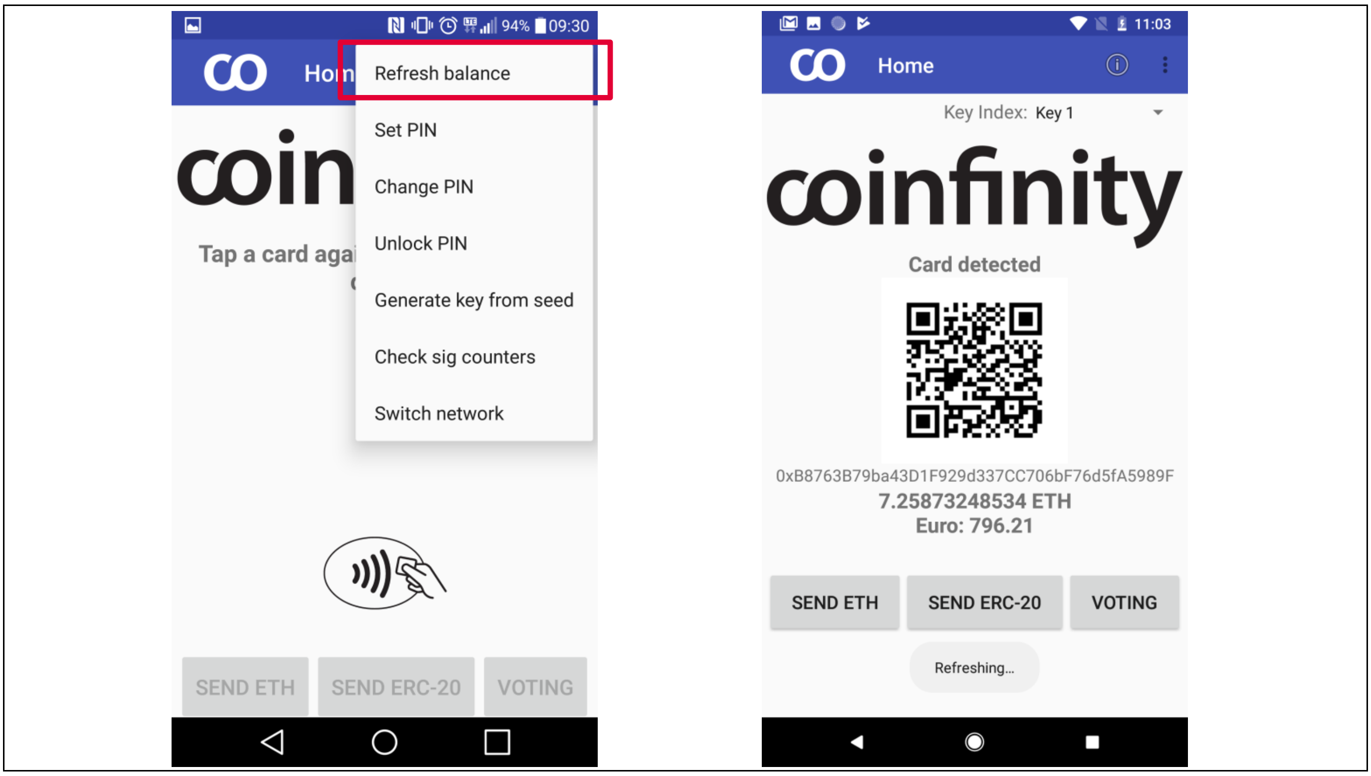
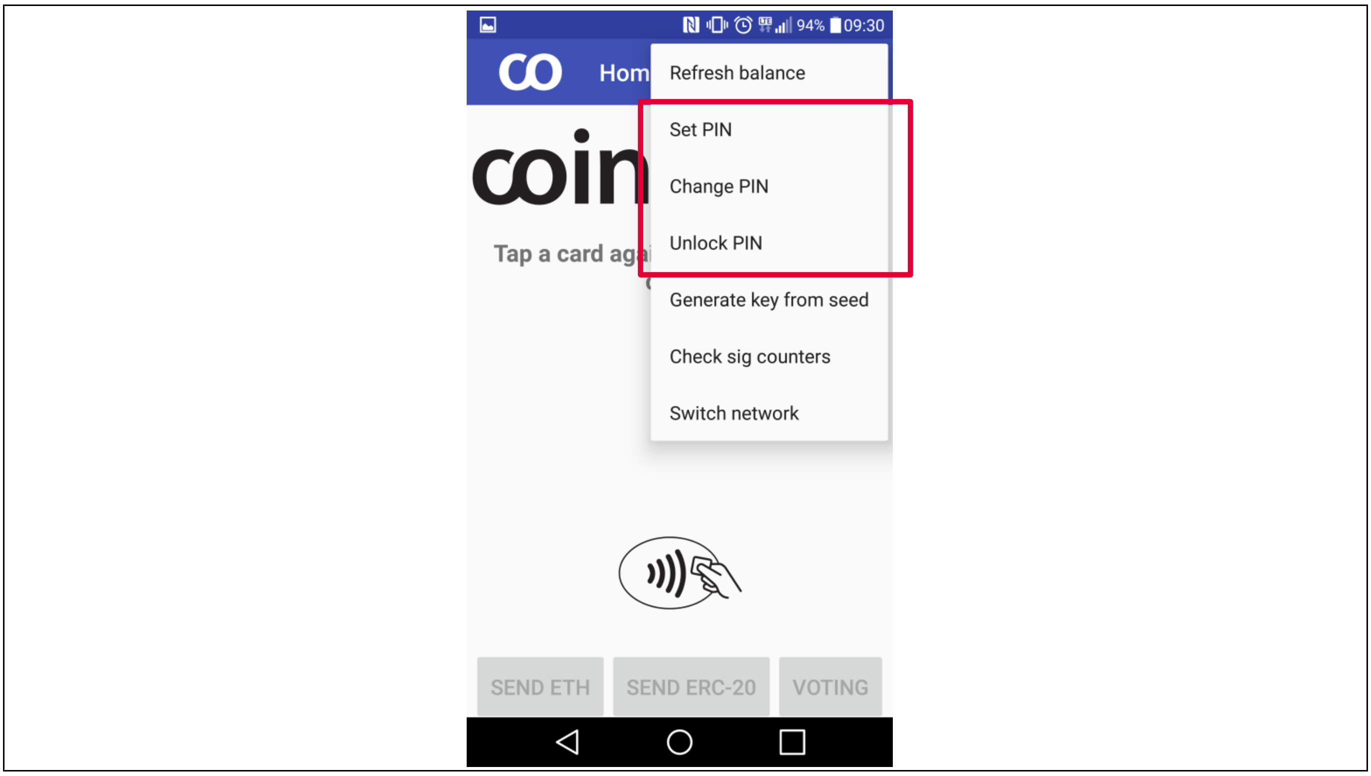
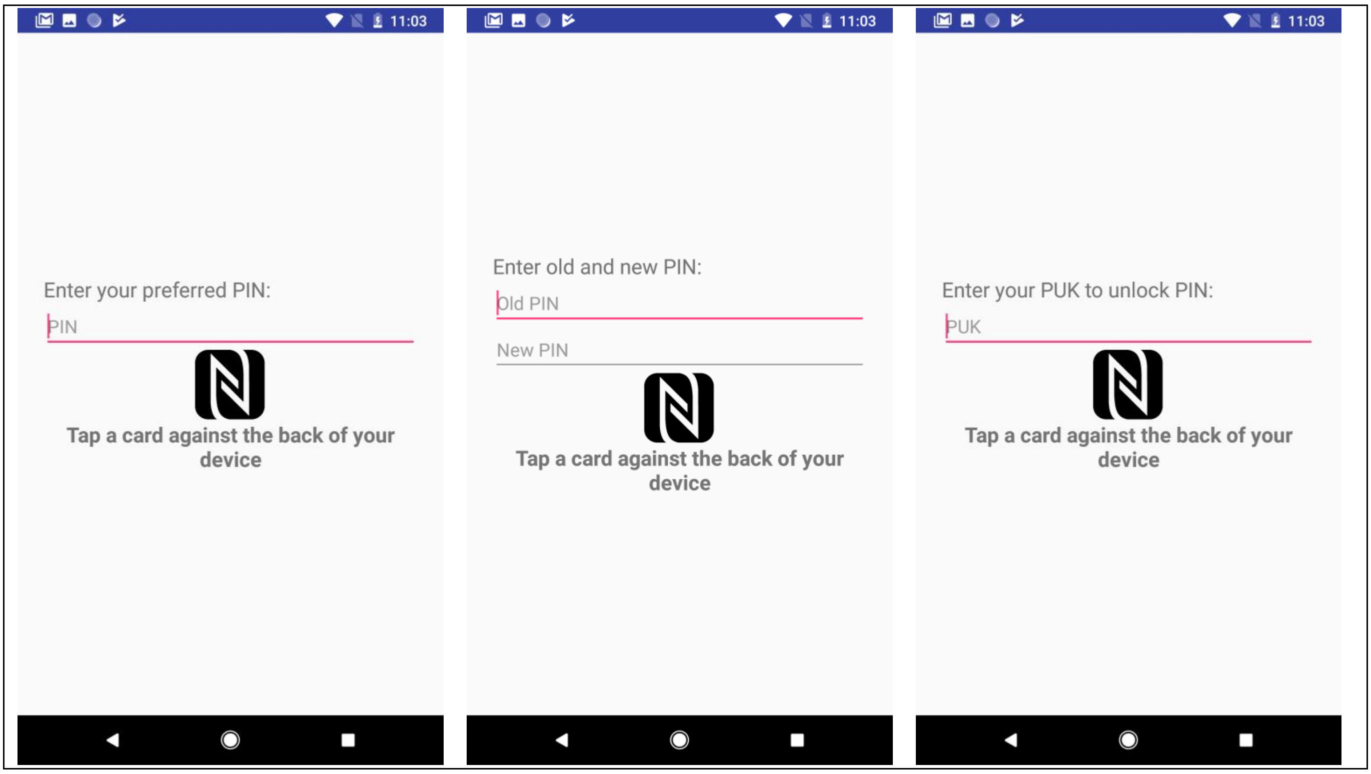


Figure 6 **Refresh balance option**

3.1.2 Set Pin, Change Pin, Unlock Pin

This option allows the setting a pin-protection for the card. After setting, the card functions are locked without using the pin. The PIN can be changed by using the option Change PIN. If the PIN is lost, a PUK can be entered.





11:03

Enter your preferred PIN:

PIN

Tap a card against the back of your device

11:03

Enter old and new PIN:

Old PIN

New PIN

Tap a card against the back of your device

11:03

Enter your PUK to unlock PIN:

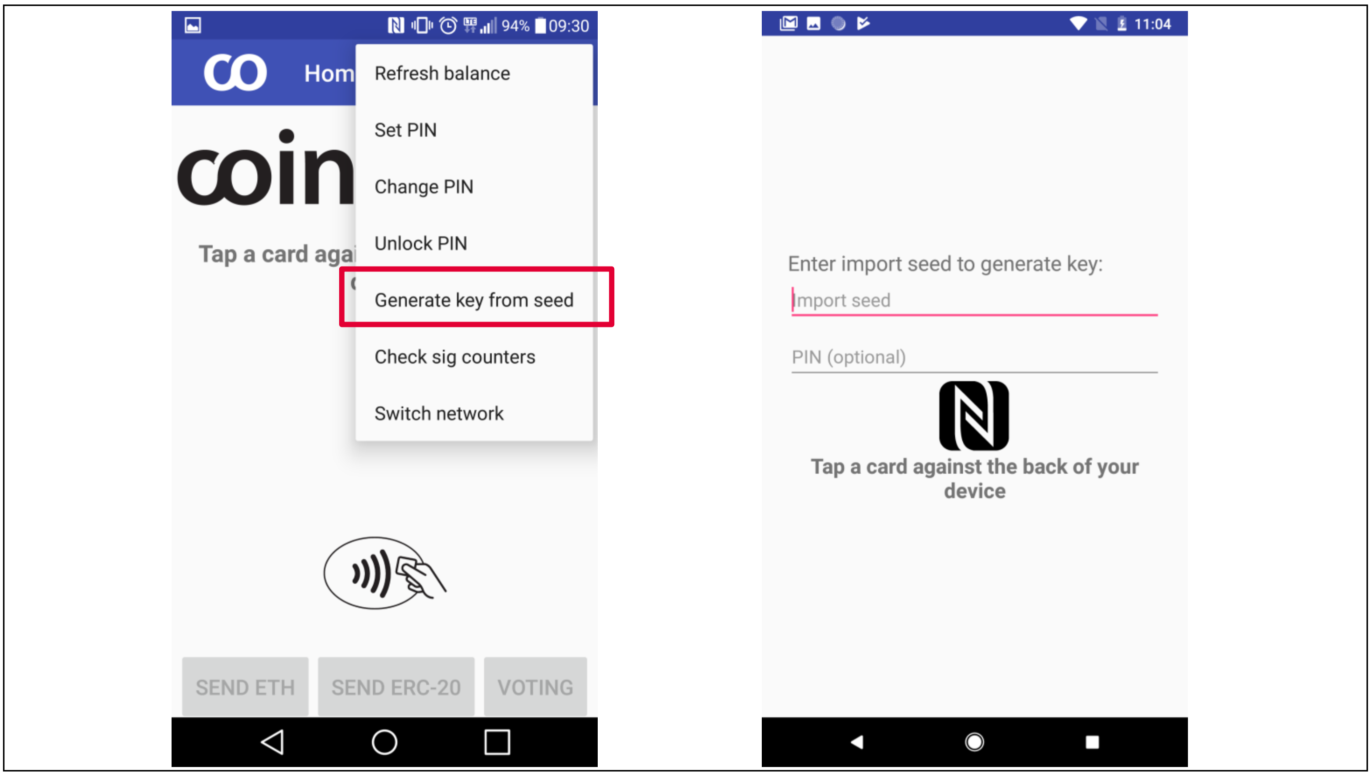
PUK

Tap a card against the back of your device

Figure 7 Set PIN: By setting a pin, the card functions locked and pin-protected

3.1.3 Generate Key from Seed

“Generate key from seed” enables the import option for key-index 0. Here a seed can be entered which is then used by the card to generate a new key. The key can be read out and is visualized with an Ethereum address in the homescreen by selecting key-index 0.



Tap a card agai

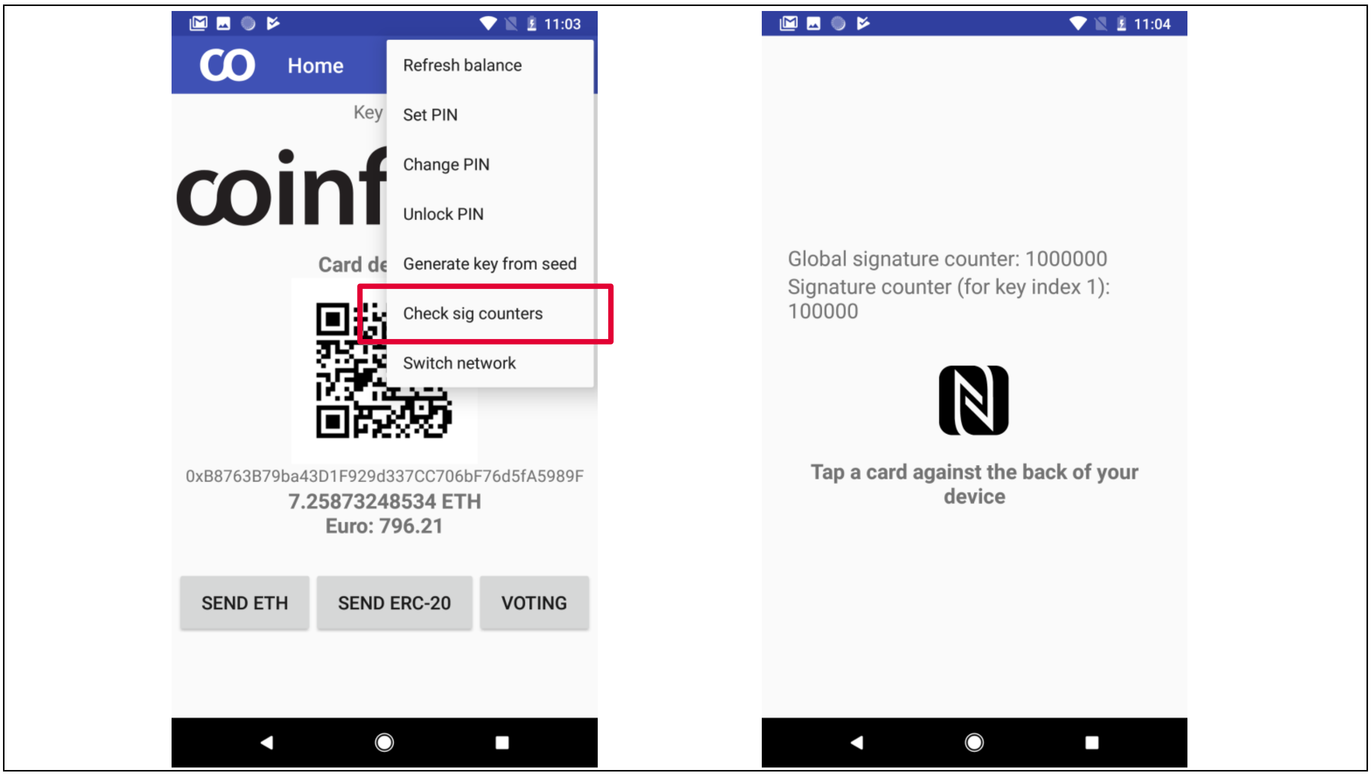
Enter import seed to generate key:

Tap a card against the back of your device

Figure 8 Generate key from seed: With this function a key is generated on the card based on the imported seed

3.1.4 Check sig counter

This option uses the expiring operations of the card. Here the signature counter of the particular key-index is read out and visualized.



0xB8763B79ba43D1F929d337CC706bF76d5fA5989F
7.25873248534 ETH
Euro: 796.21

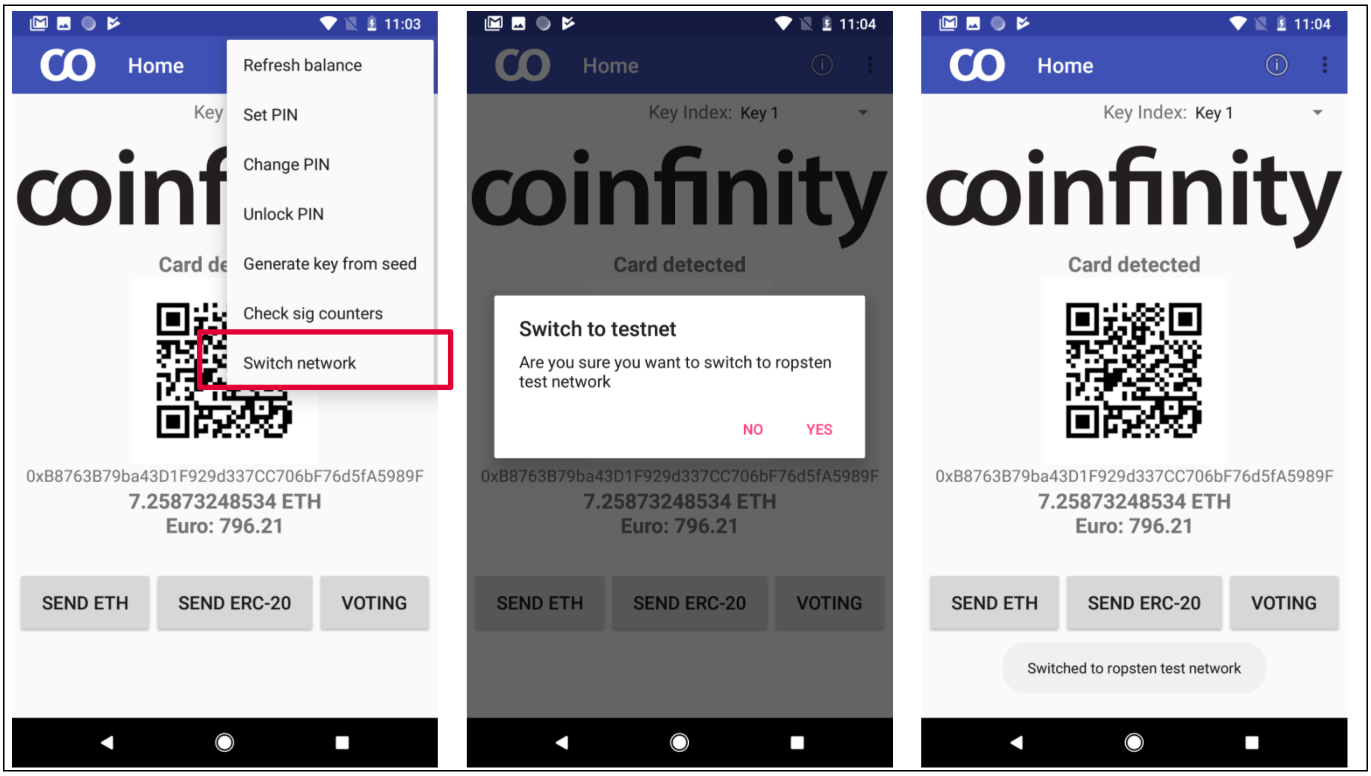
Global signature counter: 1000000
Signature counter (for key index 1): 100000

Tap a card against the back of your device

Figure 9 Key Index: The number of signatures which were used is visualized

3.1.5 Switching Network

Certainly not everyone wants to use the Ethereum mainnet in the first place. Therefore the app allows the switch to the robsten test network with the last option in the drop-down menu. As illustrated in Figure 10 the app confirms a successful switching between testnet and mainnet of the Ethereum blockchain.



Switch to testnet

Are you sure you want to switch to ropsten test network

0xB8763B79ba43D1F929d337CC706bF76d5fA5989F
7.25873248534 ETH
Euro: 796.21

Switched to ropsten test network

Figure 10 Switch to network: With this option you can switch between the Ethereum testnet and mainnet

4 References

[1] Web3j, https://github.com/web3j/web3j

[2] Android application example, https://play.google.com/store/apps/details?id=co.coinfinity.infineonandroidapp&rdid=co.coinfinity.infineonandroidapp

[3] infura.io API, https://infura.io/docs

[4] qr client google playstore, https://play.google.com/store/apps/details?id=com.google.zxing.client.android

[5] Barcode Scanner+, https://play.google.com/store/apps/details?id=com.srowen.bs.android

[6] Solidity documentation, https://solidity.readthedocs.io/en/latest/

[7] Truffle documentation, https://truffleframework.com/docs/

[8] Android Studio, https://developer.android.com/studio/

[9] Etherscan smart contract example, https://etherscan.io/address/0x2c680955cd340eae72703e6886957bf8465f9583

[10] Coinfinity GmbH, https://coinfinity.co/

[11] Metamask, https://metamask.io/

[12] MetaMask Ether Faucet, https://faucet.metamask.io/

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition yyyy-mm-dd

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: erratum@infineon.com

Document reference

IMPORTANT NOTICE
The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie") .

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer's products and any use of the product of Infineon Technologies in customer's applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS
Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.