

# Papers GmbH

## Cosmos Implementation Review

<b>Document Name:</b>	report_85589_Crypto_Currency_Protocol_Review_Cosmos_v1.0.docx
<b>Version:</b>	v1.0
<b>Project Number:</b>	85589
<b>Date of Delivery:</b>	January 24th, 2019
<b>Author:</b>	Lukasz Dykcik, Compass Security Schweiz AG
<b>Classification:</b>	STRICTLY CONFIDENTIAL

## Table of Contents

<b>1 OVERVIEW.....</b>	<b>3</b>
1.1 To the Reader.....	3
1.2 Document Structure.....	3
<b>2 OVERALL STATEMENT.....</b>	<b>4</b>
2.1 Goals and Methodology.....	4
2.2 Results.....	4
2.3 Disclaimer.....	4
<b>3 VULNERABILITIES AND REMEDIATION.....</b>	<b>5</b>
3.1 Cosmos Tests.....	5
<b>4 COSMOS TESTS.....</b>	<b>6</b>
4.1 Test #1.....	6
4.2 Test #2.....	8
4.3 Test #3.....	9
4.4 Test #4.....	10
4.5 Test #5.....	11
4.6 Test #6.....	12
4.7 Test #7.....	13
4.8 Test #8.....	15
4.9 Test #9.....	16
4.10 Test #10.....	17
4.11 Test #11.....	18
<b>5 APPENDIX.....</b>	<b>20</b>
5.1 Compass Weaknesses Rating.....	20
5.1.1 What the rating IS NOT.....	20
5.1.2 What to do with the weaknesses table.....	20
5.1.3 Examples.....	20
5.1.4 Tests with result "INFO" and N/A.....	20
5.2 Recheck Coloring.....	21

# 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 usage of Cosmos cryptocurrency on the AirGap Vault mobile application. 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	Overall statement explaining the outcome of the security tests
3	A list of the detected weaknesses as well as suggestions for improvement
4	Protocol of the performed security tests
5	Appendix

## 2 Overall Statement

In January 2020, Compass Security tested the implementation of the Cosmos protocol during a 2-person-day timespan. No critical vulnerabilities have been found, only a few security hardening possibilities. In order to achieve a high security standard, it is recommended to apply the proposed recommendations.

### 2.1 Goals and Methodology

The goal of the project was to find vulnerabilities in the implementation of the Cosmos protocol. The focus of the tests was put on attack vectors that may result in the user of the application losing his funds.

The tests were performed on the Android application v3.0.0 compiled on 20<sup>th</sup> December 2019. For the tests, the Cosmos cosmoshub-3 blockchain was used. During the tests, access to the source code of the application was granted as well.

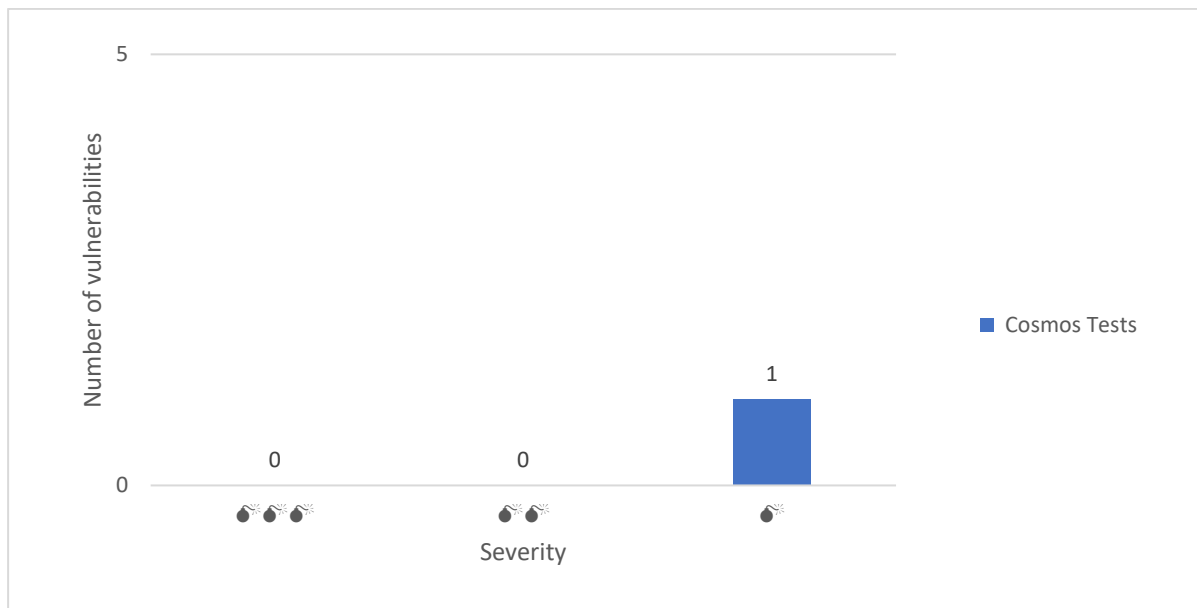
### 2.2 Results

During the tests, no attack vector that would allow an attacker to steal money from a careful user of the AirGap Vault application was found. The application accepts only a single type of potentially untrusted input, that is the serialized transaction to approve. The serialized transaction contains parameters that will be used for creating the actual transaction inside the application. The provided parameters are checked by the application before they are used, therefore, it was not possible to change the unit of the transaction value nor to set an unexpected transaction type.

Although no security issue was found, there are a few aspects of the application that could be improved. The type of operations in a transaction should be clearly visible to the user. Currently the user needs to read extra transaction details to figure out what type of transaction he signs.

Moreover, there is a bug in the transaction fee calculation. If a transaction contains multiple operations, the fee will be shown much larger than it will be actually.

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



Compass Security recommends addressing all issues listed in the vulnerability table in section 3 according to their rating. Vulnerabilities with a high severity should be addressed as soon as possible. Medium- and low-rated vulnerabilities can be mitigated in the medium term.

### 2.3 Disclaimer


This statement is applicable to the application as tested during the project. The application may have undergone changes since.

### 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 <b>INFO</b> : Not security relevant issue  <i>See section 5.1 for detailed description.</i>	

#### 3.1 Cosmos Tests

No.	Reference	Weakness	Threat	Remediation	Rating	Comment
1.	4 #7	<b>Operation Type Ambiguity</b>  The type of operations in the transaction is shown only in the extra transaction details.	As there is no clear indication what transaction a user is going to approve, a user may sign for example a transaction with spend operations instead of delegate.	Introduce an easily noticeable difference between different types of operations to avoid user confusion.		
2.	4 #3	<b>Multiple Values for a Single Operation</b>  According to how the application handles unsigned transaction, it is possible to put an array of values for the same operation. The value shown to the user is the sum of values.	Transactions containing operations with multiple values are not valid in the blockchain thus no security issues of such behavior were identified.	Unless there is a special purpose for parsing operations with multiple values, the application should accept only transactions containing a single value in each operation.	<b>INFO</b>	
3.	4 #11	<b>Improper Fee Calculation</b>  Transactions with multiple operations have improperly displayed transaction fee. Instead of showing a single fee for the entire transaction, the fee is shown for each operation. As a result, the total fee is higher than in reality.	-	Correct the displayed transaction fee by not multiplying the fee by the number of operations in the transaction.	<b>INFO</b>	

## 4 Cosmos Tests

### 4.1 Test #1

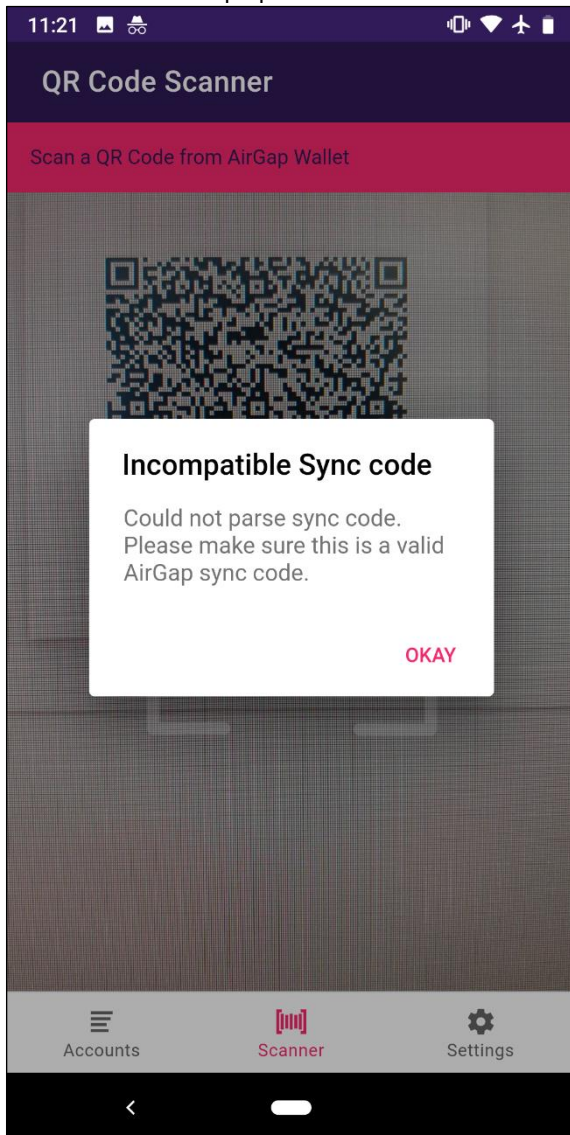
No.	Description of Test	Expected Result	Actual Result	PASS FAIL
1.	Is it possible to modify the denomination of the transaction in a way that the incorrect amount will be shown to the user?	No.	No, other denominations than <code>uatom</code> cannot be used.	<b>PASS</b>

#### Details #1

The following payload is used, where the denomination is changed from `uatom` to `atom`:

```
[b'2', b'0', [[b'0', b'5', b'cosmos', [b'airgap-wallet://?d=',
b'039f63dbe4d9548aa196847c91bb2bb9346f292ae99a76251b1c61234e451beb02', [b'11032',
b'cosmoshub-3', [[b'5000', b'uatom']], b'200000'], b'', [[b'12', b'atom']],
b'cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzjsm',
b'cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7', b'0']], b'4']]]]
```

A transaction with improper denomination cannot even be scanned:



In the source code, it was confirmed that only `uatom` can be used as a valid denomination:

```
export interface CosmosCoinJSON {
  denom: string
  amount: string
}

export class CosmosCoin implements JSONConvertible, RPCConvertible {
  private static supportedDonominations = ['uatom']
  public readonly denom: string
  public readonly amount: string

  constructor(denom: string, amount: string) {
    this.denom = denom
    this.amount = amount
  }

  public toJSON(): CosmosCoinJSON {
    return {
      amount: this.amount,
      denom: this.denom
    }
  }

  public static fromJSON(json: CosmosCoinJSON): CosmosCoin {
    if (!CosmosCoin.supportedDonominations.includes(json.denom)) {
      throw new Error('Unsupported cosmos denomination')
    }
    return new CosmosCoin(json.denom, json.amount)
  }
}
```

## 4.2 Test #2

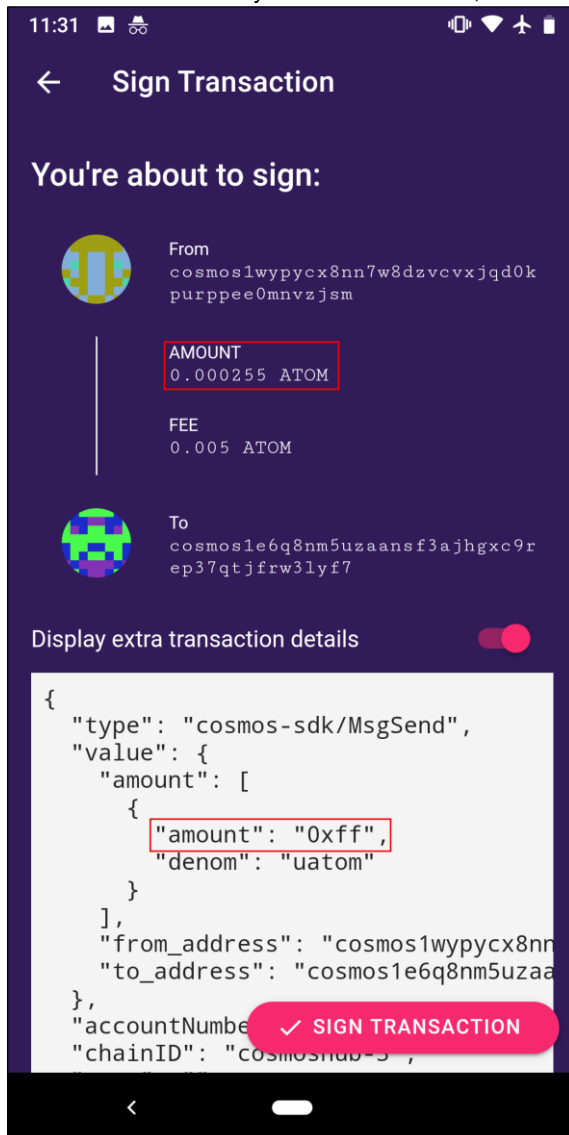
No.	Description of Test	Expected Result	Actual Result	PASS FAIL
2.	Is it possible to put characters different than digits in the transaction value field?	No.	It is possible to put a value in a hexadecimal or exponential notation. However, the user sees always the value in decimal. If the provided value cannot be decoded, the transaction value shown to the user is empty.	PASS

### Details #2

A payload with transaction value as a hexadecimal string:

```
[b'2', b'0', [[b'0', b'5', b'cosmos', [b'airgap-wallet://?d=',
b'039f63dbe4d9548aa196847c91bb2bb9346f292ae99a76251b1c61234e451beb02', [b'11032',
b'cosmoshub-3', [[b'5000', b'uatom']], b'200000'], b'', [[[[b'0xff', b'uatom']],
b'cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzjsm',
b'cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7', b'0']], b'4']]]]]]
```

A decimal value is always shown to the user, in the extra details he can see the actual unconverted value:



Nevertheless, such transactions are considered invalid in the blockchain.



### 4.3 Test #3

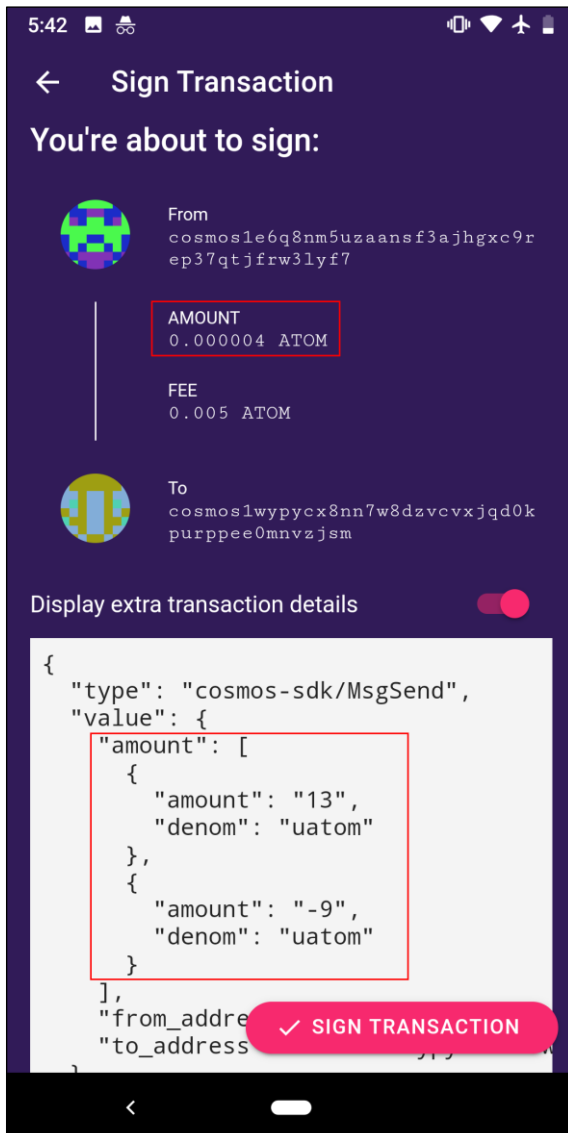
No.	Description of Test	Expected Result	Actual Result	PASS FAIL
3.	Is it possible to put multiple transaction values for a single transaction?	No.	Yes, it is possible to put multiple values and the amount shown to the user will represent the sum of those values.	INFO

#### Details #3

A transaction with two values, one is negative:

```
[b'2', b'0', [[b'0', b'5', b'cosmos', [b'airgap-wallet://?d=', b'03b41f590f719357b3c403ab932674f1b718e2038f8176ea8b60ba03b19a0d56b5', [b'20335', b'cosmoshub-3', [[b'5000', b'uatom']], b'200000'], b'', [[b'13', b'uatom'], [b'-9', b'uatom']], b'cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7', b'cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzjsm', b'0']], b'29']]]]
```

The user will see amount of the transaction as the sum of all values, however, in the extra details he can see each of the values:



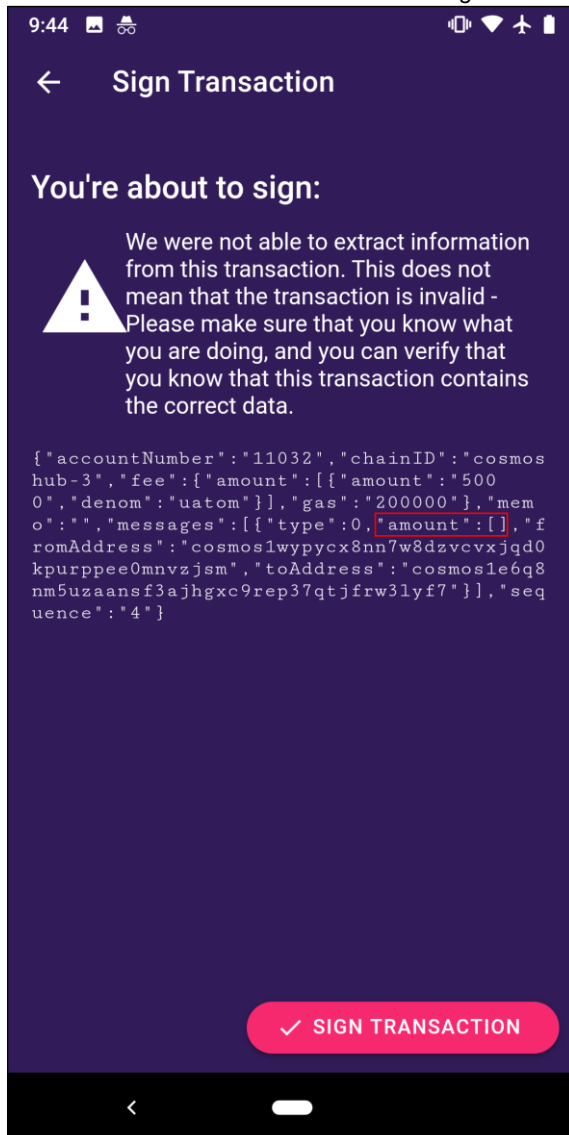
Such transactions with two values, even if both values are positive are not valid in the blockchain.

#### 4.4 Test #4

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
4.	Is it possible to specify a transaction with no value field?	No.	As expected.	PASS

#### Details #4

A transaction with no value field is not recognized as valid:



## 4.5 Test #5

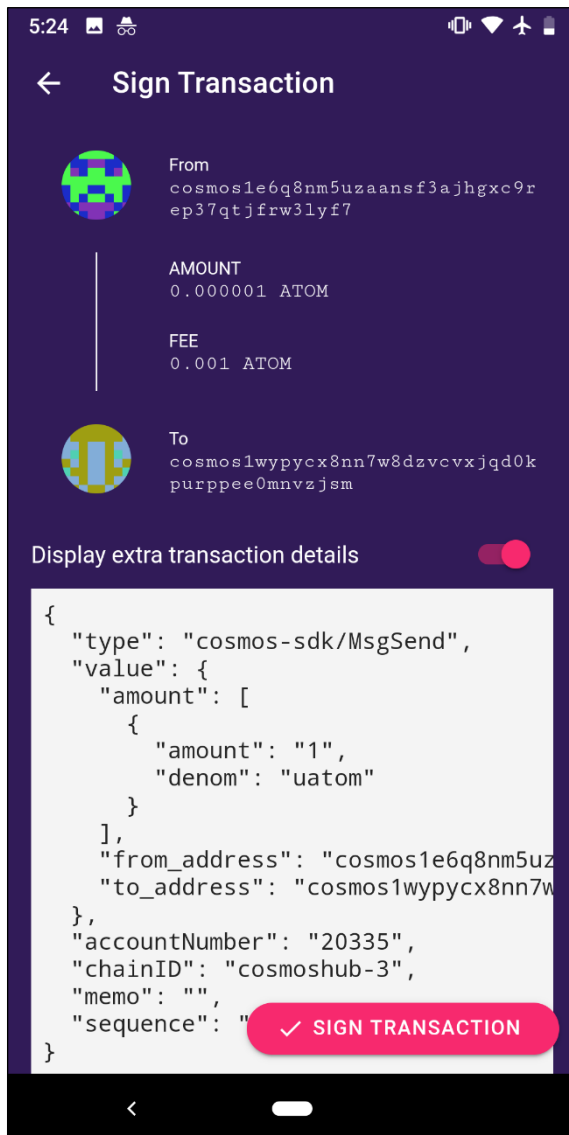
No.	Description of Test	Expected Result	Actual Result	PASS FAIL
5.	Is it possible to create a transaction where an incorrect fee is shown to the user?	No.	No, similar kind of attacks were tried as when attempting to manipulate the transaction value. Either the manipulated transaction was not scannable or it was invalid in the blockchain.	PASS

### Details #5

A transaction with added second transaction value:

```
[b'2', b'0', [[b'0', b'5', b'cosmos', [b'airgap-wallet://?d=',
b'03b41f590f719357b3c403ab932674f1b718e2038f8176ea8b60ba03b19a0d56b5', [b'20335',
b'cosmoshub-3', [[b'500', b'uatom'], [b'500', b'uatom']], b'200000'], b'', [[b'1',
b'uatom']], b'cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7',
b'cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzjsm', b'0']], b'32']]]]
```

The user sees the sum of values shown as the fee. Transaction details do not show the fee field:



Nevertheless, a transaction with two fee values is not valid in the blockchain. Specifying another unit for the fee resulted in a transaction that could not be scanned.

## 4.6 Test #6

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
6.	Is it possible to trick user into signing a transaction that will be valid for another blockchain?	No.	The application does not check whether the specified blockchain id matches the expected one: cosmoshub-3. However, the user is able to see the chainID field in the extra transaction details and currently such transactions cannot be valid.	PASS

### Details #6

Representation of unsigned transaction for cosmoshub-3:

```
[b'2', b'0', [[b'0', b'5', b'cosmos', [b'airgap-wallet://?d=',
b'03b41f590f719357b3c403ab932674f1b718e2038f8176ea8b60ba03b19a0d56b5', [b'20335',
b'cosmoshub-3', [[b'500', b'uatom']], b'200000'], b'', [[b'1', b'uatom']],
b'cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7',
b'cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzjsm', b'0']], b'33']]]]
```

A signed transaction intended to be sent to cosmoshub-3 blockchain:

```
[b'2', b'0', [[b'0', b'6', b'cosmos', [b'0d56b5', b'{"tx":{"msg":[{"type":"cosmos-
sdk/MsgSend","value":{"amount":[{"amount":"1","denom":"uatom"}],"from_address":"cosmos1e6q8n
m5uzaansf3ajhgxc9rep37qtjfrw3lyf7","to_address":"cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzj
sm"}]},"fee":{"amount":[{"amount":"500","denom":"uatom"}],"gas":"200000"},"signatures":[{"si
gnature":"41IRPFdmWg/NtOiiPukw1YUy4TlqbQkZKhWmWhtvscNbUaDuj756Gq8800FQsIJpBpt3p1t84gMJshk7KJ
qjYg==","pub_key":{"type":"tendermint/PublicKeySecp256k1","value":"A7QfWQ9xklezxAOrkyZ08bcY4gOP
gXbqi2C6A7GaDVal"}]},"memo":"","mode":"sync"}]]]]]
```

After changing the blockchain id in the unsigned transaction, the transaction can still be scanned and signed:

```
[b'2', b'0', [[b'0', b'5', b'cosmos', [b'airgap-wallet://?d=',
b'03b41f590f719357b3c403ab932674f1b718e2038f8176ea8b60ba03b19a0d56b5', [b'20335',
b'cosmoshub-2', [[b'500', b'uatom']], b'200000'], b'', [[b'1', b'uatom']],
b'cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7',
b'cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzjsm', b'0']], b'33']]]]
```

The signature is different than previously. This transaction is not accepted by the blockchain; thus, it is possible to use the application to sign transactions for other blockchain than intended cosmoshub-3: Nevertheless, the user has always a possibility to verify the chainID field in extra transaction details.

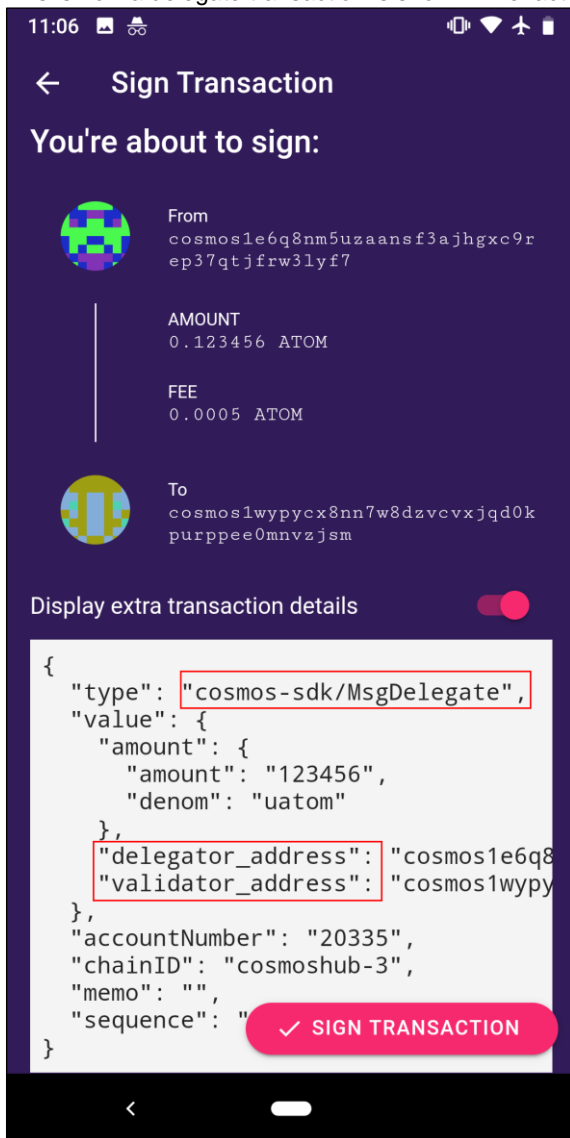
```
[b'2', b'0', [[b'0', b'6', b'cosmos', [b'0d56b5', b'{"tx":{"msg":[{"type":"cosmos-
sdk/MsgSend","value":{"amount":[{"amount":"1","denom":"uatom"}],"from_address":"cosmos1e6q8n
m5uzaansf3ajhgxc9rep37qtjfrw3lyf7","to_address":"cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzj
sm"}]},"fee":{"amount":[{"amount":"500","denom":"uatom"}],"gas":"200000"},"signatures":[{"si
gnature":"SmC/6qlOx8wetZpualhc+v3bxcjxp7TjJBaaZr6S/AYNUJfCvScCKpuYFGsqVzHTkfHGGMtWUHeP5SE+Yb
PgUQ==","pub_key":{"type":"tendermint/PublicKeySecp256k1","value":"A7QfWQ9xklezxAOrkyZ08bcY4gOP
gXbqi2C6A7GaDVal"}]},"memo":"","mode":"sync"}]]]]]
```

## 4.7 Test #7

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
7.	Is it possible to trick the user into signing a spending transaction while he intended to approve a delegate or undelegated transaction?	No.	The only difference between spending and delegating transaction is present in the extra transaction details. No easily noticeable indication of transaction type is present.	<b>FAIL</b>

### Details #7

This is how a delegate transaction is shown. The fact that its type delegate is present in the extra details only:





## 4.8 Test #8

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
8.	Is it possible to create a transaction of an unsupported type that would be shown to the user as one of the supported types?	No.	No, only MsgSend, MsgDelegate, MsgUndelegate and MsgWithdrawDelegationReward types are supported. Scanning a transaction with a different type causes an error.	<b>PASS</b>

### Details #8

The source code provides an overview of what transactions are supported. Scanning a transaction of another type is not possible:

```
export enum CosmosMessageTypeIndex {
  SEND = 0,
  DELEGATE = 1,
  UNDELEGATE = 2,
  WITHDRAW_DELEGATION_REWARD = 3
}
[CUT BY COMPASS]

constructor(index: CosmosMessageTypeIndex) {
  this.index = index
  switch (index) {
    case CosmosMessageTypeIndex.SEND:
      this.value = 'cosmos-sdk/MsgSend'
      break
    case CosmosMessageTypeIndex.DELEGATE:
      this.value = 'cosmos-sdk/MsgDelegate'
      break
    case CosmosMessageTypeIndex.UNDELEGATE:
      this.value = 'cosmos-sdk/MsgUndelegate'
      break
    case CosmosMessageTypeIndex.WITHDRAW_DELEGATION_REWARD:
      this.value = 'cosmos-sdk/MsgWithdrawDelegationReward'
      break
    default:
      throw new Error('Unknown message type')
  }
}
```

## 4.9 Test #9

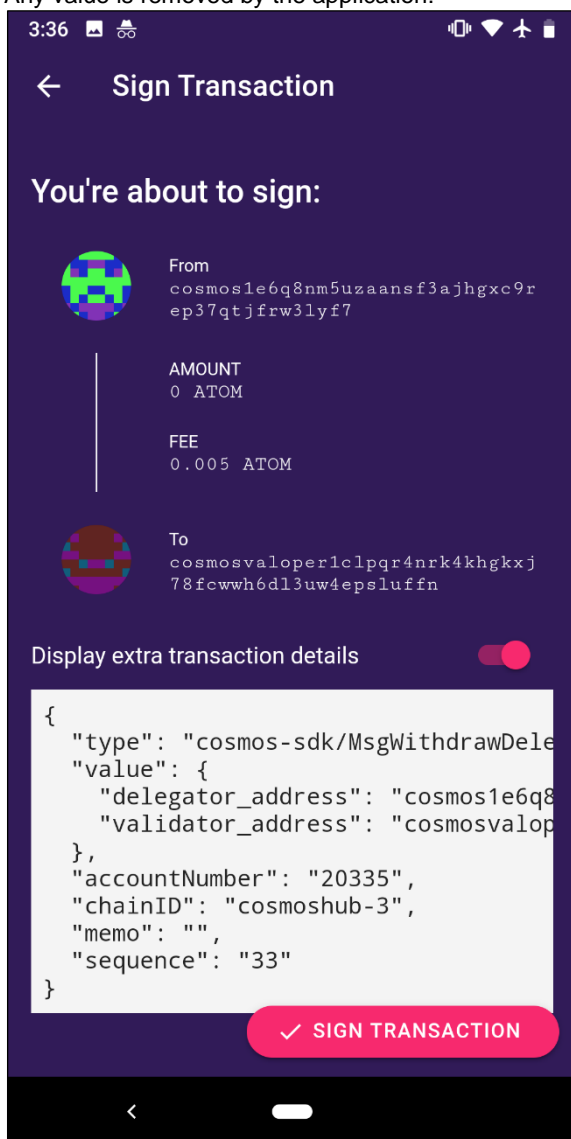
No.	Description of Test	Expected Result	Actual Result	PASS FAIL
9.	Is it possible to put value into the reward withdrawal transaction?	If the user is able to see what he signs then it may be possible.	No, it is possible to specify the value in the unsigned transaction but during parsing the value is set to 0.	<b>PASS</b>

### Details #9

Reward withdrawal transaction with specified value:

```
[b'2', b'0', [[b'0', b'5', b'cosmos', [b'airgap-wallet://?d=',
b'03b41f590f719357b3c403ab932674f1b718e2038f8176ea8b60ba03b19a0d56b5', [b'20335',
b'cosmoshub-3', [[b'5000', b'uatom']], b'200000'], b'', [[[[b'123', b'uatom']],
b'cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7',
b'cosmosvaloper1clpqr4nrk4khgkxj78fcwwh6dl3uw4epsluffn', b'3']], b'33']]]]]]
```

Any value is removed by the application:





## 4.10 Test #10

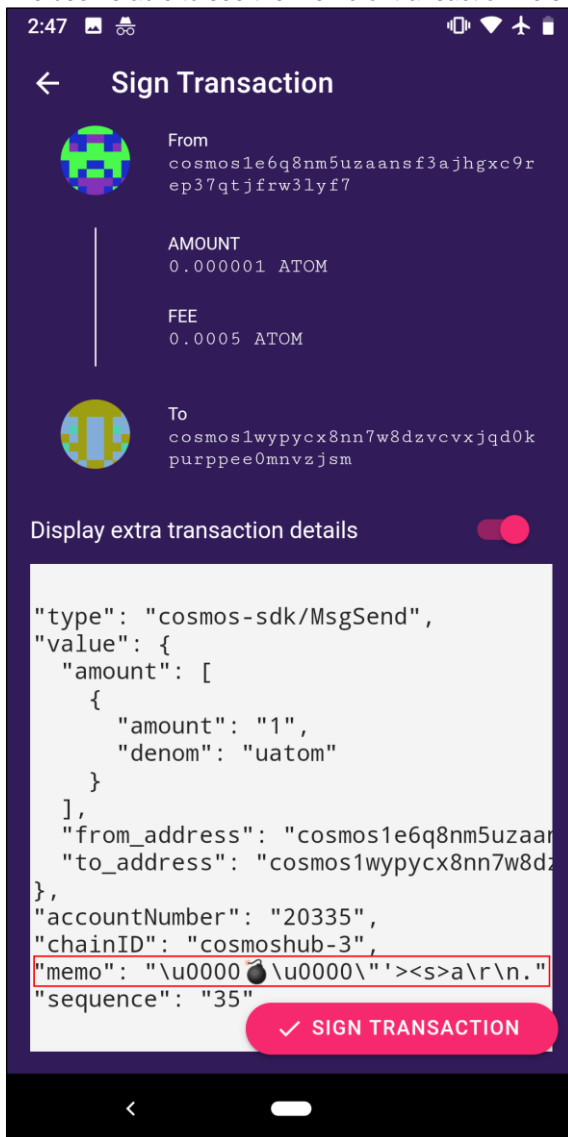
No.	Description of Test	Expected Result	Actual Result	PASS FAIL
10.	Do special characters in the memo field of the transaction cause problems during displaying it?	No.	No encoding issues were found. It was not possible to cause any ambiguity when the transaction is displayed.	PASS

### Details #10

A transaction with special characters in the memo field:

```
[b'2', b'0', [[b'0', b'5', b'cosmos', [b'airgap-wallet://?d=',
b'03b41f590f719357b3c403ab932674f1b718e2038f8176ea8b60ba03b19a0d56b5', [b'20335',
b'cosmoshub-3', [[b'5000', b'uatom']], b'200000'],
b'\x00\xF0\x9F\x92\xA3\x00'\><s>a\x0d\x0a.', [[b'1', b'uatom']],
b'cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7',
b'cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzjsm', b'0']], b'35']]]]
```

The user is able to see the memo of transaction he signs, however the memo string is properly shown, no injection was found.



A transaction with special characters in the memo could be signed but was not accepted by the blockchain.

## 4.11 Test #11

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
11.	Is it possible to put multiple operations in a single transaction?	If all operations are clearly presented to the user before he approves the transaction, then it is not an issue.	All operations are shown to the user; however, the total fee is calculated improperly. The fee shown to the user is the transaction fee multiplied by the number of operations.	INFO

### Details #11

The following transaction including three operations is used:


```
[b'2', b'0', [[b'0', b'5', b'cosmos', [b'airgap-wallet://?d=',
b'03b41f590f719357b3c403ab932674f1b718e2038f8176ea8b60ba03b19a0d56b5', [b'20335',
b'cosmoshub-3', [[b'5000', b'uatom']], b'800000'], b'', [[b'1', b'uatom']],
b'cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7',
b'cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzjsm', b'0'], [[b'2', b'uatom']],
b'cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7',
b'cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzjsm', b'0'], [[b'99', b'uatom']],
b'cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7',
b'cosmosvaloper1clpqr4nrk4khgkxj78fcwwh6dl3uw4epspluffn', b'1']], b'34']]]]
```

The above transaction can be signed and is valid in the blockchain:


### TRANSACTION DETAILS

#### Information


TxHash	51D2F69EDC76BD0A852E91C75800220DE04C96C760E46C897909A0EEDB593A76
Status	✓ Success
Height	451376
Time	34s ago ( 2020-01-17 13:59:09 )
Fee	0.005000 ATOM
Gas ( used / wanted )	155,852 / 800,000


**IOV Name Service.** Secure and fast name service.  
The IOV Name Service provides a human readable address instead of blockchain addresses to receive any kind of crypto-currencies.
[Explore](#)


#### Msgs

 Send

From	cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7
To	cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzjsm
Amount	0.000001 ATOM

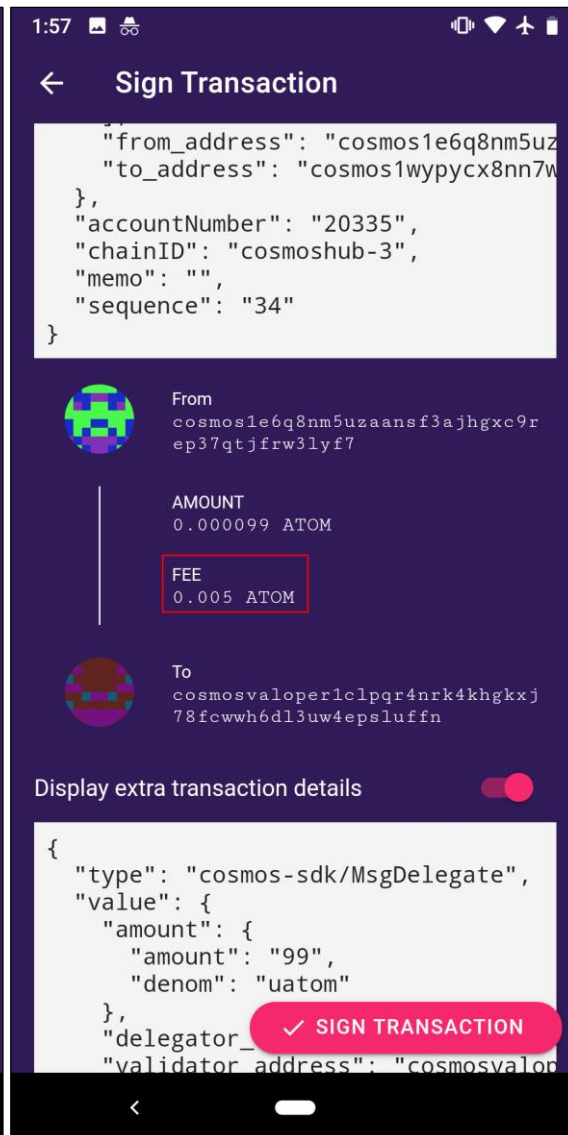
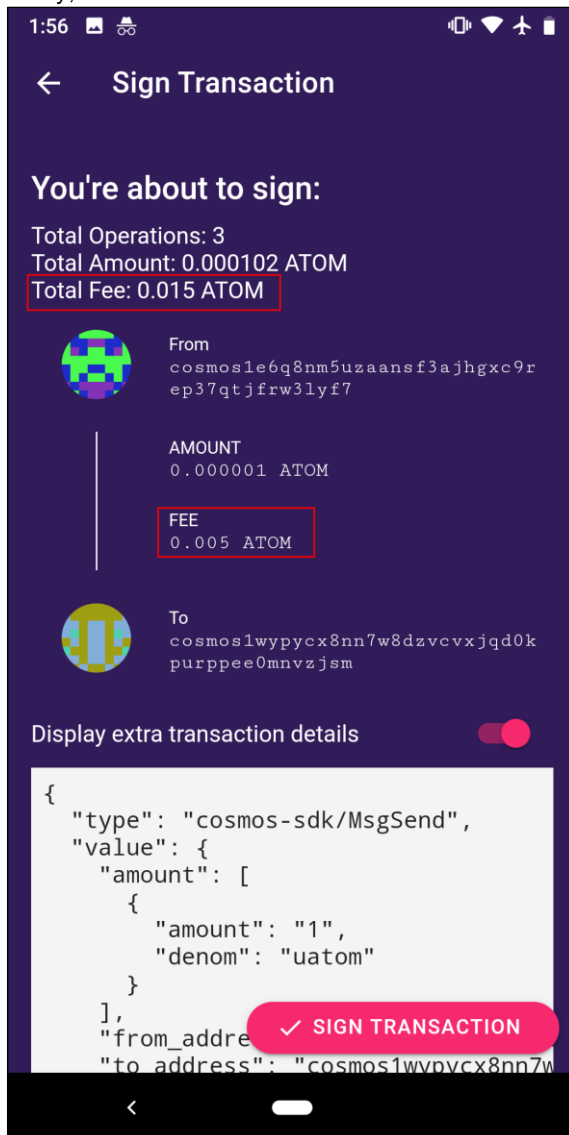
 Send

From	cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7
To	cosmos1wypycx8nn7w8dzvcvxjqd0kpurppee0mnvzjsm
Amount	0.000002 ATOM

 Delegate

Delegator	cosmos1e6q8nm5uzaansf3ajhgxc9rep37qtjfrw3lyf7
Validator	cosmosvaloper1clpqr4nrk4khgkxj78fcwwh6dl3uw4epspluffn (Cosmostation)
Delegation Amount	0.000099 ATOM

Before signing it, the user was able to see all three operations as well as their details, similarly as in case of transactions containing a single operation. However, the total fee is shown as the transaction fee multiplied by the number of operations. In reality, the entire transaction fee is 0.005 ATOM.



## 5 Appendix

### 5.1 Compass Weaknesses Rating

Please read this section to understand the Compass weaknesses rating.

#### 5.1.1 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.

#### 5.1.2 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.

#### 5.1.3 Examples

Rating	Severity	Examples
 High	<ul style="list-style-type: none"> <li>▪ Exploitation is easy and leads to high privileges and/or affects many users.</li> <li>▪ System can be controlled with little effort</li> <li>▪ High impact if vulnerability is disclosed</li> </ul> <p>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.</p>	<ul style="list-style-type: none"> <li>▪ SQL Injection or Cross-Site Scripting (XSS)</li> <li>▪ Privilege escalation vulnerabilities</li> <li>▪ Remote shell vulnerabilities</li> <li>▪ Authorization bypass vulnerabilities</li> <li>▪ Default accounts with high privileges</li> <li>▪ Security filter bypass</li> <li>▪ Weak encryption ciphers or protocols</li> <li>▪ Phone in surveillance mode</li> <li>▪ XML External Entity (XXE)</li> </ul>
 Medium	<ul style="list-style-type: none"> <li>▪ Exploitation can lead to higher privileges if combined with other weaknesses</li> <li>▪ Exploitation requires significant effort</li> </ul> <p>Fix should be implemented in a reasonable time.</p>	<ul style="list-style-type: none"> <li>▪ Exposed management interfaces</li> <li>▪ Caching of sensitive data</li> <li>▪ Denial-of-Service conditions</li> <li>▪ Insecure cookie settings</li> <li>▪ Disclosure of usernames, email-addresses</li> <li>▪ Large attack surface due to open ports</li> </ul>
 Low	<ul style="list-style-type: none"> <li>▪ Abuse does not lead to higher privileges</li> <li>▪ Information disclosure vulnerabilities</li> </ul> <p>Can be solved in the long term.</p>	<ul style="list-style-type: none"> <li>▪ Disclosure of product and version (banners)</li> <li>▪ Default pages and samples</li> <li>▪ DNS zone transfer</li> <li>▪ DNS reverse lookups</li> </ul>
<b>INFO</b>	Just an informational point without security relevant implications.	<ul style="list-style-type: none"> <li>▪ Usability and performance issues</li> <li>▪ Developer and staging bugs</li> <li>▪ Clean-up notes</li> </ul>

#### 5.1.4 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

## 5.2 Recheck Coloring

The following color code is used for pointing out, whether a previously identified vulnerability is solved, partly solved, not solved, no recheck conducted or if new vulnerabilities have been found.

Lavender	Red	Yellow	Green	Gray
A new vulnerability was found.	Vulnerability still exists.	Vulnerability was partially eliminated.	Vulnerability was eliminated.	No recheck conducted.