

# SPC Authenticator User Guide Manual

Version	Date	Note
V0.0	2020.08.10	Original version (HF)
V1.0	2020.09.27	Revised version

SPC Authenticator is developed based on the Google Authenticator. Compared to the Google Authenticator, we add an RSA encryption mechanism, improving the security of our multisignature transactions for SpaceChain corporate users.

There are two main functions in the SPC Authenticator: 1) RSA encryption and 2) OTP generation. We will describe these two functions in detail.

Please refer to the link below for the Google Authenticator:

<https://github.com/google/google-authenticator-android>

SPC Authenticator can be downloaded from the address below:

[https://github.com/spacechain/opensource\\_otp\\_app](https://github.com/spacechain/opensource_otp_app)

# **1.RSA Tools**

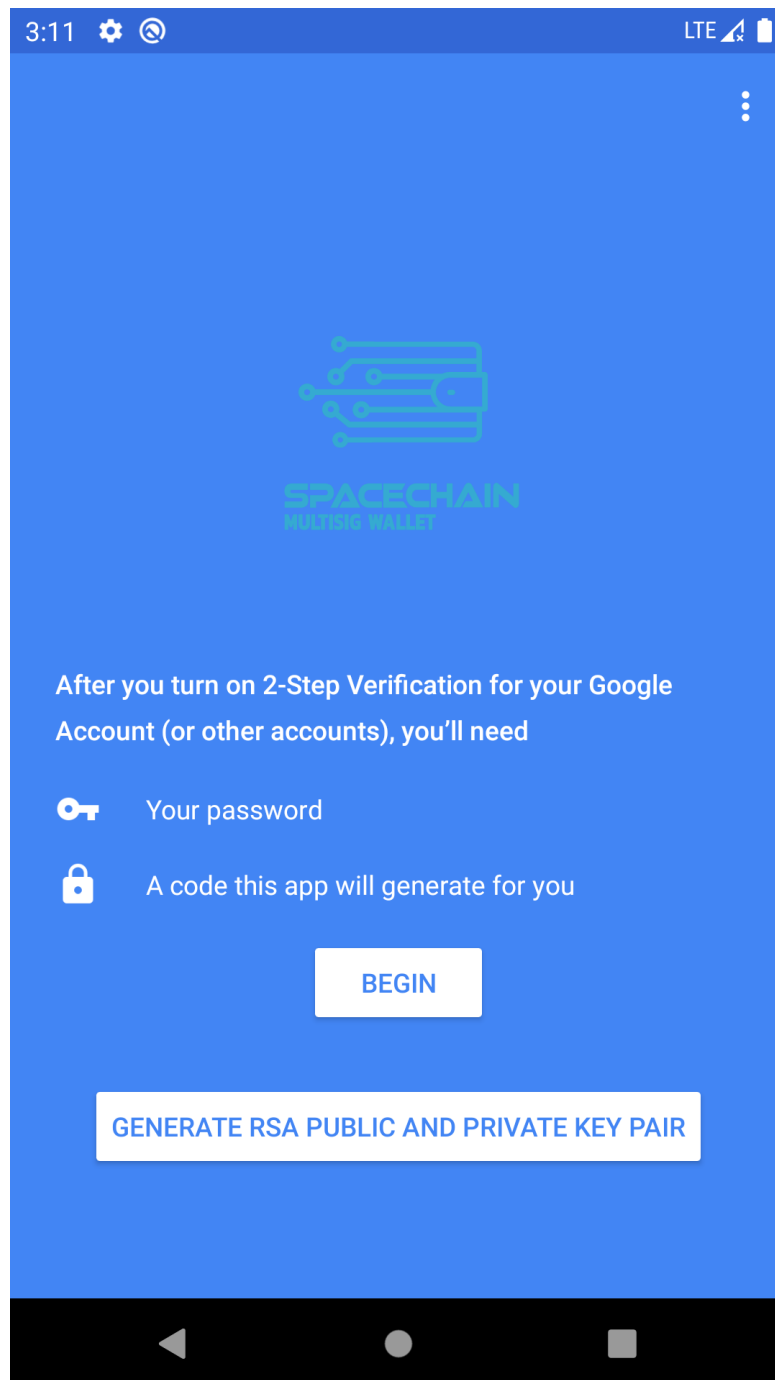
## **Introduction**

During the account registration, users need to provide the TX information of BTC or SPC token, and the RSA public key. After the TX information has been verified by SpaceChain, SPC payload will encrypt the OTP with the RSA public key, the encrypted OTP ciphertext will be sent to users via email. Users can then decrypt the ciphertext and obtain the OTP key.

Obtaining the RSA public key and decrypting ciphertext can be done through RSA Tools in the SPC Authenticator.

## **Obtain RSA public key**

Click “Generate RSA public and private key pair”.

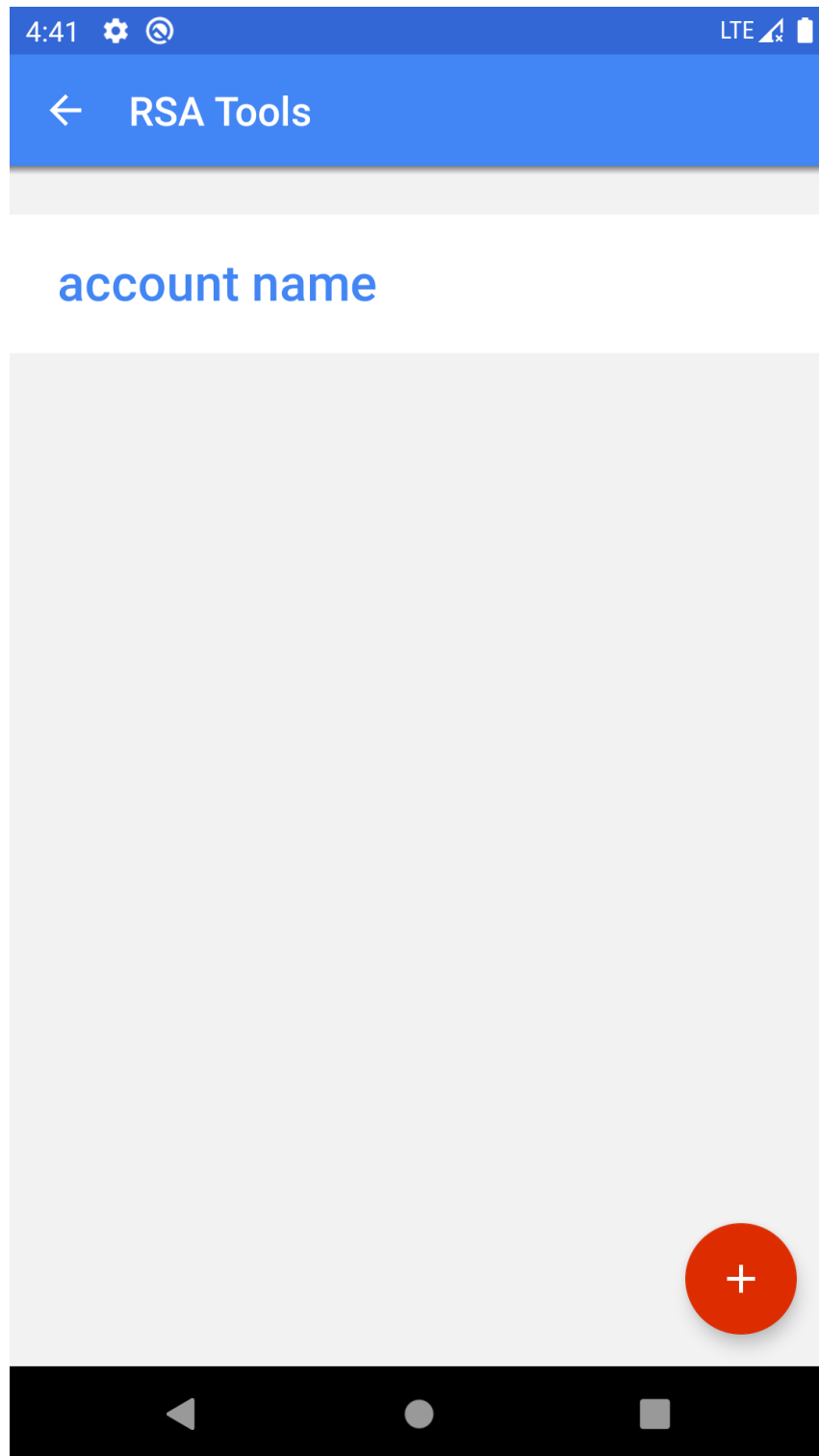


You will be directed to enter account details. Click "Add" to continue RSA key generation.

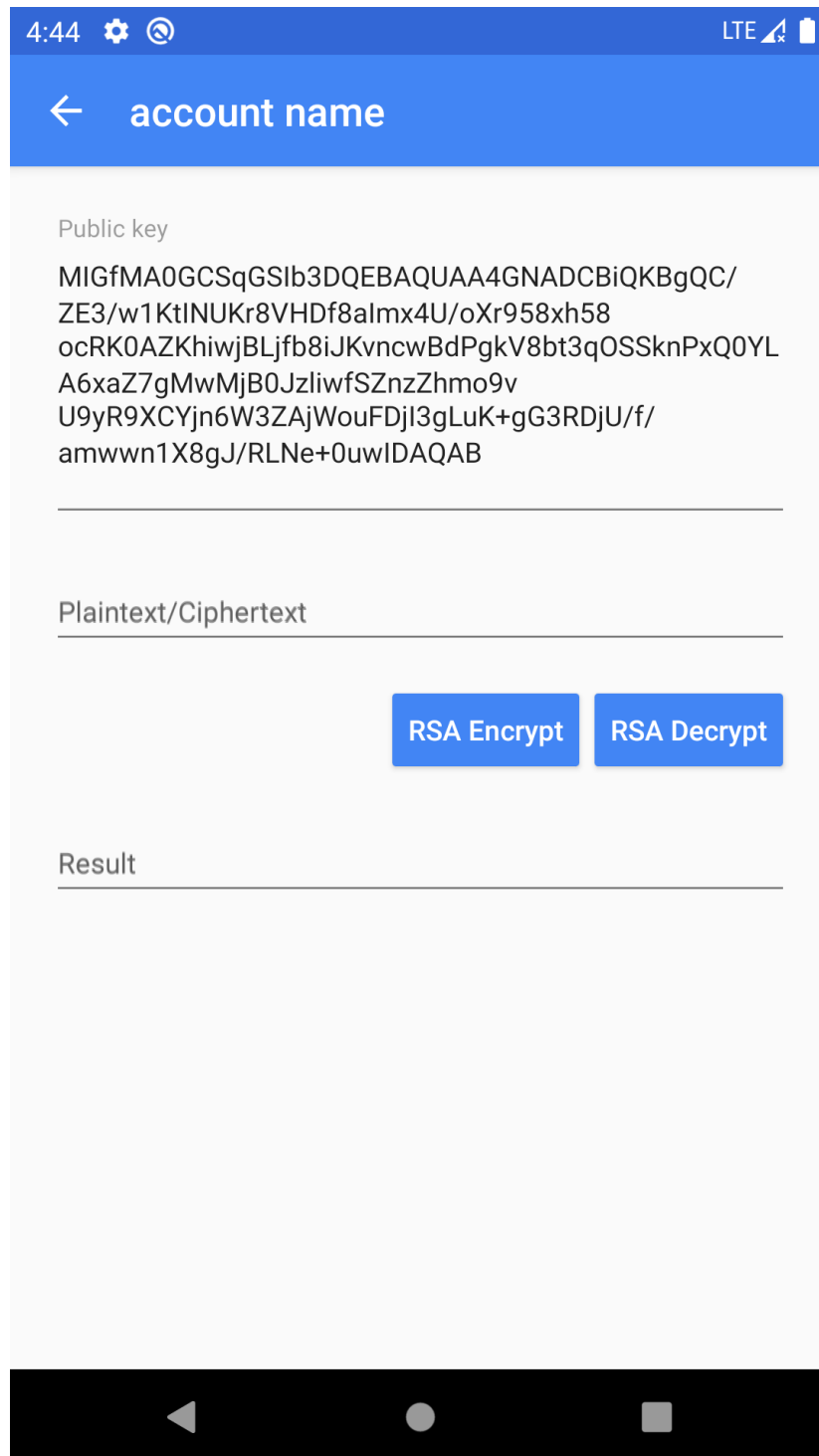
**Note:** The RSA public and private key are a pair. Files encrypted by an RSA public key can only be decrypted by its corresponding private key. The account name here is used to generate different pairs of private and public keys.

The screenshot shows a mobile application interface. At the top, a blue status bar displays the time 3:43, a gear icon for settings, a circular arrow icon for refresh, and network/battery status indicators including 'LTE' and a battery level icon. Below the status bar is a white header area with a back arrow icon and the text 'Enter account details'. The main content area is white and contains a text input field with the placeholder text 'Account name'. To the right of the input field is a blue button with the text 'ADD' in white. At the bottom of the screen is a black navigation bar with three icons: a back arrow, a circle, and a square.

You will be directed to the RSA Tools page after adding the account name.







Click “account name”.




Copy the public key. This will be used during account registration.

## RSA encryption

Users will receive an email with the theme “OTP secret key ciphertext”. Copy the content in the email to Plaintext/Ciphertext and click “RSA Decrypt”.

4:44   LTE  

 account name

Public key

MIGfMA0GCSqGSIsb3DQEBAQUAA4GNADCBiQKBgQC/  
ZE3/w1KtINUKr8VHDf8almx4U/oXr958xh58  
ocRK0AZKhiwjBLjfb8iJKvncwBdPgkV8bt3qOSSknPxQ0YL  
A6xaZ7gMwMjB0JzliwfSZnzZhmo9v  
U9yR9XCYjn6W3ZAJWouFDjI3gLuK+gG3RDjU/f/  
amwwn1X8gJ/RLNe+0uwIDAQAB



Plaintext/Ciphertext



RSA Encrypt


RSA Decrypt

Result

Copy the OTP key in the “result”.

5:01  

LTE  

 account name

Public key

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/  
ZE3/w1KtINUKr8VHDF8almx4U/oXr958xh58  
ocRK0AZKhiwjBLjfb8iJKvncwBdPgkV8bt3qOSSknPxQ0YL  
A6xaZ7gMwMjB0JzliwfSZnzZhmo9v  
U9yR9XCYjn6W3ZAJWouFDjl3gLuK+gG3RDjU/f/  
amwwn1X8gJ/RLNe+0uwIDAQAB

---

Plaintext/Ciphertext

Uddy1GzNLSA+d0VLNzz/  
u6R40nZk1rYmJuolHPP0eg6+xly52BAbVPR/  
id2Wdd2qMQc0YuM/Oxck  
UORAW+kvyl/  
wZpHG9x9gBesLBau7Ke+3VUNvYFQAeKT9s/  
kF1MU7GERvwotLUDJG9qnAAfkiH8a4  
U9ISBaLm63y6DGT5EV8=

---

RSA Encrypt

RSA Decrypt

Result

ONEOUU3ZZVDDURR3

---

copied to clipboard





## 2.OTP

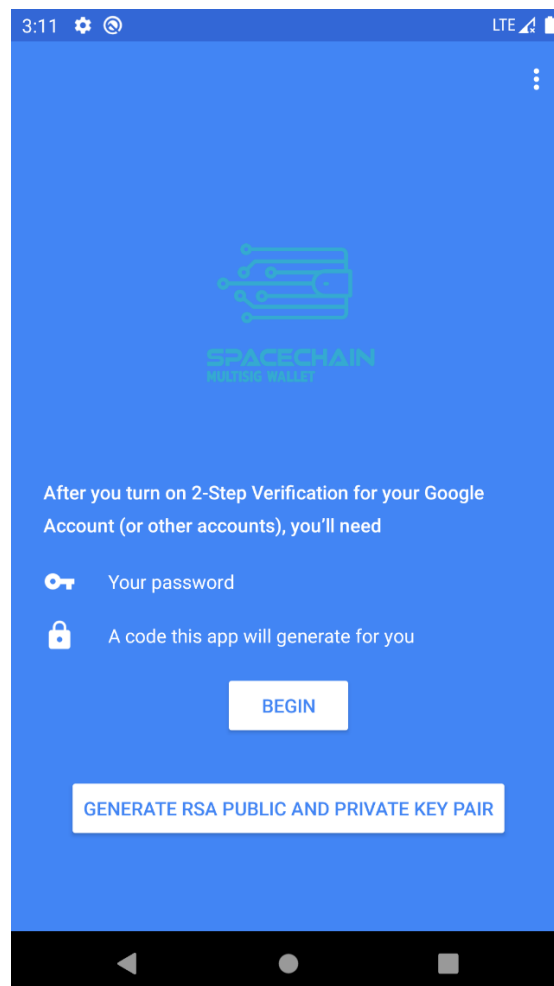
### OTP

#### Introduction

Corporate users need to use an OTP to encrypt their transaction files. SPC payload will check whether the OTP is correct. Users can obtain the OTP after configuring the RSA Tools in Step 1.

#### Add an account

Click “begin” to add an account.



Select “Enter a provided key”.

5:34 [Settings] [Notification] LTE [Signal] [Battery]

## ← Enter account details

Account name \_\_\_\_\_

Your key \_\_\_\_\_

☐ Time based

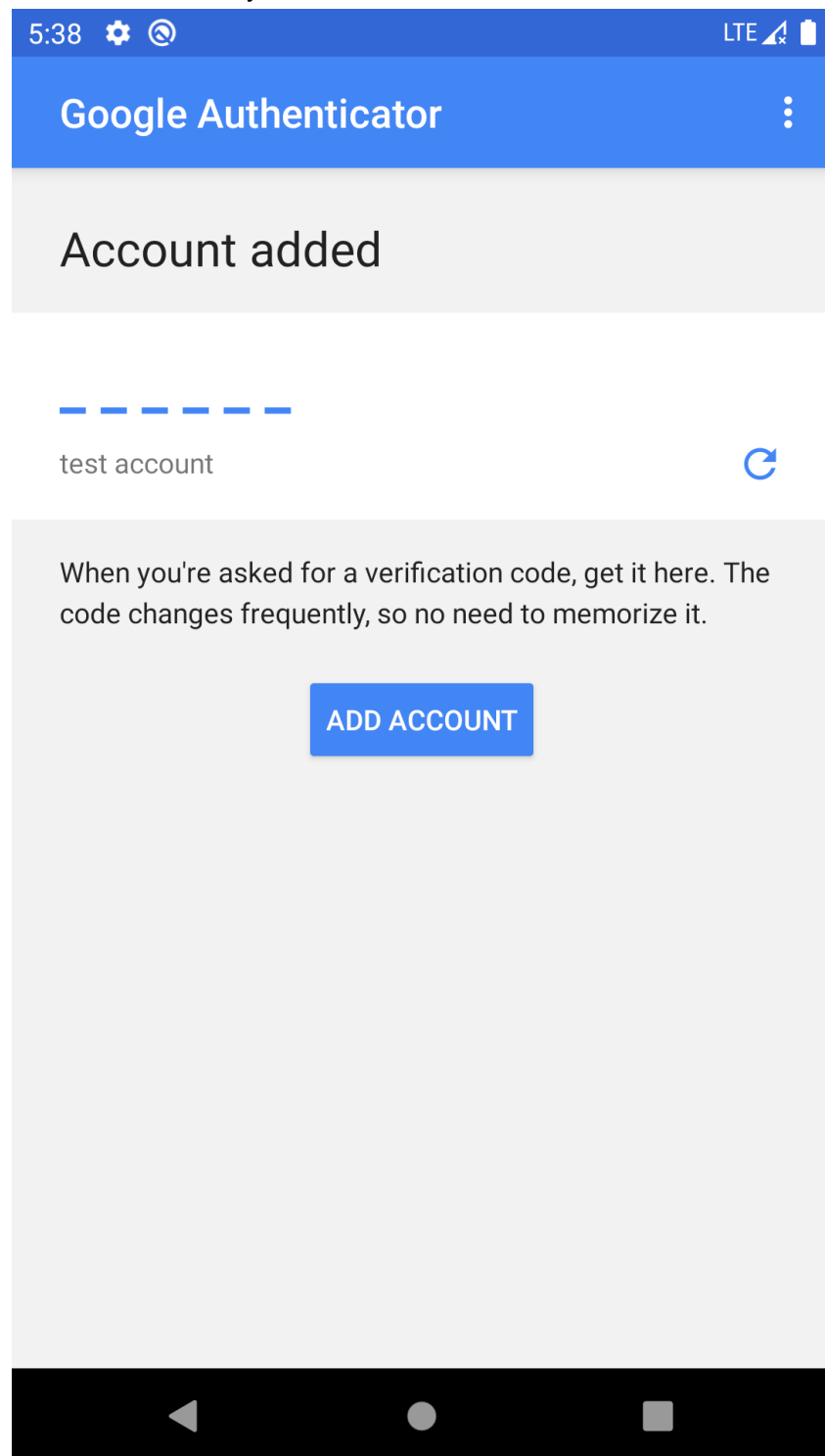
☒ Counter based

ADD

The purpose of an account name is to differentiate the OTP.

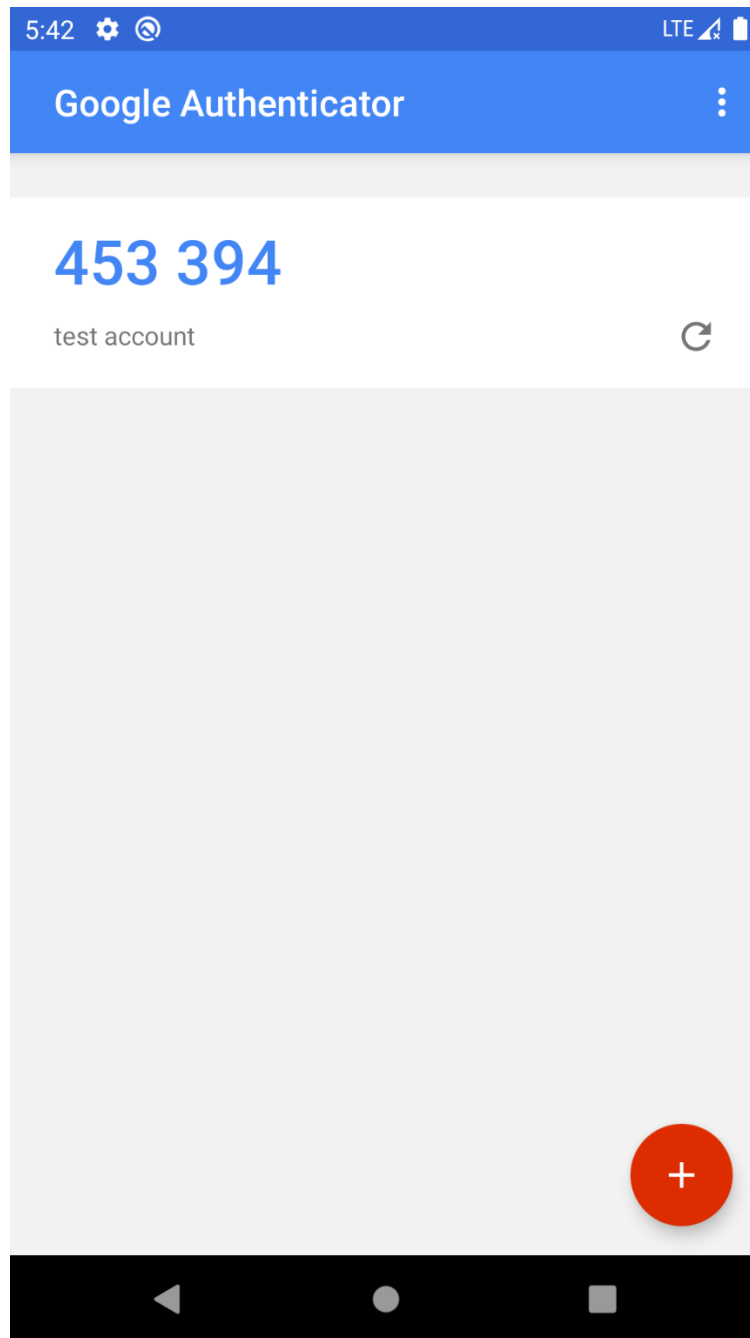
“Your key” is the OTP key generated in Step 1. Copy the OTP key to “Your key”. Select “counter based” and click “ADD”.

The account is successfully added.



## Obtain an OTP

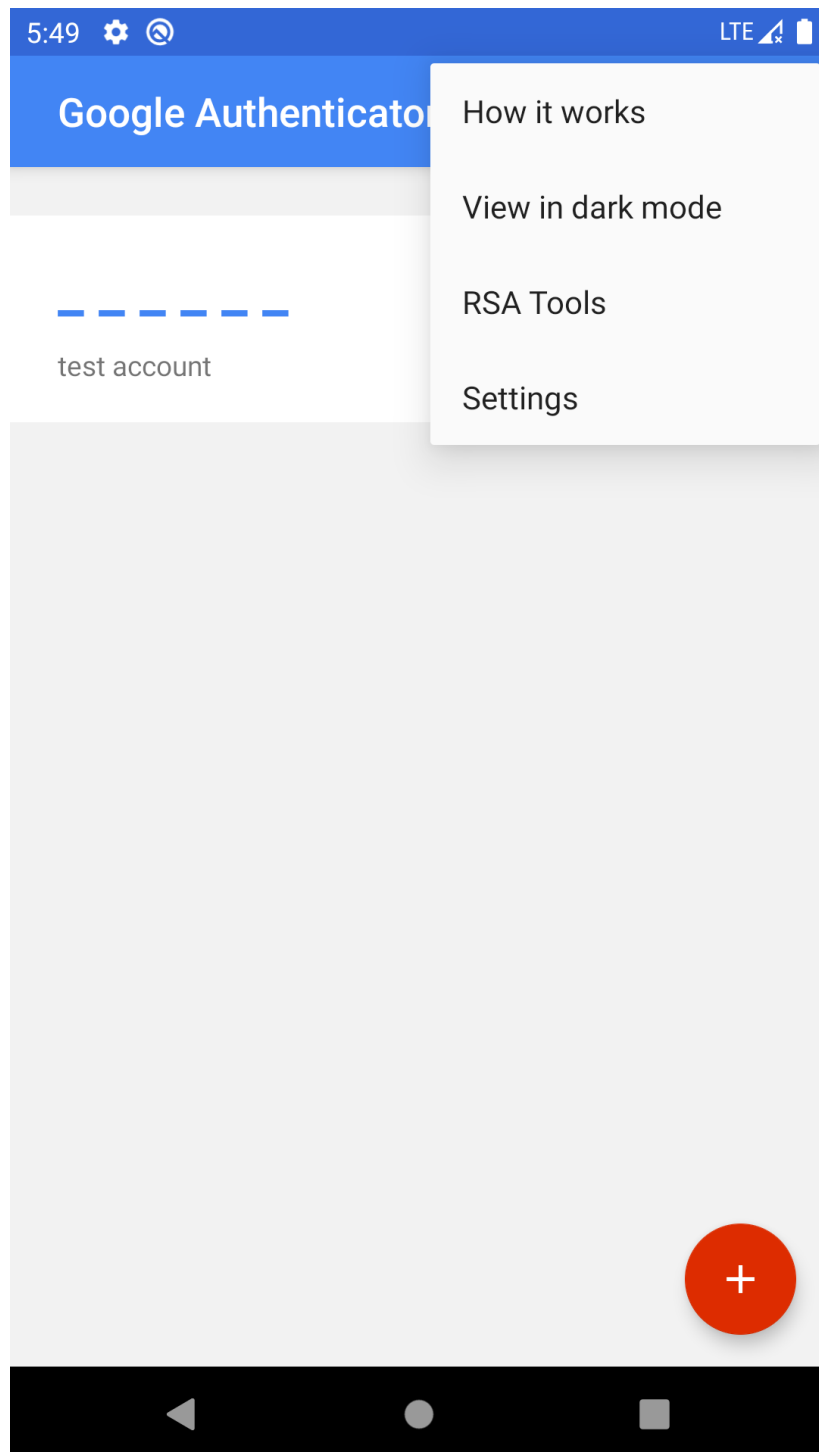
Click the account name to obtain its corresponding OTP.



### 3. Others

#### RSA Tools

Unless one is opening the app for the first time, the location RSA Tools is shown in the below figure.



## Change the account name in RSA Tools

Press and hold the “account name” to modify/delete the account name of RSA Tools.

