Back-up and recovery of IRMA attributes

Master Thesis Project

Ivar Derksen

Radboud University

Introduction

- Research done in cooperation with Alliander
- Goal: solve a frequently asked question about IRMA

  What happens when a user gets a new device?

- Currently, all attributes have to be re-collected manually
- Can we do better?

Relevant scenarios

1. New device; old device still working

2. New device; old device broken

3. New device; old device lost/stolen

Take the easy road (1)

Why not use the default recovery functionality (like WhatsApp)?

- Android back-up to Google Drive
- iCloud back-up for iOS

Problems:

- Personal data and keys stored at servers of Google and Apple
- Storage parties might be able to impersonate a user
- User cannot block lost phones
- Only entering a password is weak authentication mechanism
- Identity can be copied multiple times

Take the easy road (2)

Why not re-collect all credentials, via some renewal script?

Problem:

Involves many re-authentications, this is much work for the user

Important criteria for a proper recovery solution

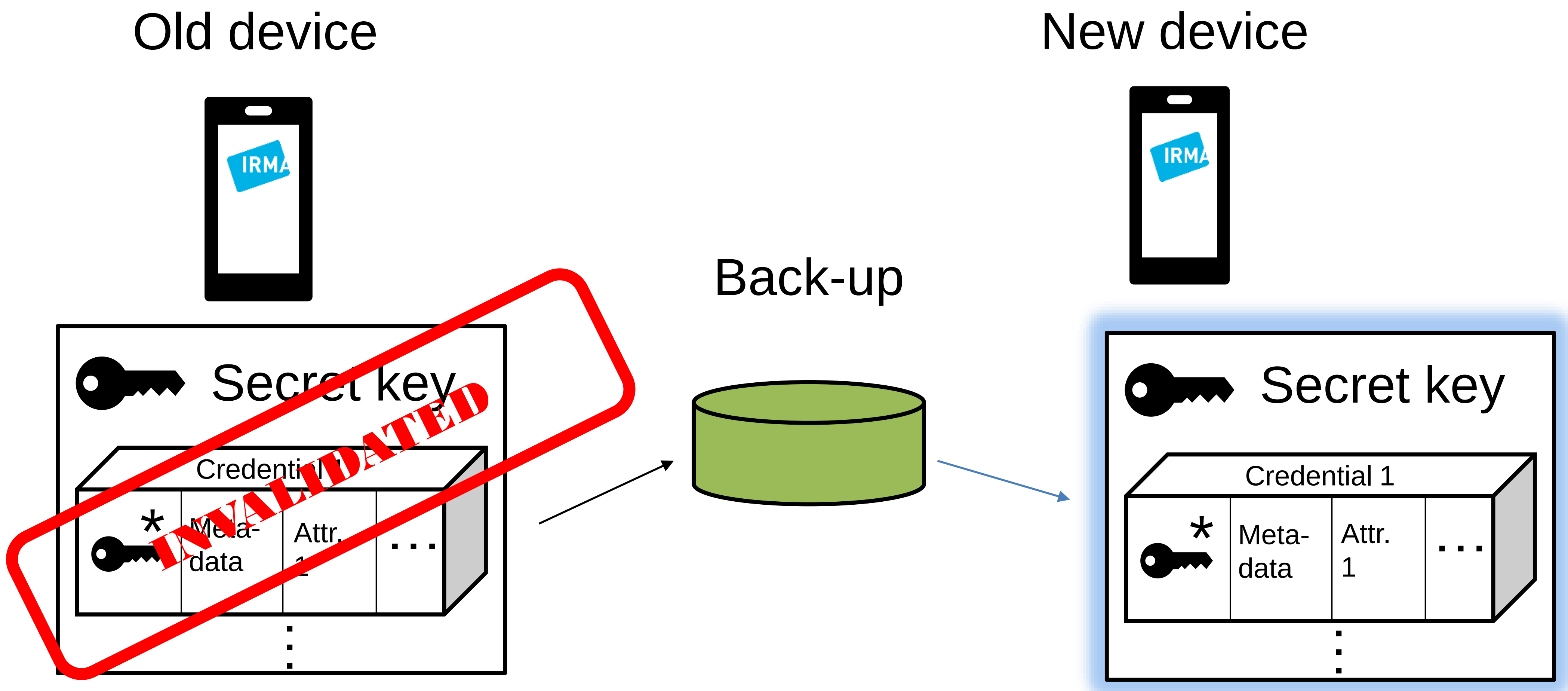
- User should be in exclusive control of recovery
- Recovery should be possible for the original user
- Procedures should be understandable and usable
- IRMA’s privacy and security guarantees should be maintained
- It should be clear which parties are involved
- Users should not become dependent on a single cloud provider

Proof-of-concept (PoC) that we designed:

- IRMA app's data is stored in back-up
- Back-up can be restored on new device
- Old device is blocked

Elements we focus on:

1. How can the back-up be secured?
2. How can old devices be blocked?



1. Make back-ups secure

- Wherever a back-up is stored, it should be secure and encrypted
- User data should be encrypted before it leaves the IRMA app
- The user should have control over the decryption key

Big question: how can a user safely store a decryption key of the back-up

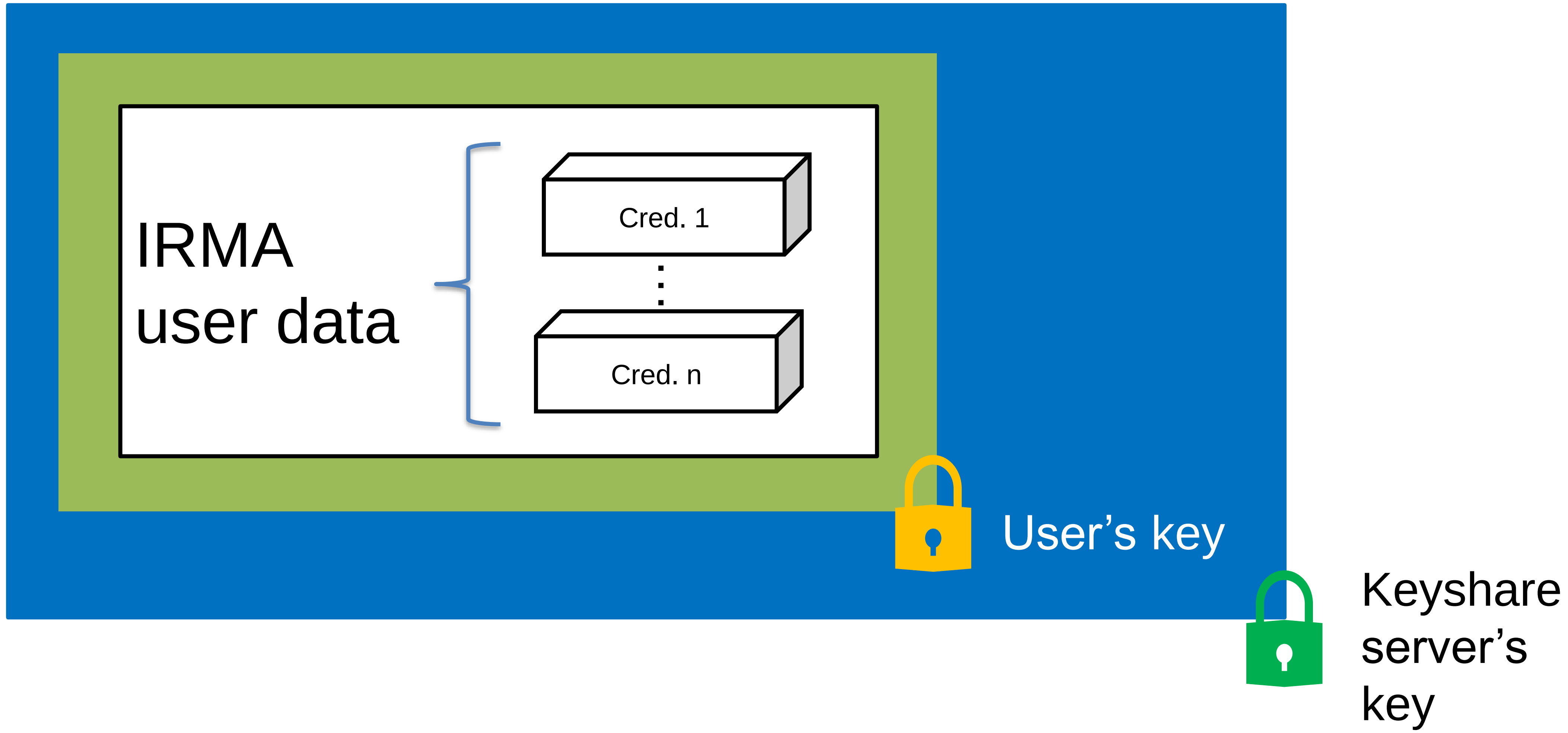
- Storing it digitally may not be transparent enough
- Storing it at a central party gives a fake notion of control
- Secret sharing is a complicated process

A solution is to store the key physically, on paper
→ Two-factor authentication

1. Make back-ups secure (technical)

In our proof-of-concept the back-up is encrypted twice for two-factor authentication

- A user key
  - Stored by the user
- A public key of the keyshare server
  - Is involved to check the user's PIN code
  - Back-up can only be decrypted when keyshare server participates



In our PoC: user key as mnemonic phrase

- Known from Bitcoin wallets
- List of 12 words is generated randomly
- Order of words is important
- Selected from word list of 2048 words
  - Selected to be easy and sufficiently unique
  - First four characters are identifying for a word
  - Available in multiple languages, can easily be extended

loop
day
cushion
rebuild
chair
warfare
search
vague
fire
verify
west
grid

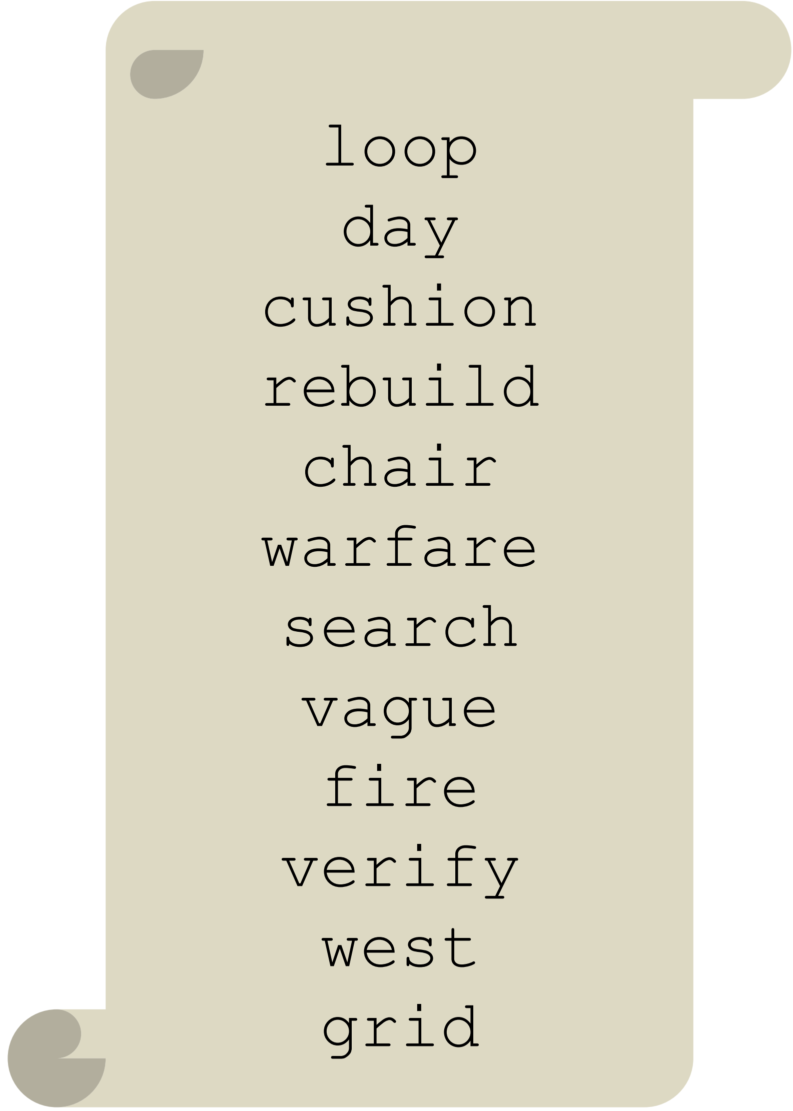
In our PoC: user key as mnemonic phrase

Advantages:

- Is understandable for every user
- No additional technology is needed

Disadvantages:

- Writing a phrase down and entering it back in requires some time
- User might make mistakes when writing it down
  - User interface can help to prevent mistakes



loop
day
cushion
rebuild
chair
warfare
search
vague
fire
verify
west
grid

2. Device revocation

IRMA account on old devices should be blocked when transferring IRMA account

Multiple reasons:

- Prevent usage of credentials without permission of user
- Prevent that credentials spread out
  - Multiple devices might have exact the same credentials (copies)
  - Possibility for users to lend out credentials
  - Link between user and device becomes weaker
- Legal reasons (eIDAS requirements)

In our PoC: device revocation via keyshare server

- In every IRMA session the user’s PIN is checked by the keyshare server
- Without PIN approval of the keyshare server nothing can be done
- It can also efficiently enforce device revocation
  → An additional check can be built-in to check whether the used device is still valid

When device is revoked:

- IRMA app cannot be opened anymore on that device
- Disclosure, issuance and signing sessions cannot be completed using that device

In our PoC: device revocation via keyshare server (technical)

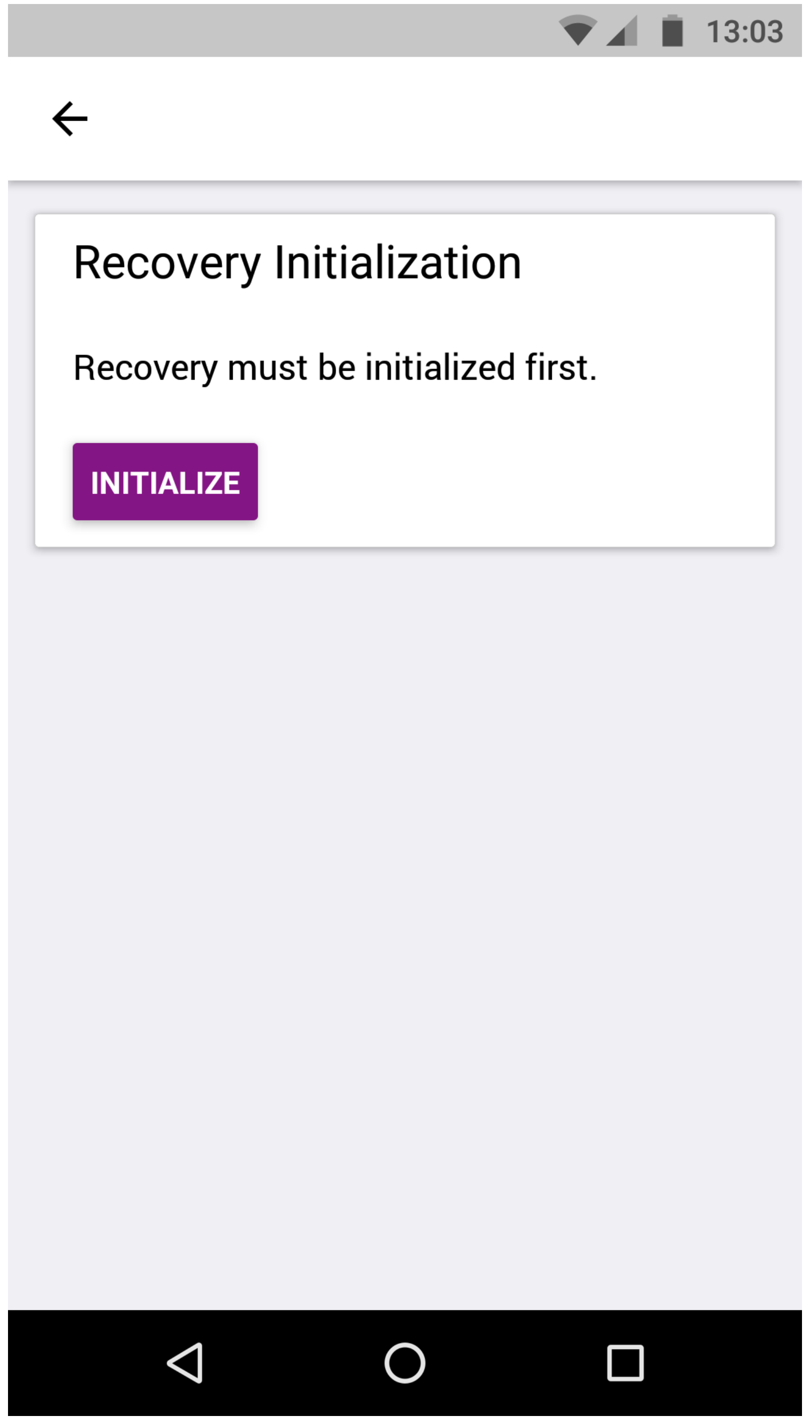
- We do this by adding a device key
  - Shared key between IRMA app containing the active IRMA account and the keyshare server
  - Sessions with the keyshare server can only be made valid knowing the device key

When recovery process is started on new device:

1. User authenticates by entering his PIN
2. New device and keyshare server agree on new device key
3. Keyshare server deletes previous device's key
4. Keyshare server helps decrypting the back-up

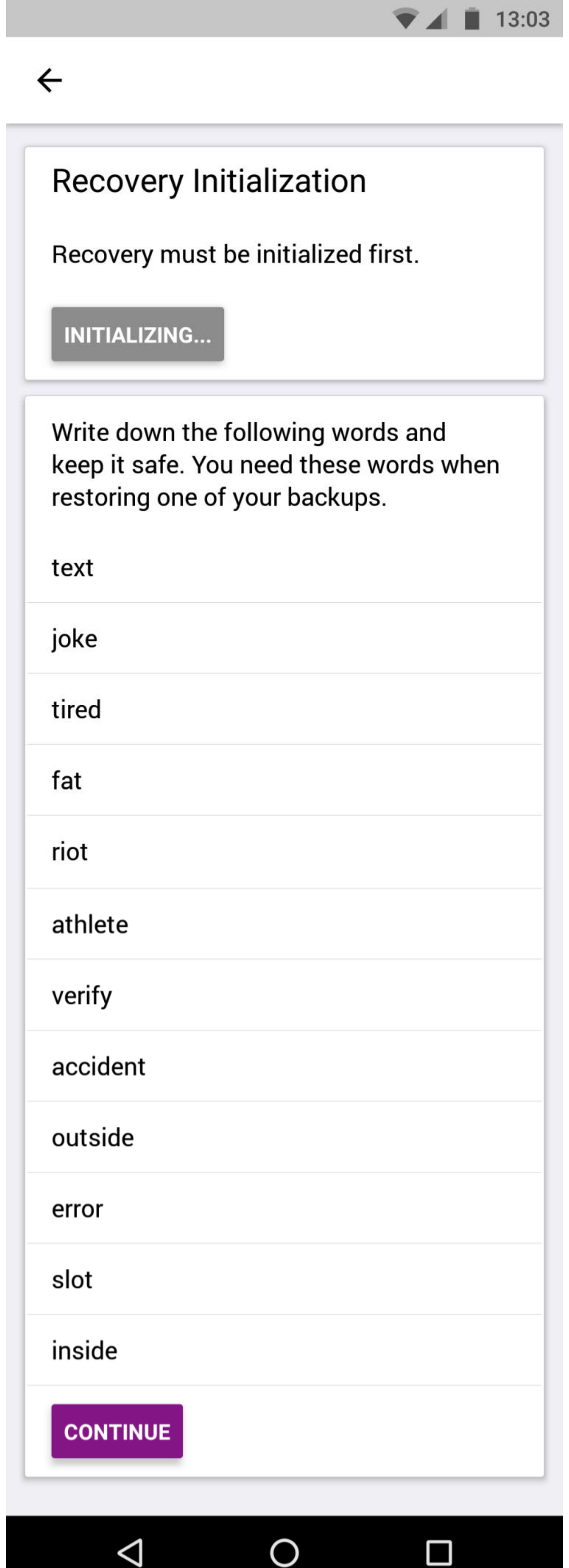
Demo

Setting up recovery



Recovery Initialization

Recovery must be initialized first.

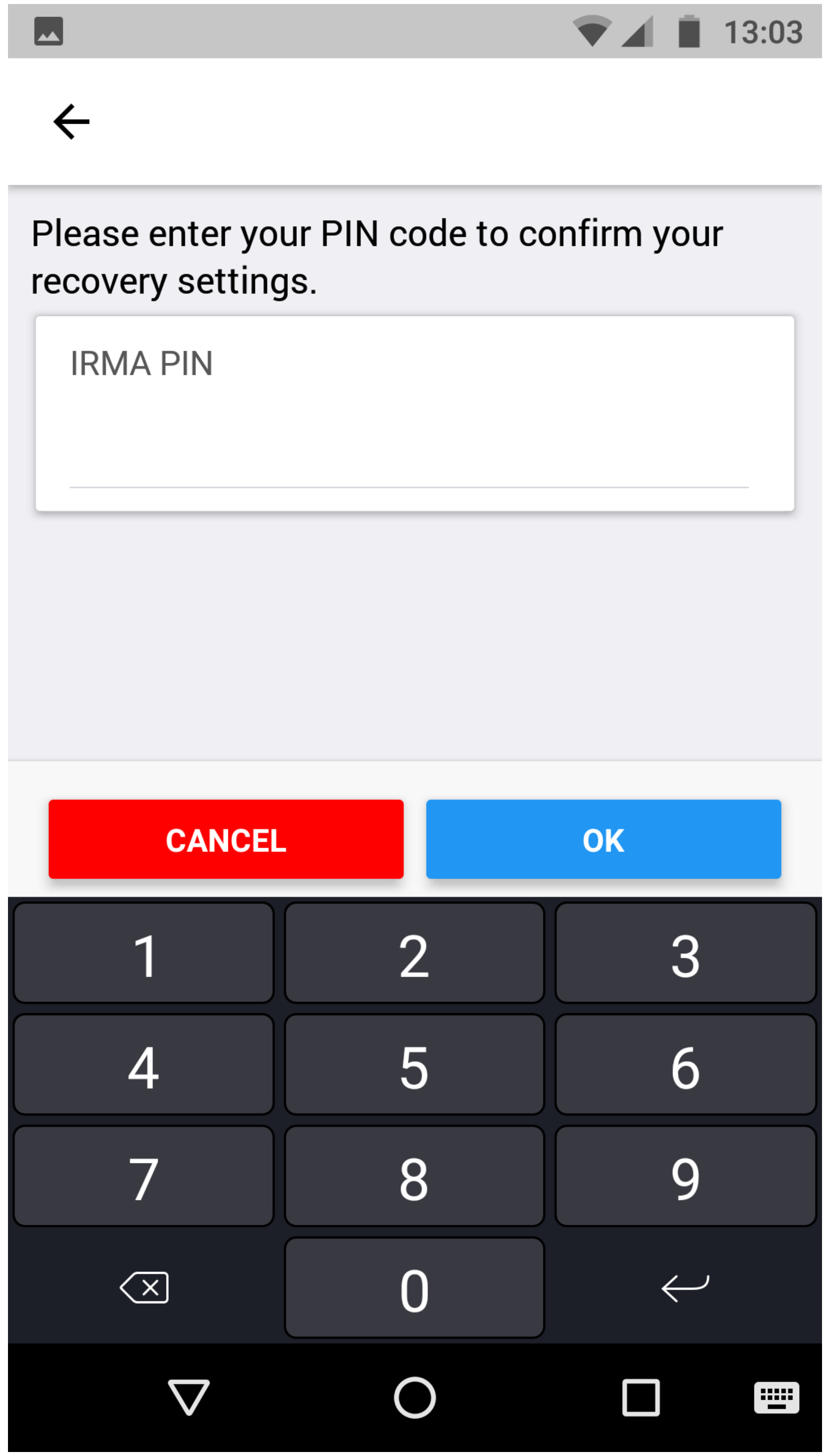


Recovery Initialization

Recovery must be initialized first.

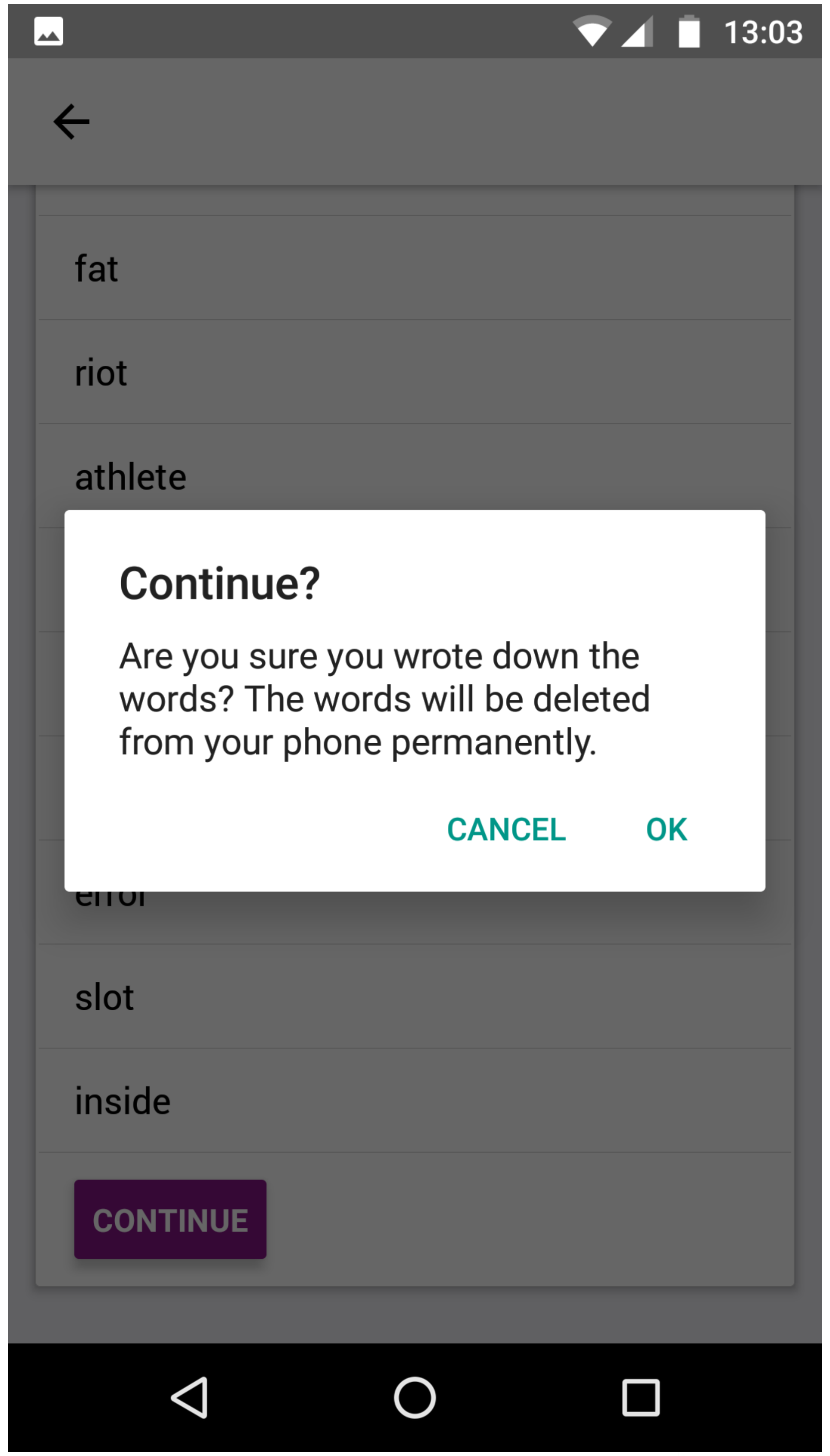
Write down the following words and keep it safe. You need these words when restoring one of your backups.

text
joke
tired
fat
riot
athlete
verify
accident
outside
error
slot
inside



Please enter your PIN code to confirm your recovery settings.

IRMA PIN



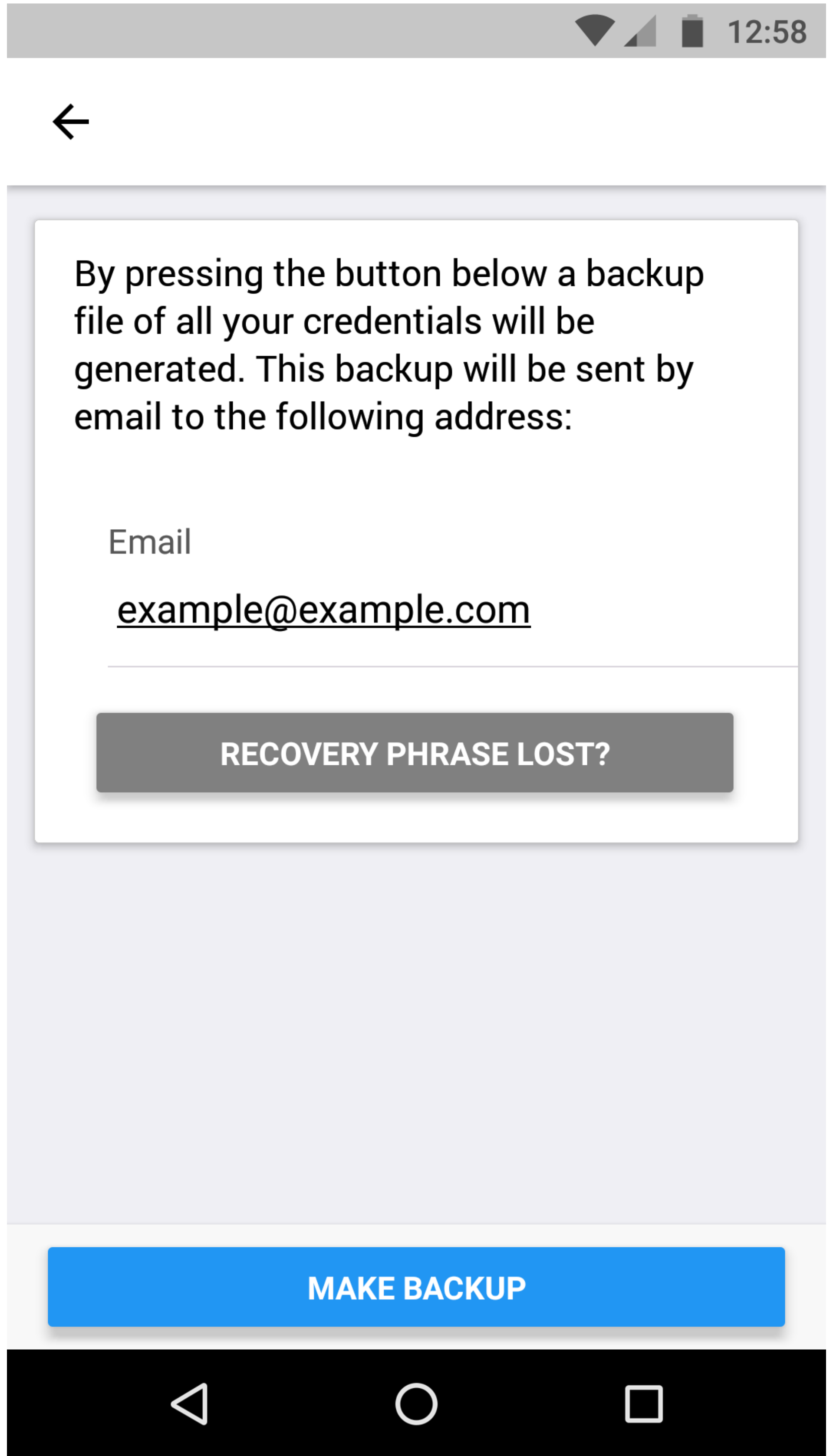
fat
riot
athlete

Continue?

Are you sure you wrote down the words? The words will be deleted from your phone permanently.

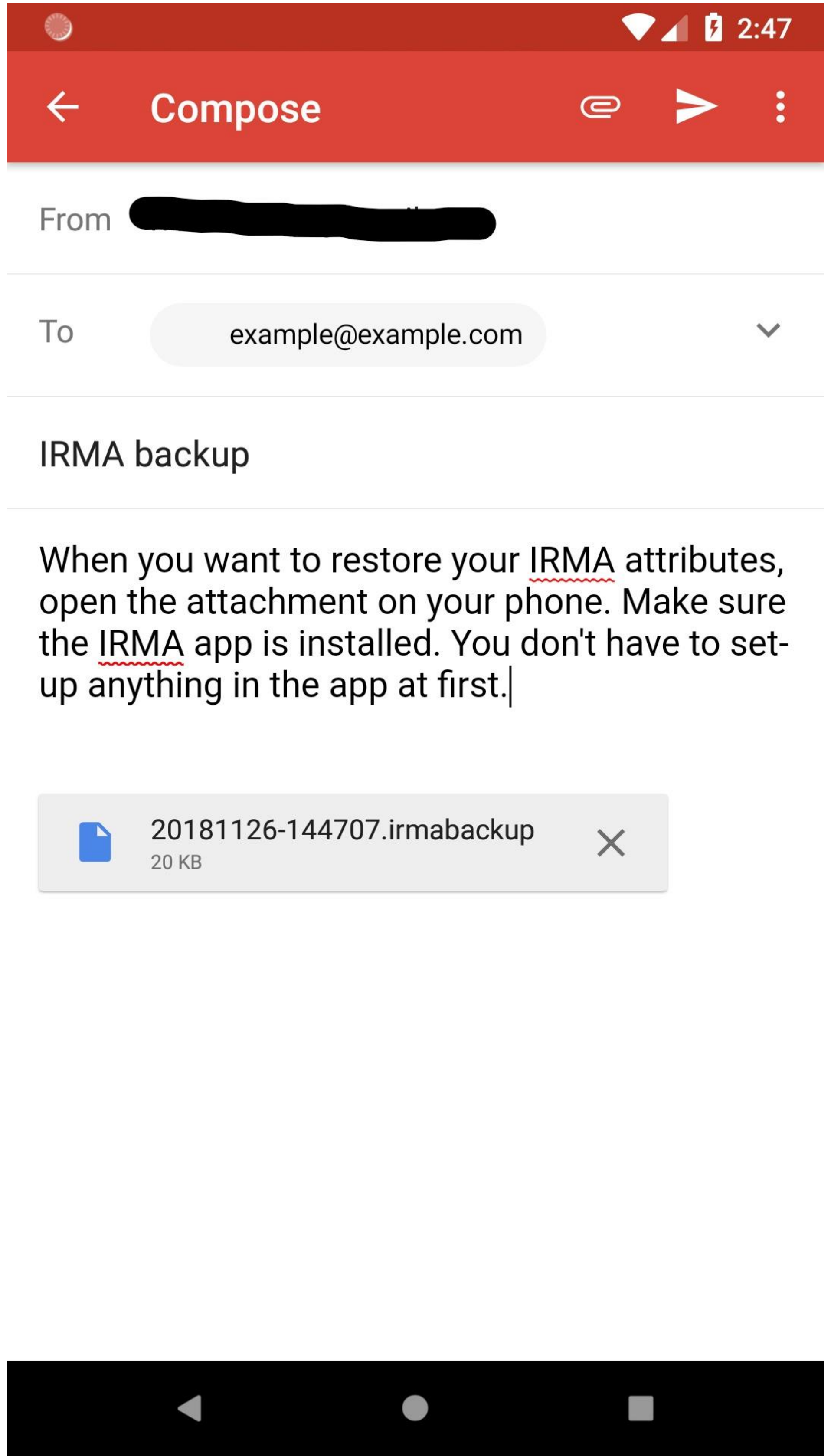
error
slot
inside

Constructing a back-up



By pressing the button below a backup file of all your credentials will be generated. This backup will be sent by email to the following address:

Email
example@example.com



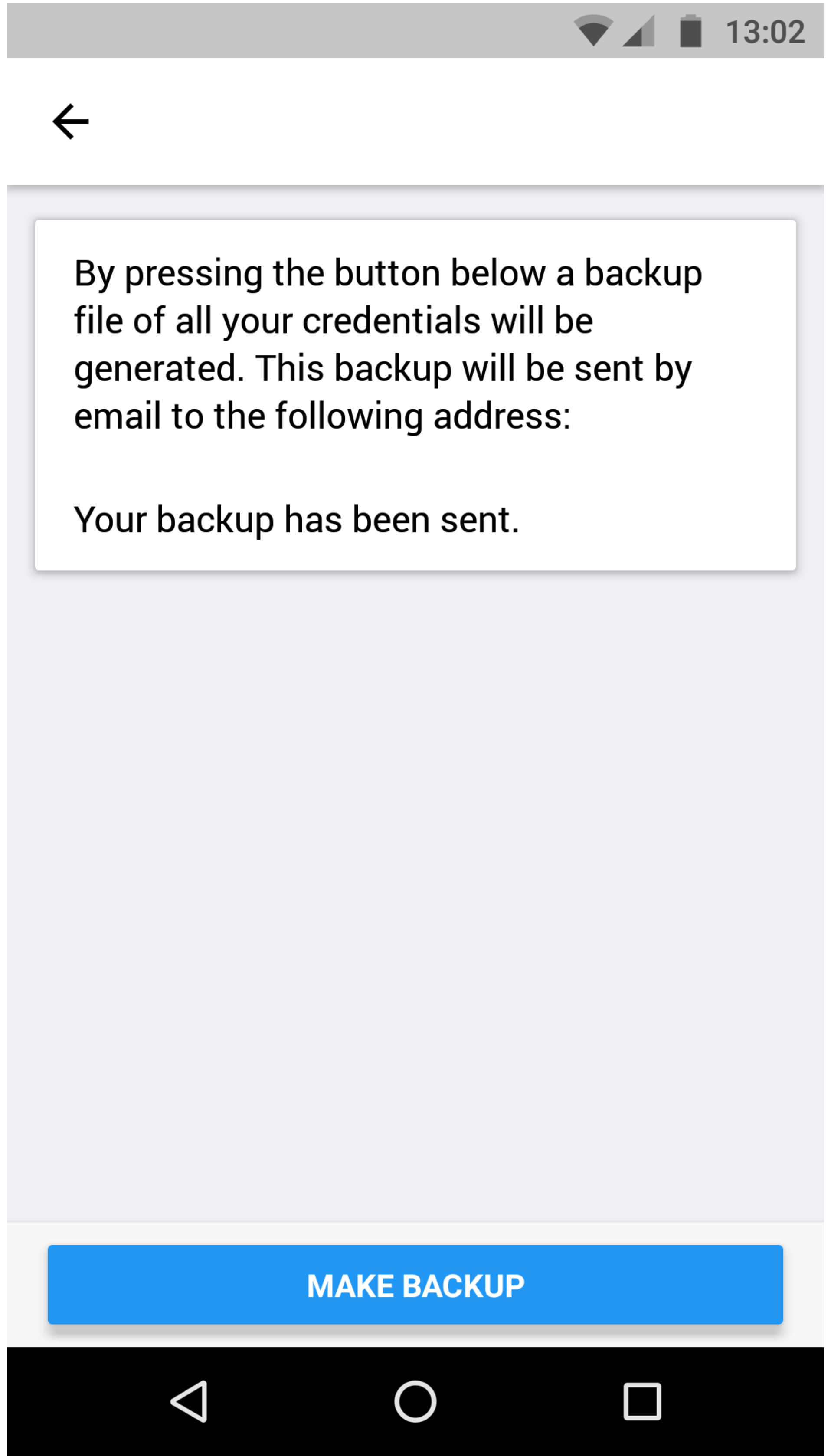
From [redacted]

To example@example.com

IRMA backup

When you want to restore your IRMA attributes, open the attachment on your phone. Make sure the IRMA app is installed. You don't have to set-up anything in the app at first.

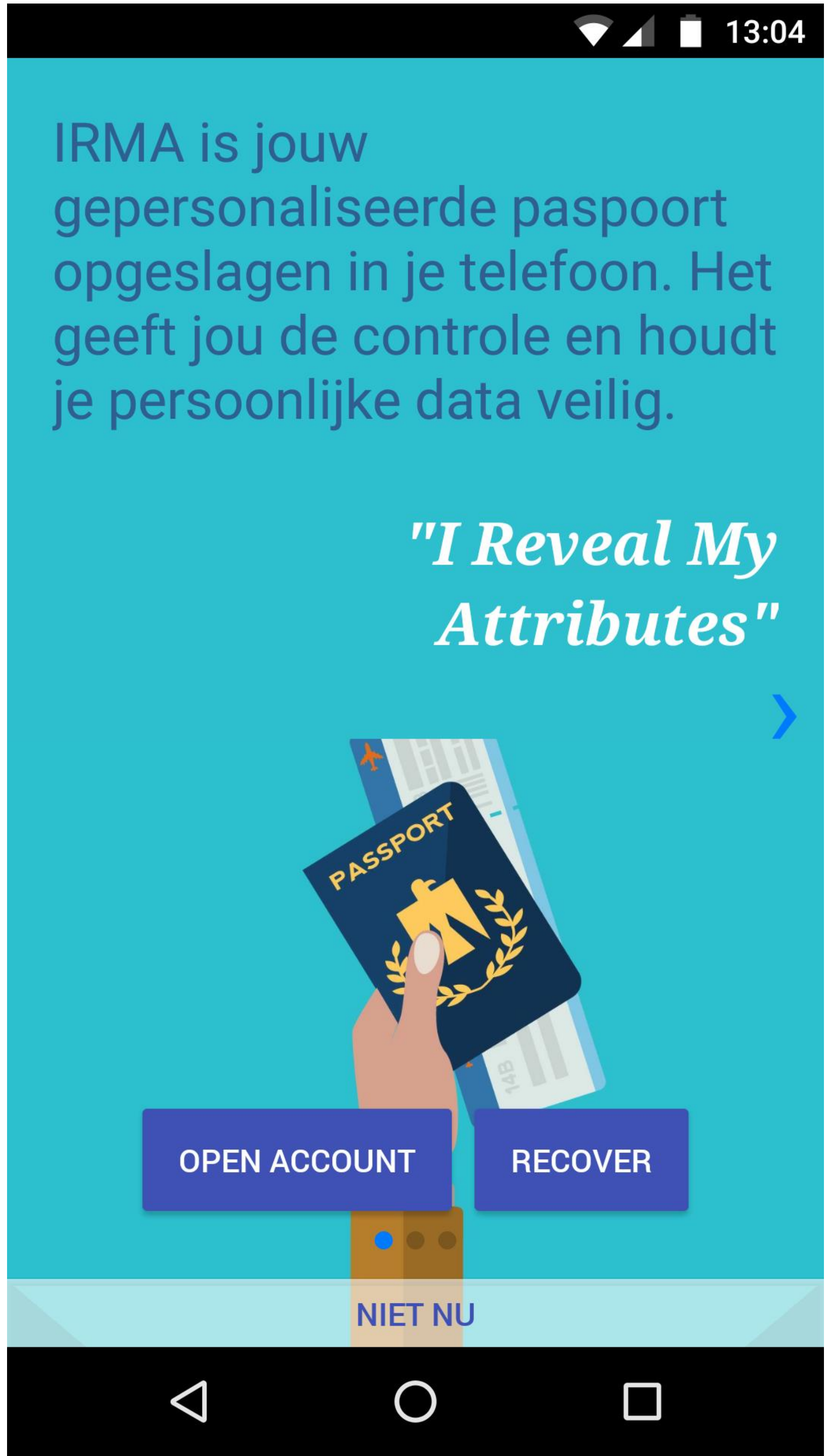
20181126-144707.irmabackup
20 KB



By pressing the button below a backup file of all your credentials will be generated. This backup will be sent by email to the following address:

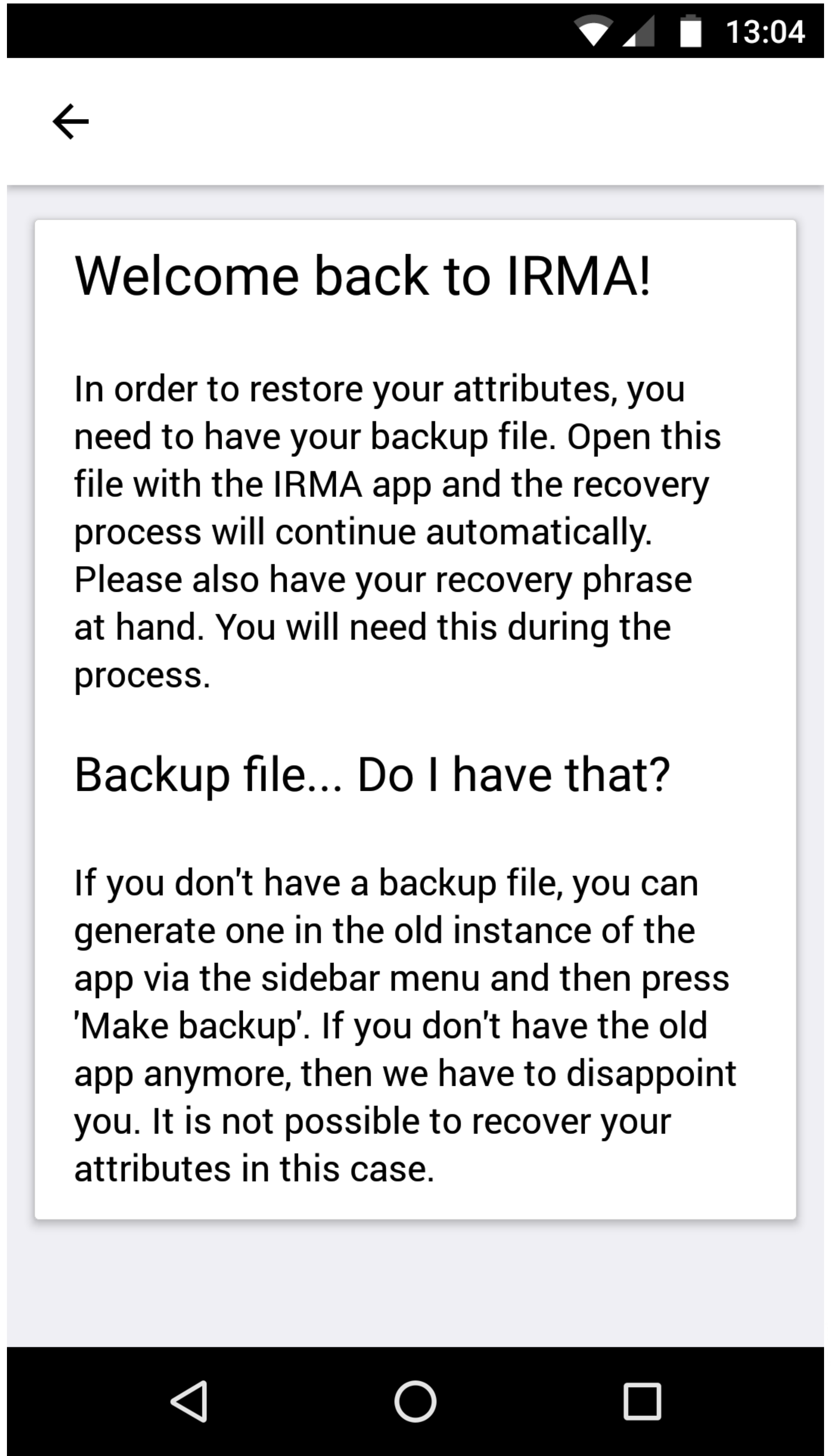
Your backup has been sent.

Opening the app on a new device



IRMA is jouw gepersonaliseerde paspoort opgeslagen in je telefoon. Het geeft jou de controle en houdt je persoonlijke data veilig.

"I Reveal My Attributes"



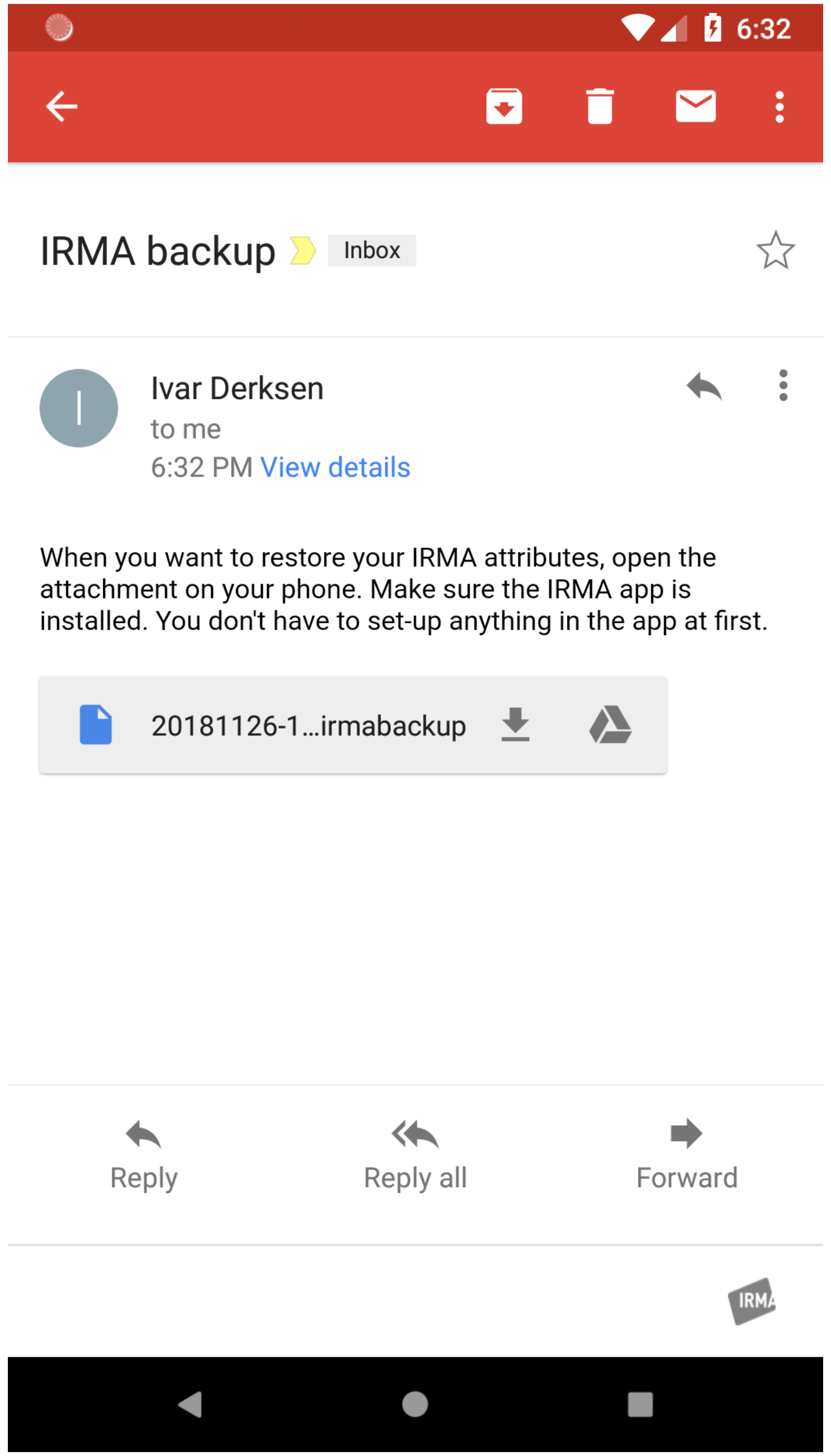
Welcome back to IRMA!

In order to restore your attributes, you need to have your backup file. Open this file with the IRMA app and the recovery process will continue automatically. Please also have your recovery phrase at hand. You will need this during the process.

Backup file... Do I have that?

If you don't have a backup file, you can generate one in the old instance of the app via the sidebar menu and then press 'Make backup'. If you don't have the old app anymore, then we have to disappoint you. It is not possible to recover your attributes in this case.

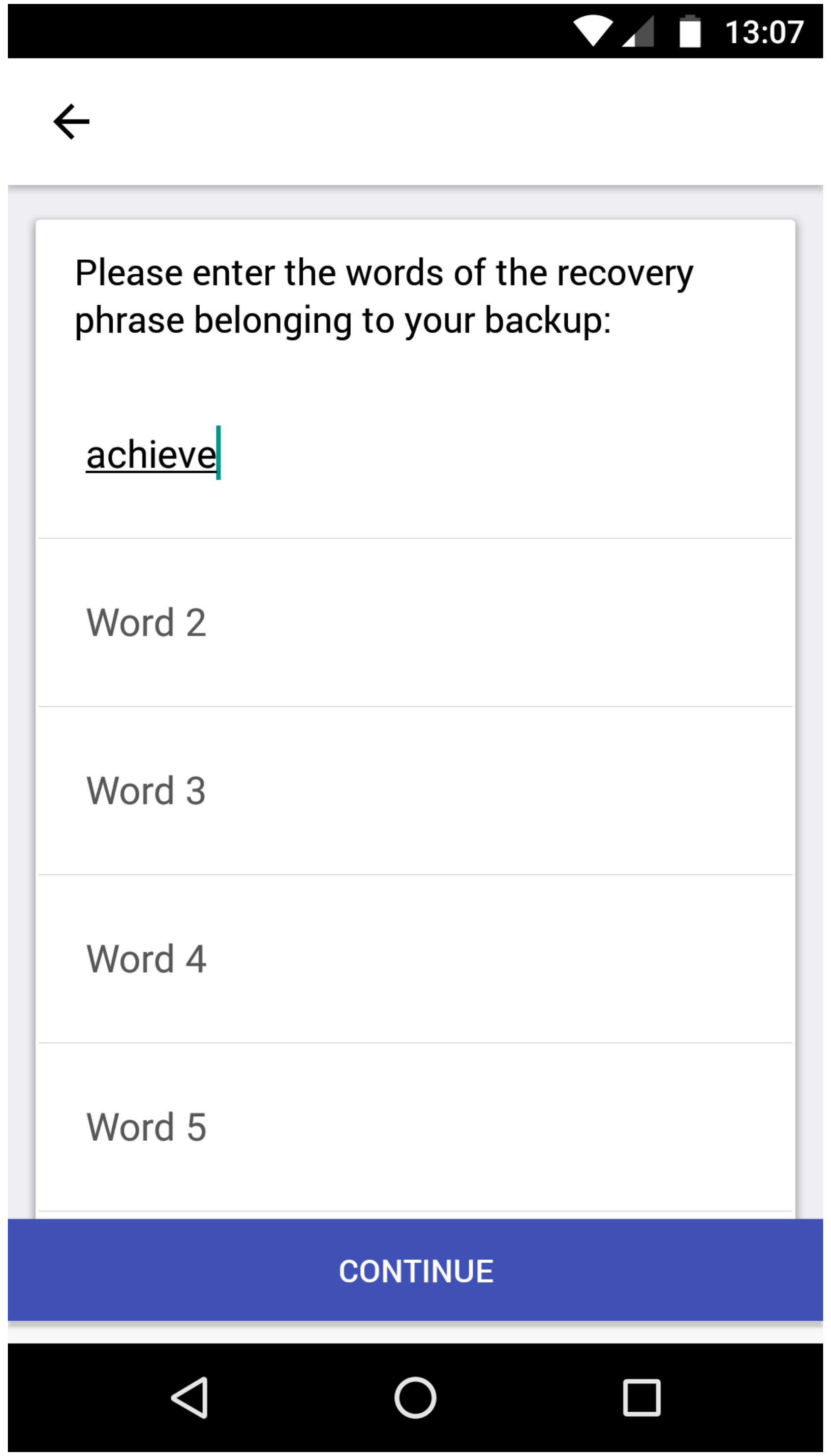
Recovery process



Ivar Derksen
to me
6:32 PM View details

When you want to restore your IRMA attributes, open the attachment on your phone. Make sure the IRMA app is installed. You don't have to set-up anything in the app at first.

20181126-1...irmabackup



Please enter the words of the recovery phrase belonging to your backup:

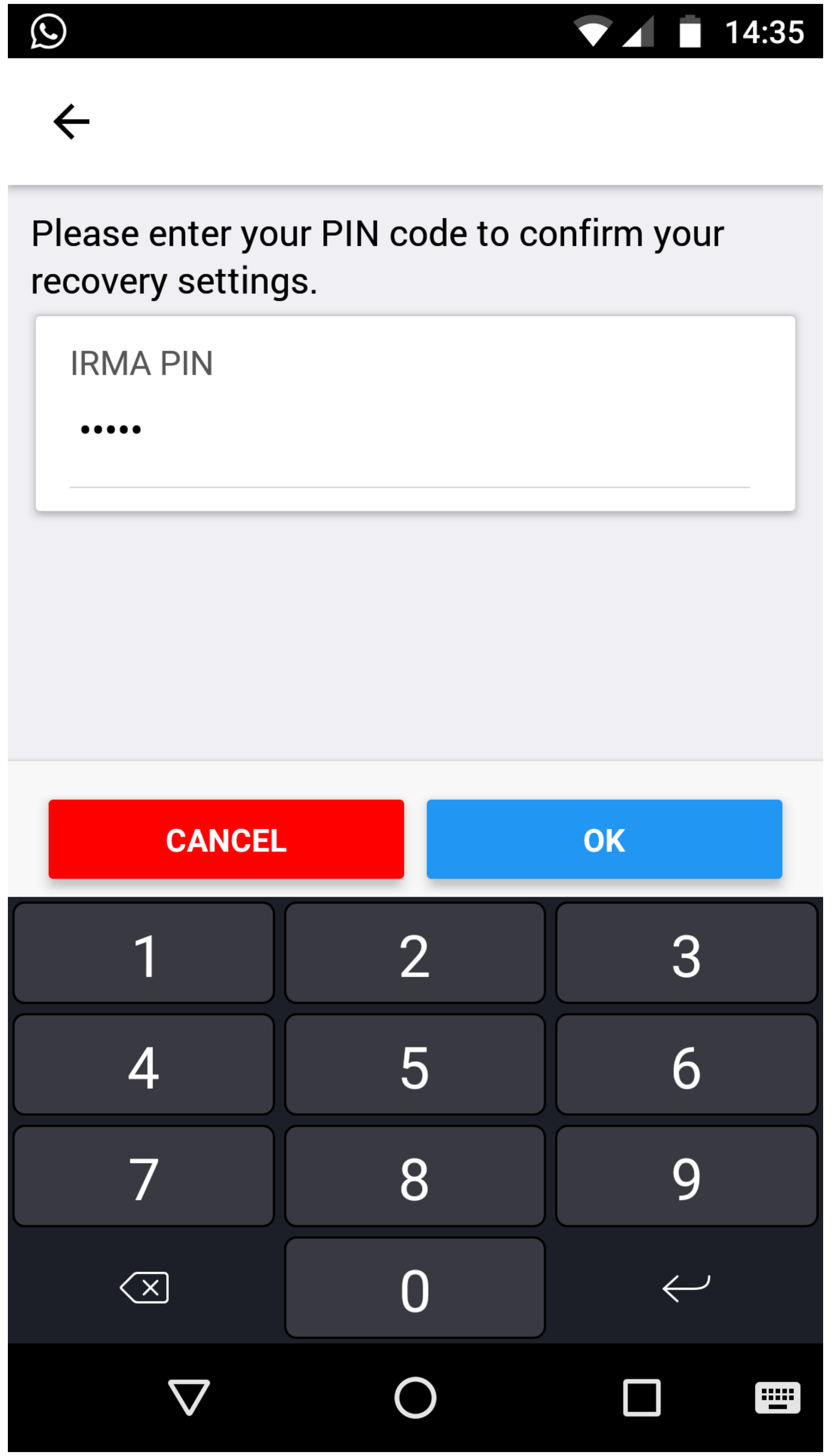
achieve

Word 2

Word 3

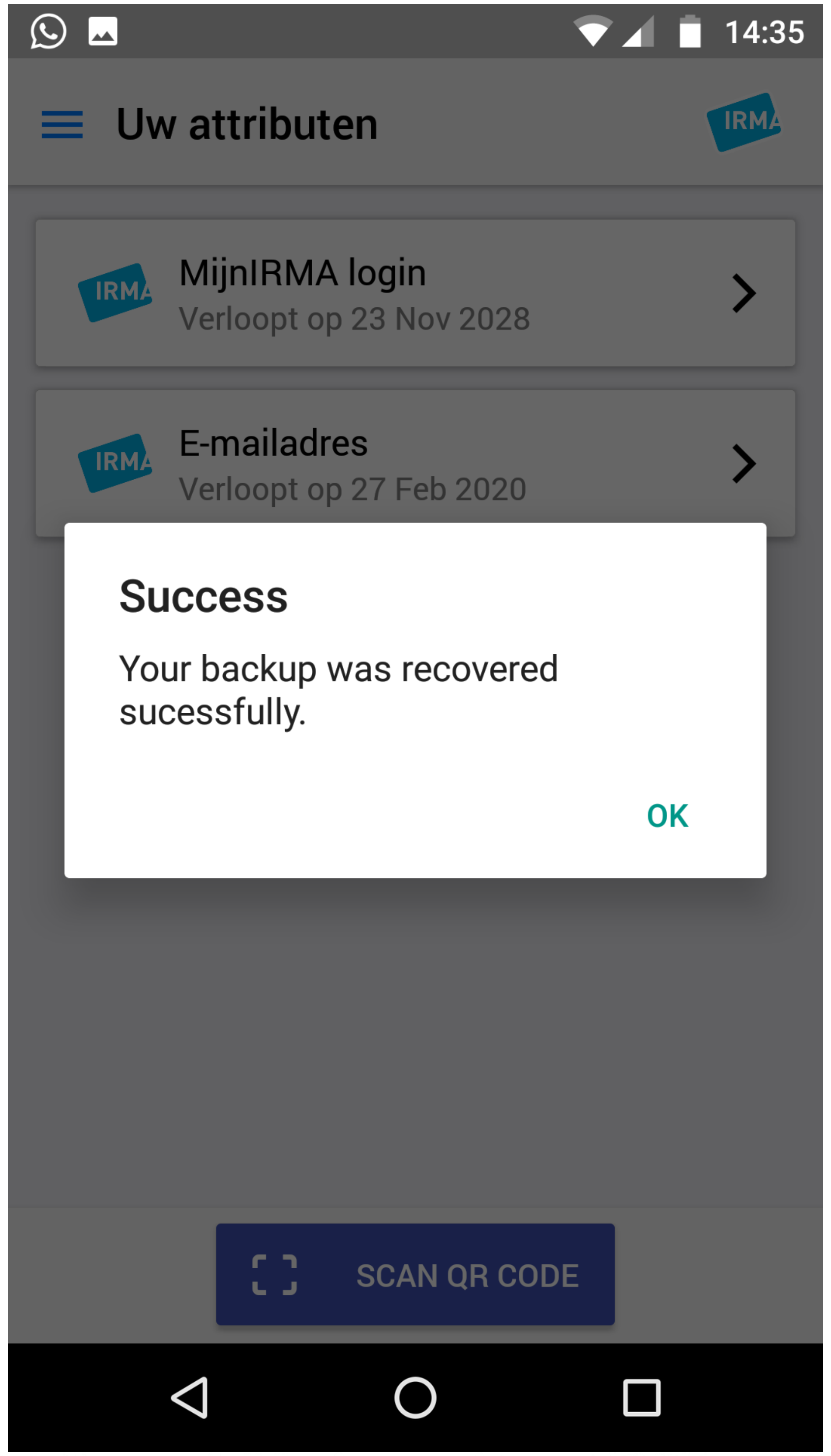
Word 4

Word 5



Please enter your PIN code to confirm your recovery settings.

IRMA PIN
•••••



MijnIRMA login
Verloopt op 23 Nov 2028

E-mailadres
Verloopt op 27 Feb 2020

Success

Your backup was recovered sucessfully.