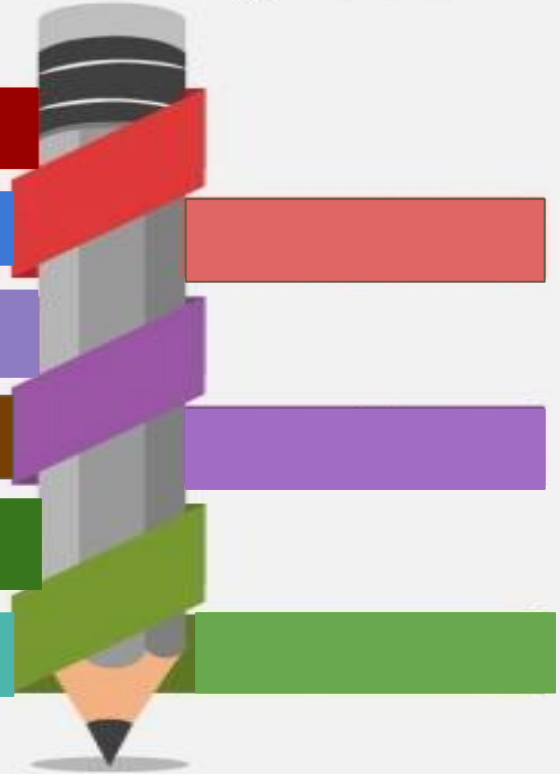
Usable Security and Privacy Lab

Matanat Ahmadova

Outline

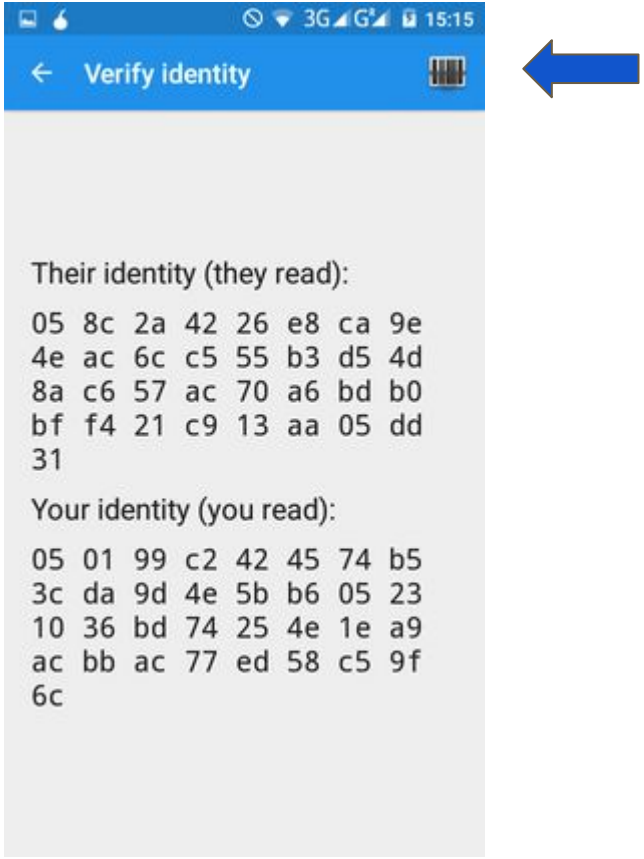


MOTIVATION

How can I verify identity of the group member?

How can I verify identity of the group member?

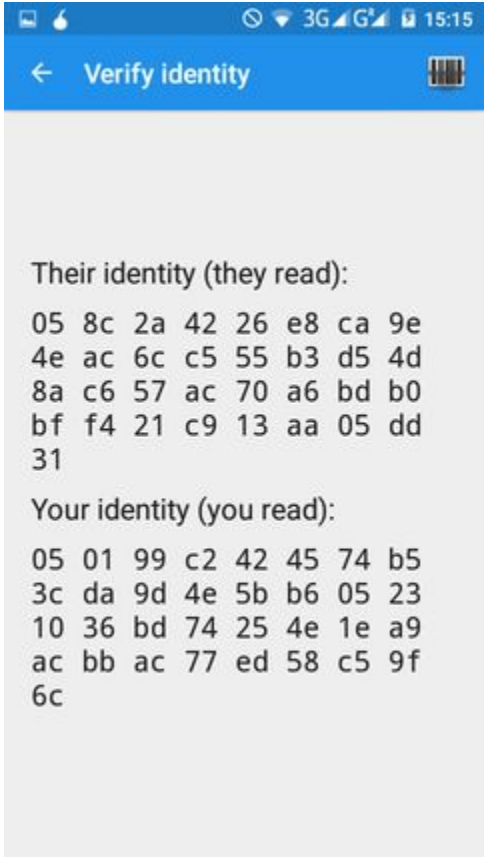
- QR code scan


15:15
Verify identity
Their identity (they read):
05 8c 2a 42 26 e8 ca 9e
4e ac 6c c5 55 b3 d5 4d
8a c6 57 ac 70 a6 bd b0
bf f4 21 c9 13 aa 05 dd
31
Your identity (you read):
05 01 99 c2 42 45 74 b5
3c da 9d 4e 5b b6 05 23
10 36 bd 74 25 4e 1e a9
ac bb ac 77 ed 58 c5 9f
6c

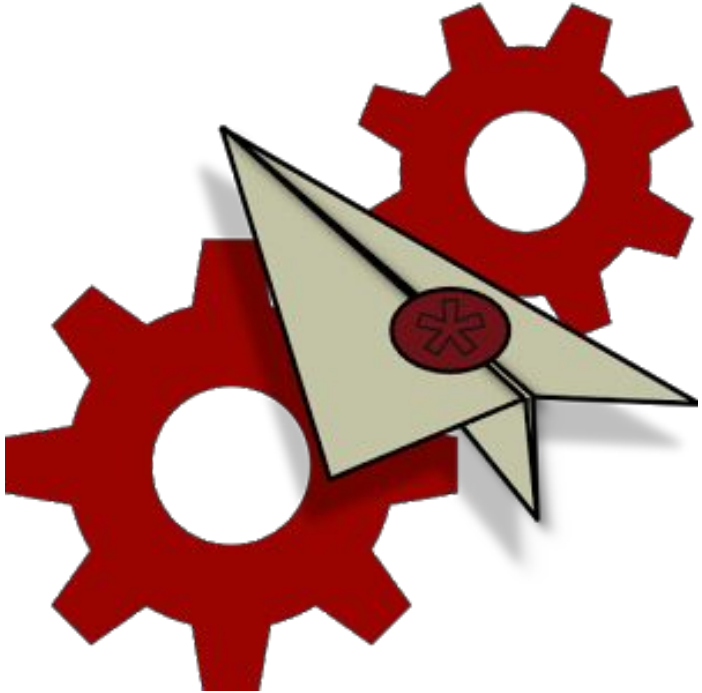
users physically located in different places?

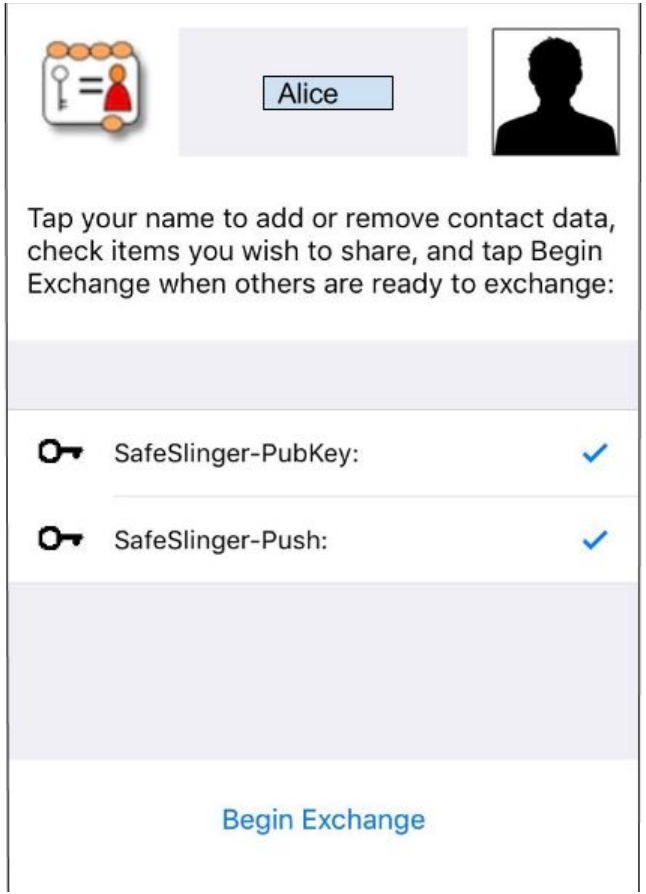
How can I verify identity of the group member?

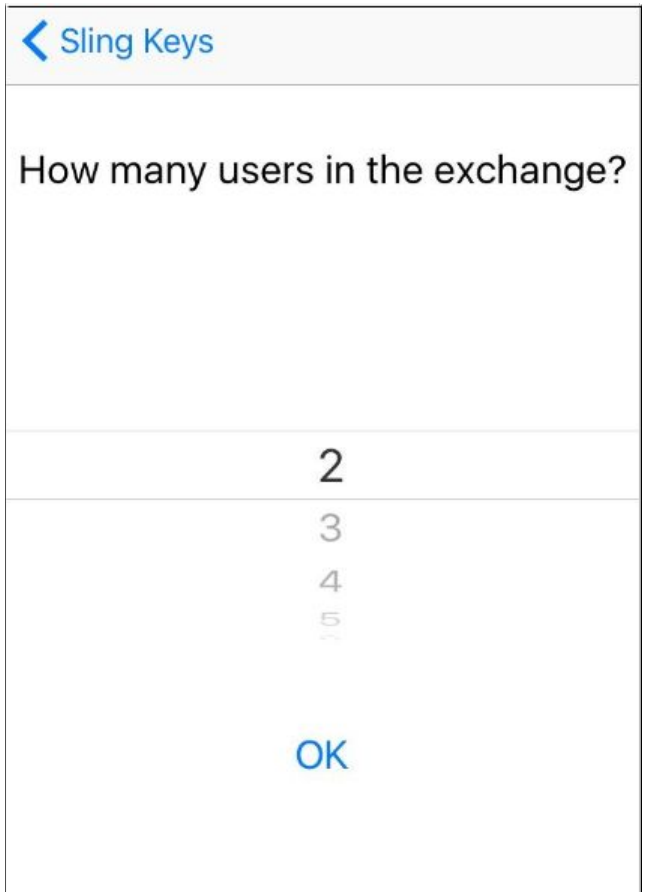
- QR code scan
- Manual fingerprint verification

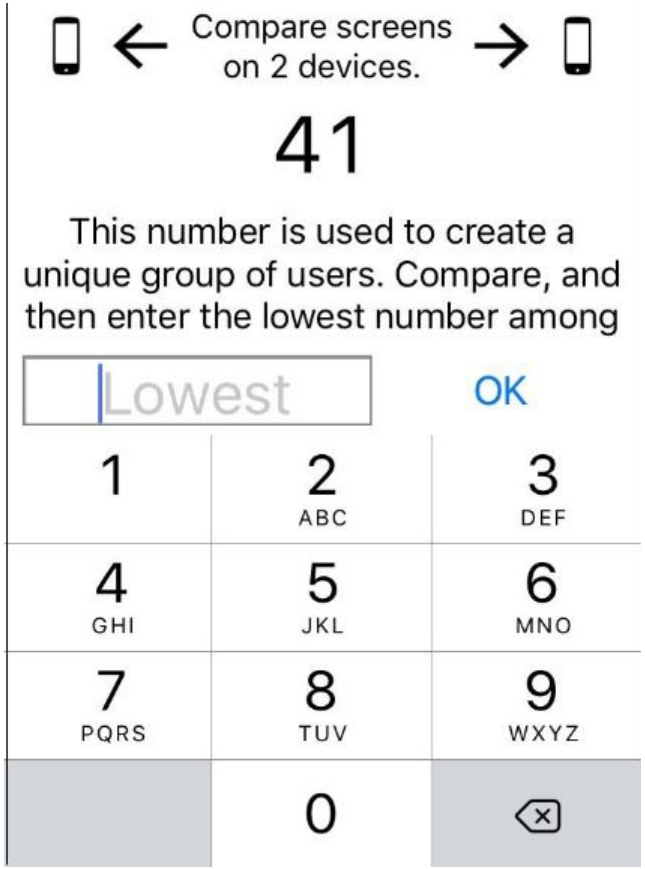

15:15
Verify identity
Their identity (they read):
05 8c 2a 42 26 e8 ca 9e
4e ac 6c c5 55 b3 d5 4d
8a c6 57 ac 70 a6 bd b0
bf f4 21 c9 13 aa 05 dd
31
Your identity (you read):
05 01 99 c2 42 45 74 b5
3c da 9d 4e 5b b6 05 23
10 36 bd 74 25 4e 1e a9
ac bb ac 77 ed 58 c5 9f
6c

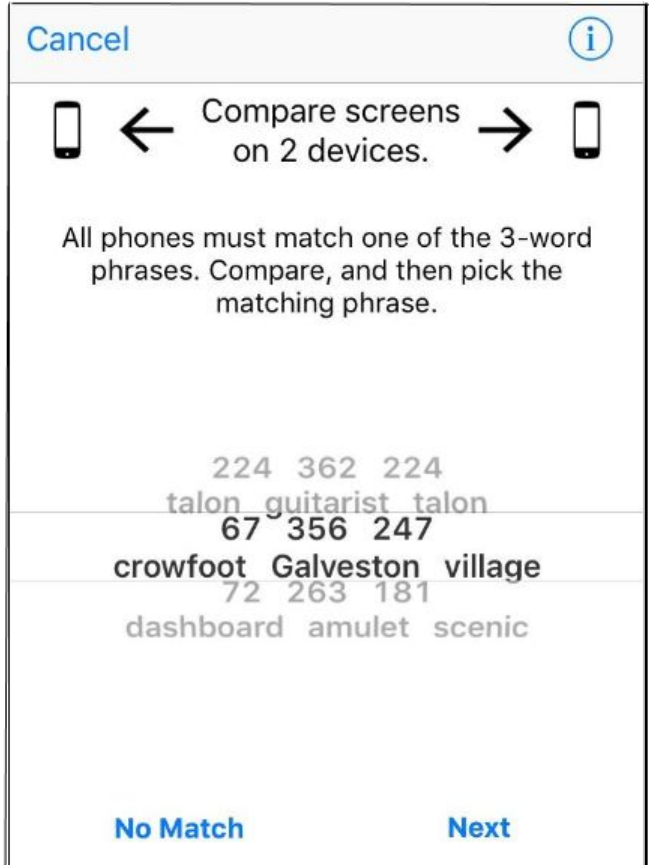
SafeSlinger exchange

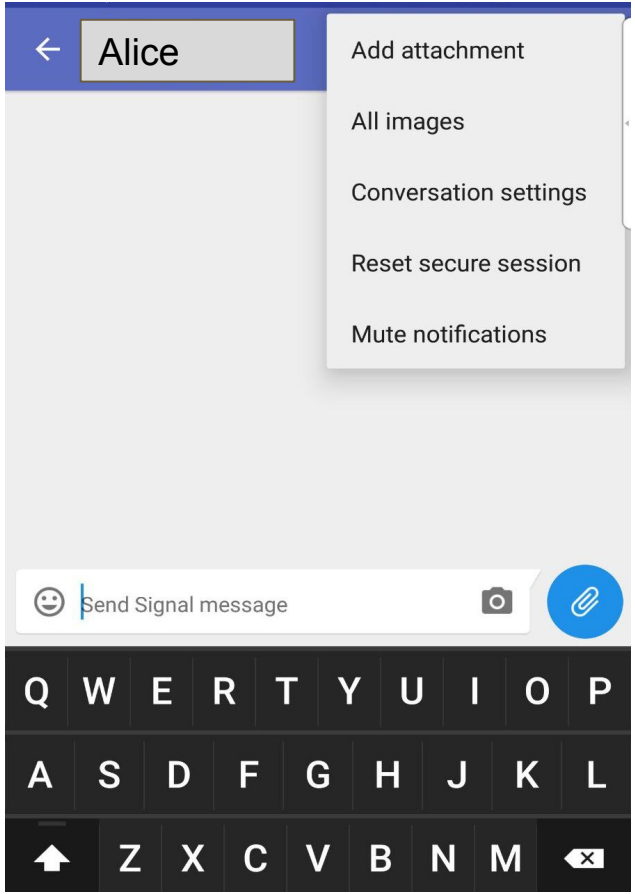


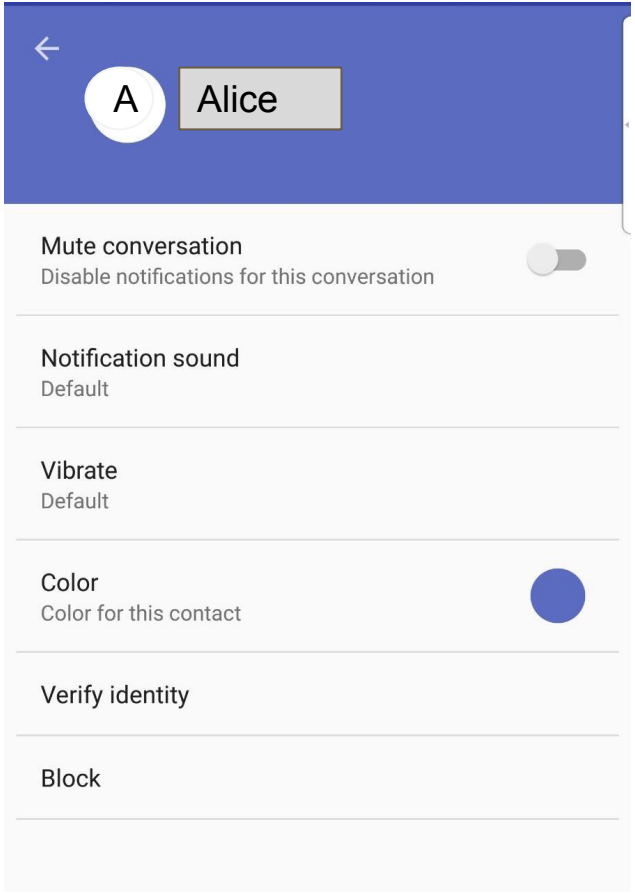

Alice
Tap your name to add or remove contact data, check items you wish to share, and tap Begin Exchange when others are ready to exchange:
SafeSlinger-PubKey:
SafeSlinger-Push:
Begin Exchange

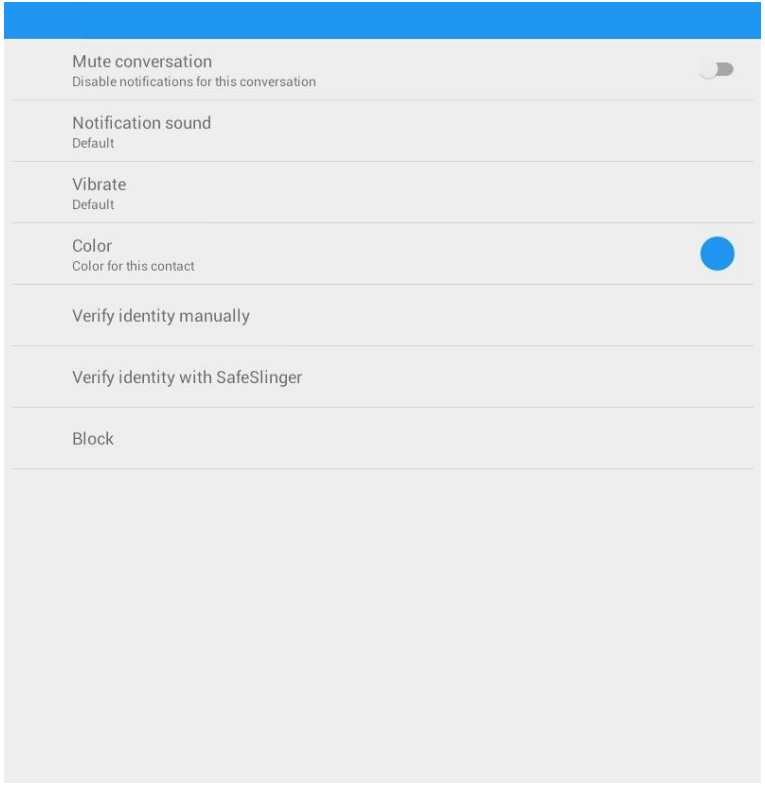

Sling Keys
How many users in the exchange?
2
3
4
OK

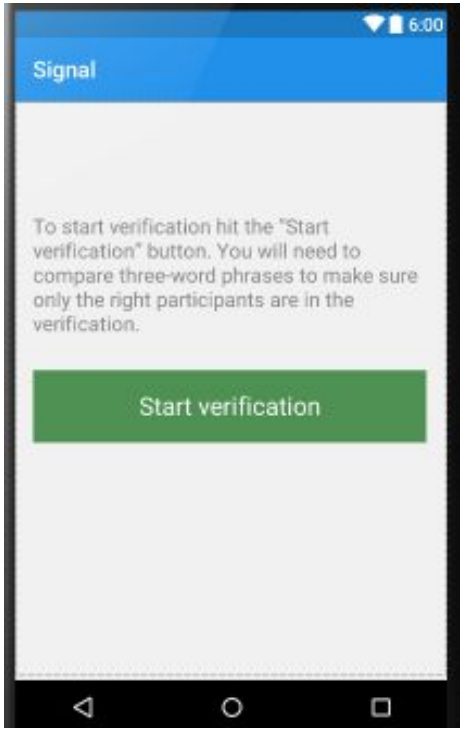

Compare screens on 2 devices.
41
This number is used to create a unique group of users. Compare, and then enter the lowest number among
Lowest
OK
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0


Cancel
Compare screens on 2 devices.
All phones must match one of the 3-word phrases. Compare, and then pick the matching phrase.
224 362 224
talon guitarist talon
67 356 247
crowfoot Galveston village
72 263 181
dashboard amulet scenic
No Match
Next


Alice
Add attachment
All images
Conversation settings
Reset secure session
Mute notifications
Send Signal message
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M

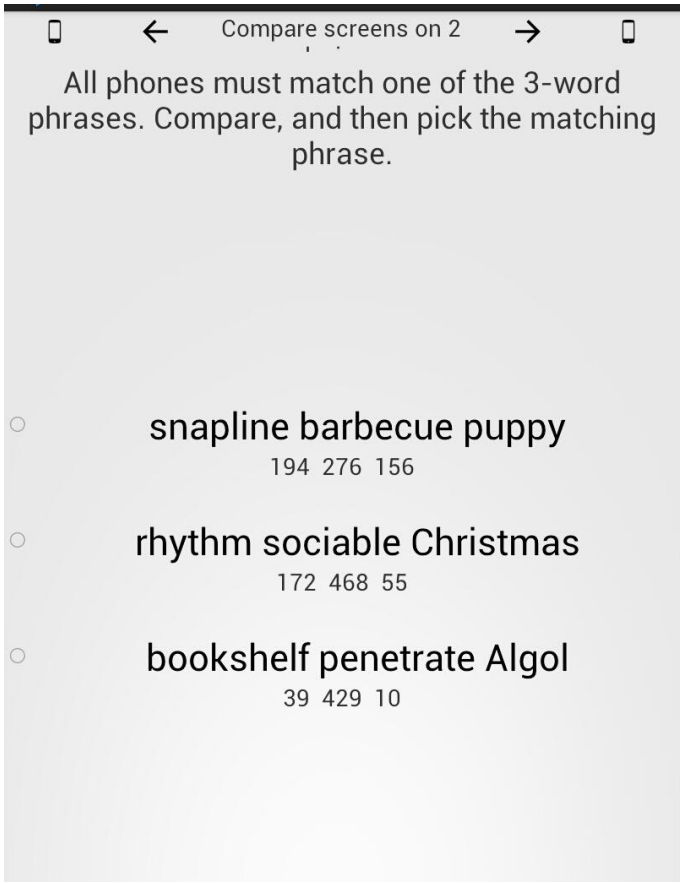

A
Alice
Mute conversation
Disable notifications for this conversation
Notification sound
Default
Vibrate
Default
Color
Color for this contact
Verify identity
Block

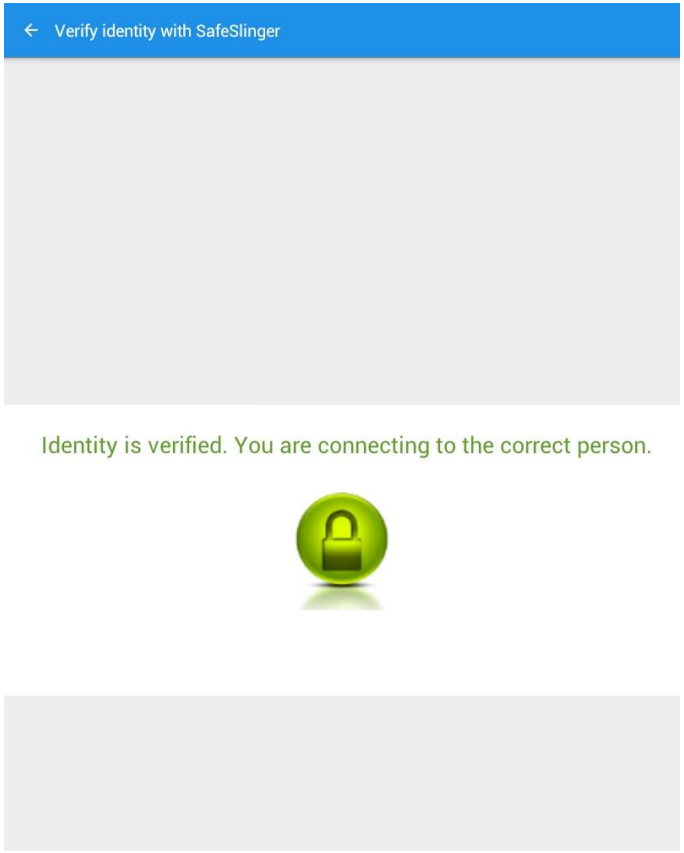

Mute conversation
Disable notifications for this conversation
Notification sound
Default
Vibrate
Default
Color
Color for this contact
Verify identity manually
Verify identity with SafeSlinger
Block

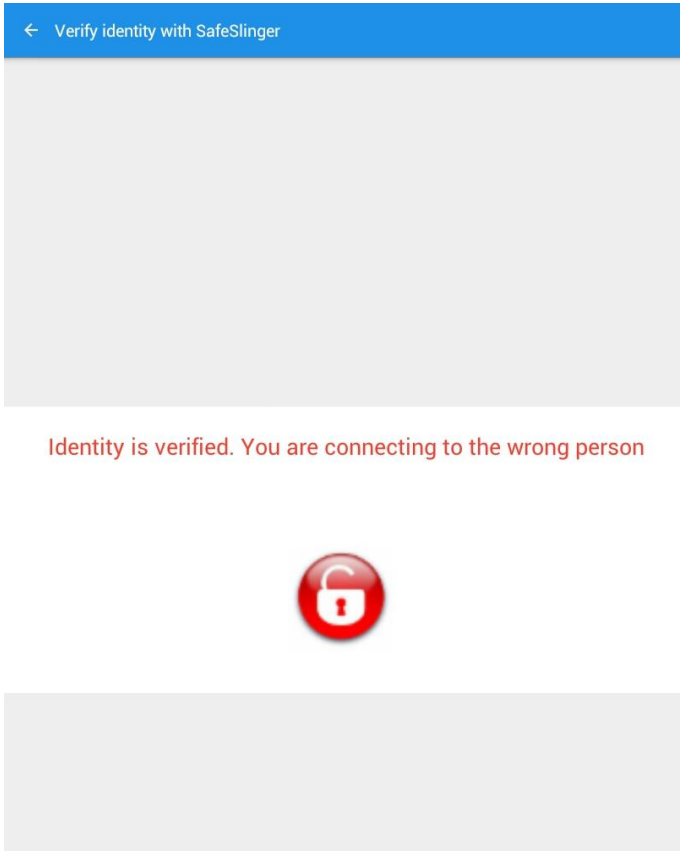

6:00
Signal
To start verification hit the "Start verification" button. You will need to compare three-word phrases to make sure only the right participants are in the verification.
Start verification

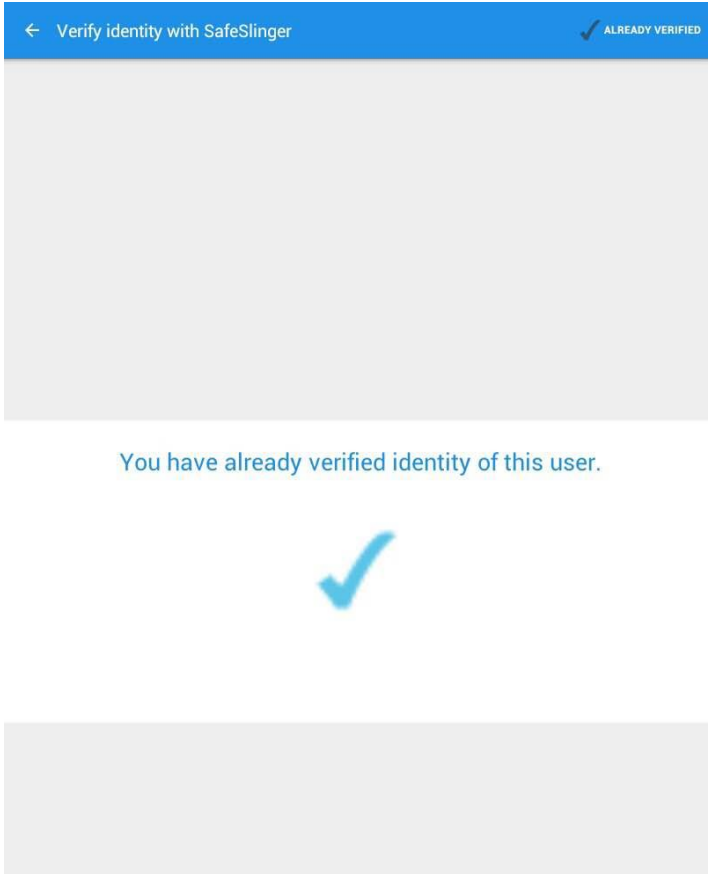
Start verification

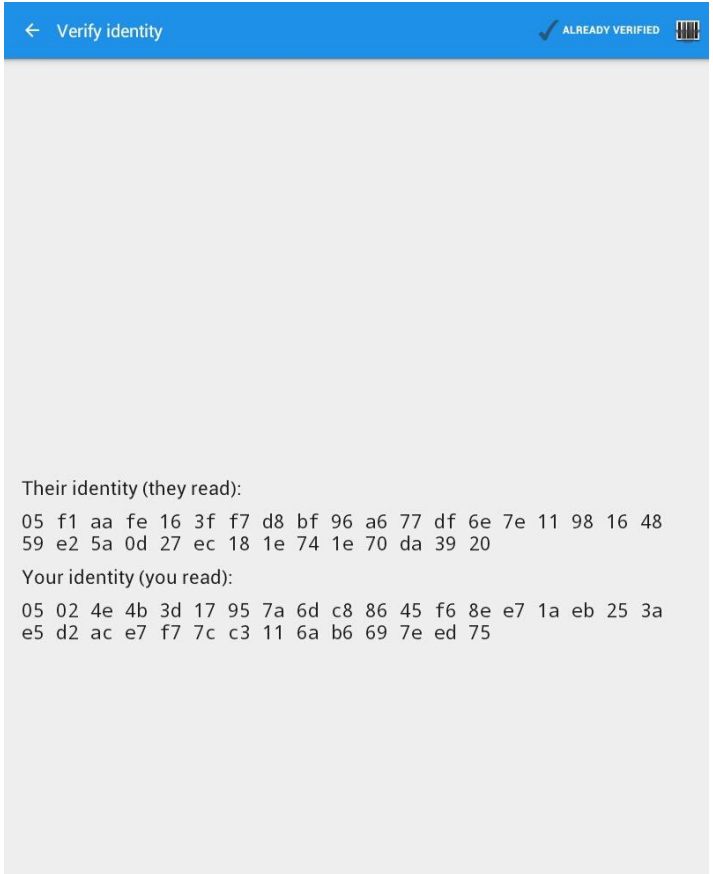
- Number of users in a group
- Fingerprint
- Group Name
- Attempt Name

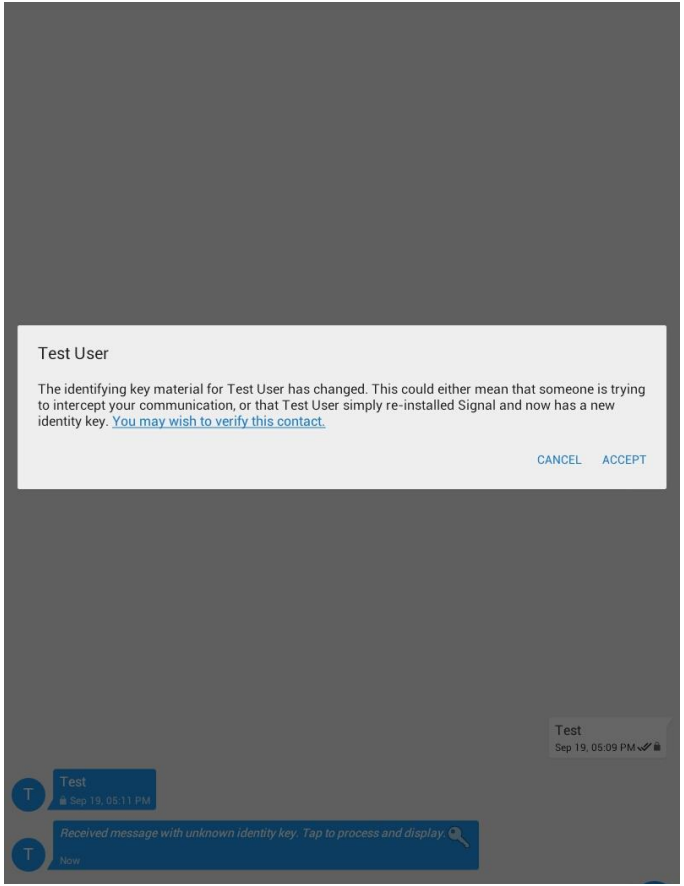

Compare screens on 2
All phones must match one of the 3-word phrases. Compare, and then pick the matching phrase.
snapline barbecue puppy
194 276 156
rhythm sociable Christmas
172 468 55
bookshelf penetrate Algol
39 429 10


Verify identity with SafeSlinger
Identity is verified. You are connecting to the correct person.


Verify identity with SafeSlinger
Identity is verified. You are connecting to the wrong person

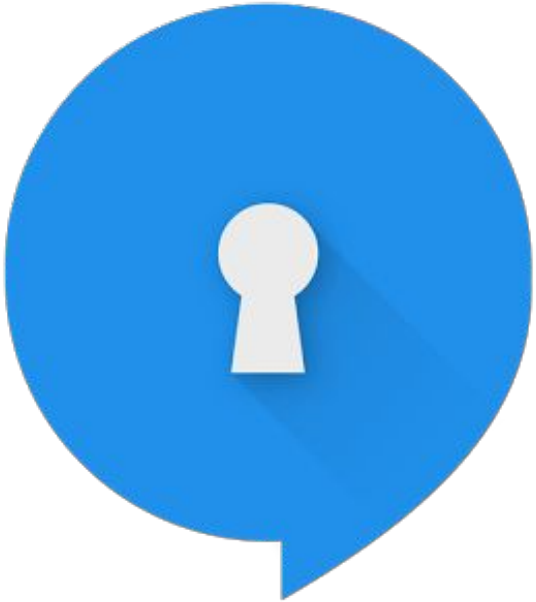

Verify identity with SafeSlinger
ALREADY VERIFIED
You have already verified identity of this user.


Verify identity
ALREADY VERIFIED
Their identity (they read):
05 f1 aa fe 16 3f f7 d8 bf 96 a6 77 df 6e 7e 11 98 16 48
59 e2 5a 0d 27 ec 18 1e 74 1e 70 da 39 20
Your identity (you read):
05 02 4e 4b 3d 17 95 7a 6d c8 86 45 f6 8e e7 1a eb 25 3a
e5 d2 ac e7 f7 7c c3 11 6a b6 69 7e ed 75


Test User
The identifying key material for Test User has changed. This could either mean that someone is trying to intercept your communication, or that Test User simply re-installed Signal and now has a new identity key. You may wish to verify this contact.
CANCEL
ACCEPT
Test
Sep 19, 05:09 PM
T
Test
Sep 19, 05:11 PM
T
Received message with unknown identity key. Tap to process and display.
Now

Technologies

- ★ Textsecure Server
- ★ Push Server
- ★ postgresql, redis and memcache
- ★ Certificates



Summary

Advantages of using SafeSlinger for identity verification:

- ★ More usable than manual fingerprint verification.
- ★ Secure user data exchange. Prevents MitM, GitM attacks.
- ★ Provides user privacy.
- ★ Efficient to use.

Future plan

- Verify identity of multiple users at the same time

References

- WhisperSystems/signal-android: A private messenger for android. https://github.com/WhisperSystems/Signal-Android.
- Y.-H. Lin T. H.-J. Kim J. McCune , M. Farb and A. Perrig. 'SafeSlinger: Easy-to-use and secure public-key exchange,'. in International Conference on Mobile Computing Networking, pages 417–428, ACM, 2013.
- SafeSlinger Project. https://github.com/SafeSlingerProject.

DEMO