# Secure (Desktop) Messengers

## Usability vs. Security

Securi-Tay 2017

24th February, 2017

@slashcrypto @pycycle

# $whoami$^2$

- David Wind & Christoph Rottermanner
- Bachelor degree in IT Security at the University of Applied Sciences St. Pölten
  - More info: https://www.fhstp.ac.at/en
- Currently Master in Information Security
- Working for XSEC in Vienna since more than two years
  - Focus on penetration testing, code-auditing and social engineering


Germany
Belgium
Luxembourg
Czechia
Slovakia
Austria
Switzerland
Liechtenstein
Hungary
Slovenia
Croatia
Bosnia and
Dortmund
Essen
Antwerp
Brussels
Cologne
Lille
Leipzig
Dresden
Wrocław
Kielce
Frankfurt
Prague
Katowice
Kraków
Rzeszow
Mannheim
Nuremberg
Ostrava
Zakopane
Brno
Karlsruhe
Stuttgart
Košice
Strasbourg
Augsburg
Munich
Vienna
Bratislava
Salzburg
Budapest
Debrecen
Zürich
Graz
Oradea
Szeged
Geneva
Lyon
Como
Milan
Verona
Venice
Trieste
Zagreb
Timişoara
Grenoble
Turin
Padua
Novi Sad
Нови Сад
Belgrade
Београд
Genoa
Bologna

# Agenda

- Secure Messengers - Recap
- Usability vs. Security
- Signal Usability Study
- Desktop Messengers
  - Signal Desktop
  - WhatsApp Web
  - General Issues
- Conclusion

# Secure Messengers | Recap

# Secure Messengers | Recap

## Signal on the outside, Signal on the inside

moxie0 on 30 Mar 2016

A few months ago we completed the process of unifying all of our apps across Android, iOS, and the Desktop under the name 'Signal.' This simplified the language around our apps and eliminated a lot of confusion. Now we're doing the same thing "inside" our apps by renaming Axolotl to Signal Protocol.

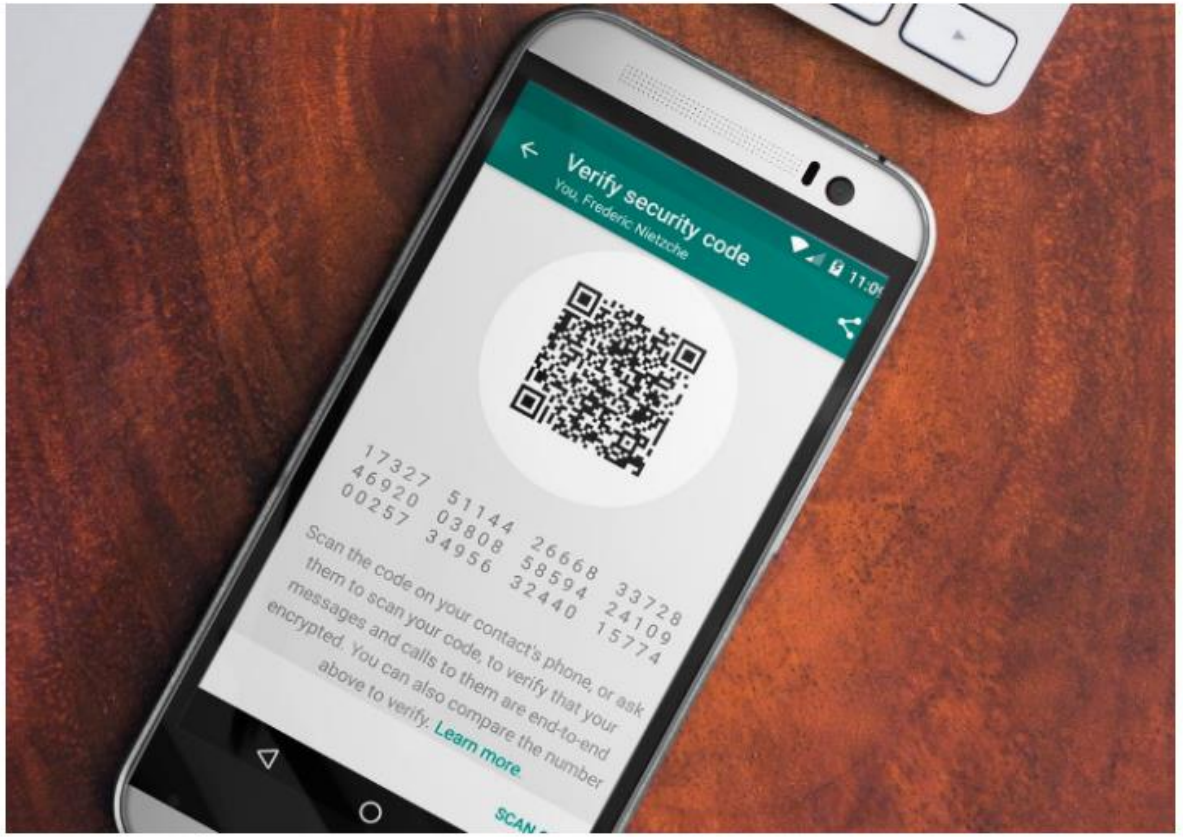
# Secure Messengers | Recap

Signa

A few months ago
and the Desktop u
eliminated a lot of
Axolotl to Signal Pr

## WhatsApp's Signal Protocol integration is now complete

moxie0 on 05 Apr 2016

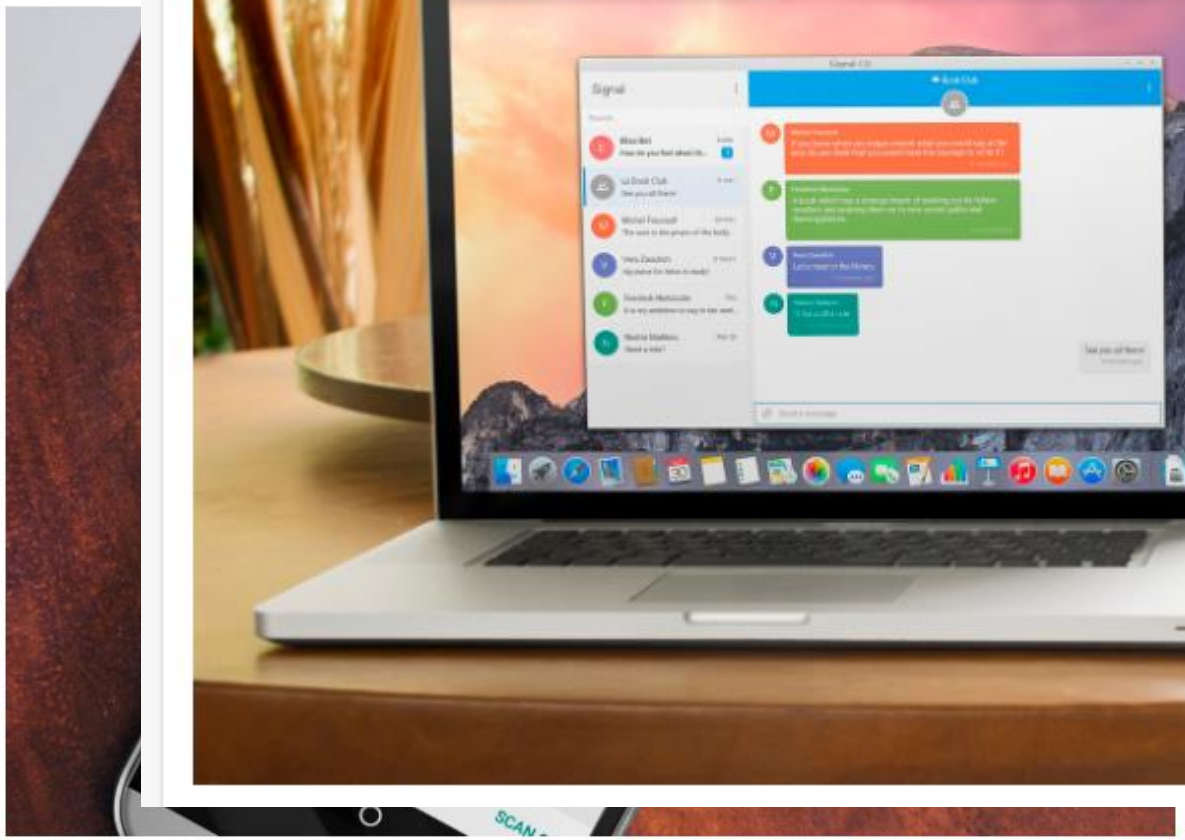


# Secure Me

Wh

Signa

A few months ago
and the Desktop u
eliminated a lot of
Axolotl to Signal Pr

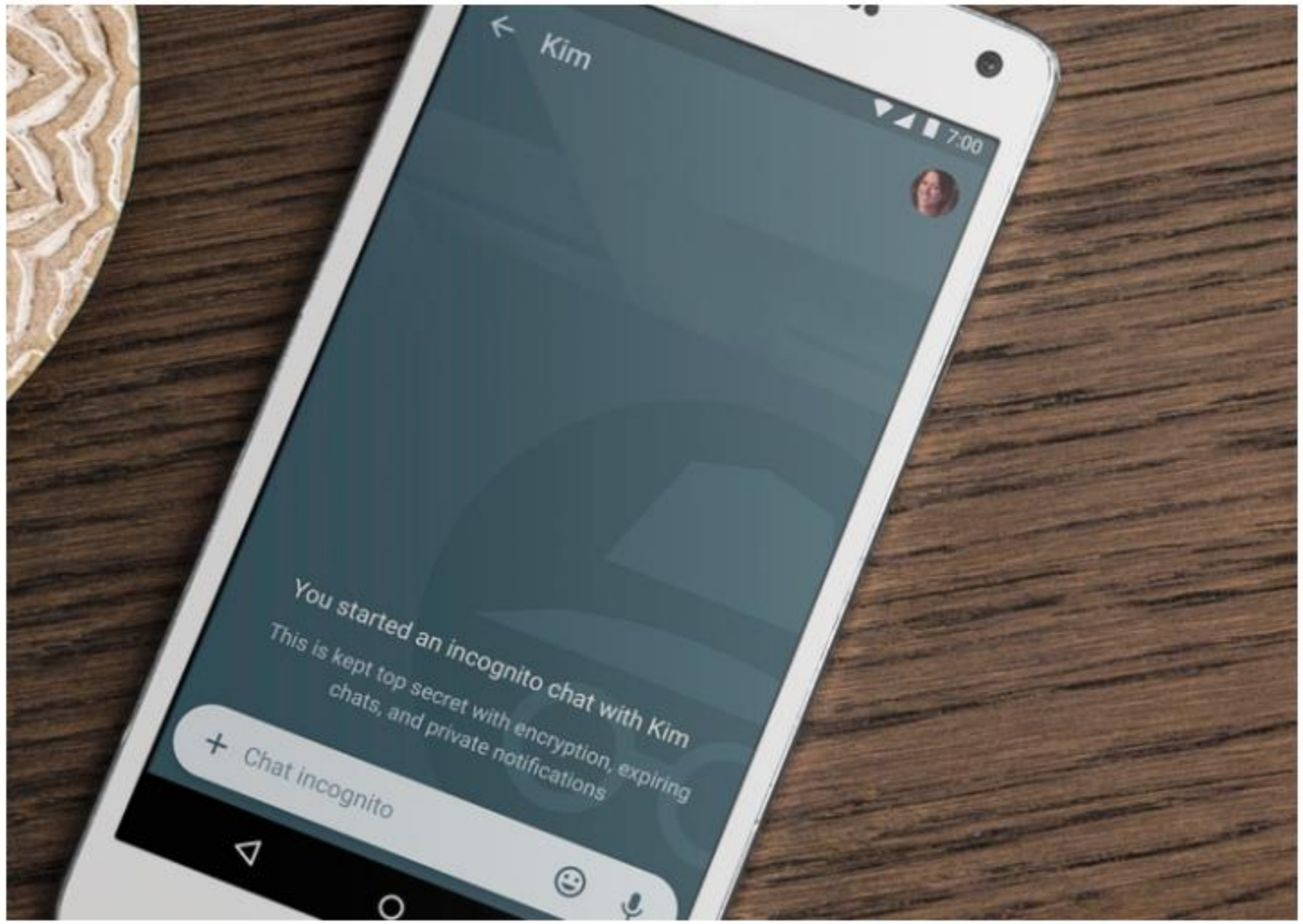


## Signal Desktop beta now publicly available

liliakai on 07 Apr 2016

# Open Whisper Systems partners with Google on end-to-end encryption for Allo

moxie0 on 18 May 2016

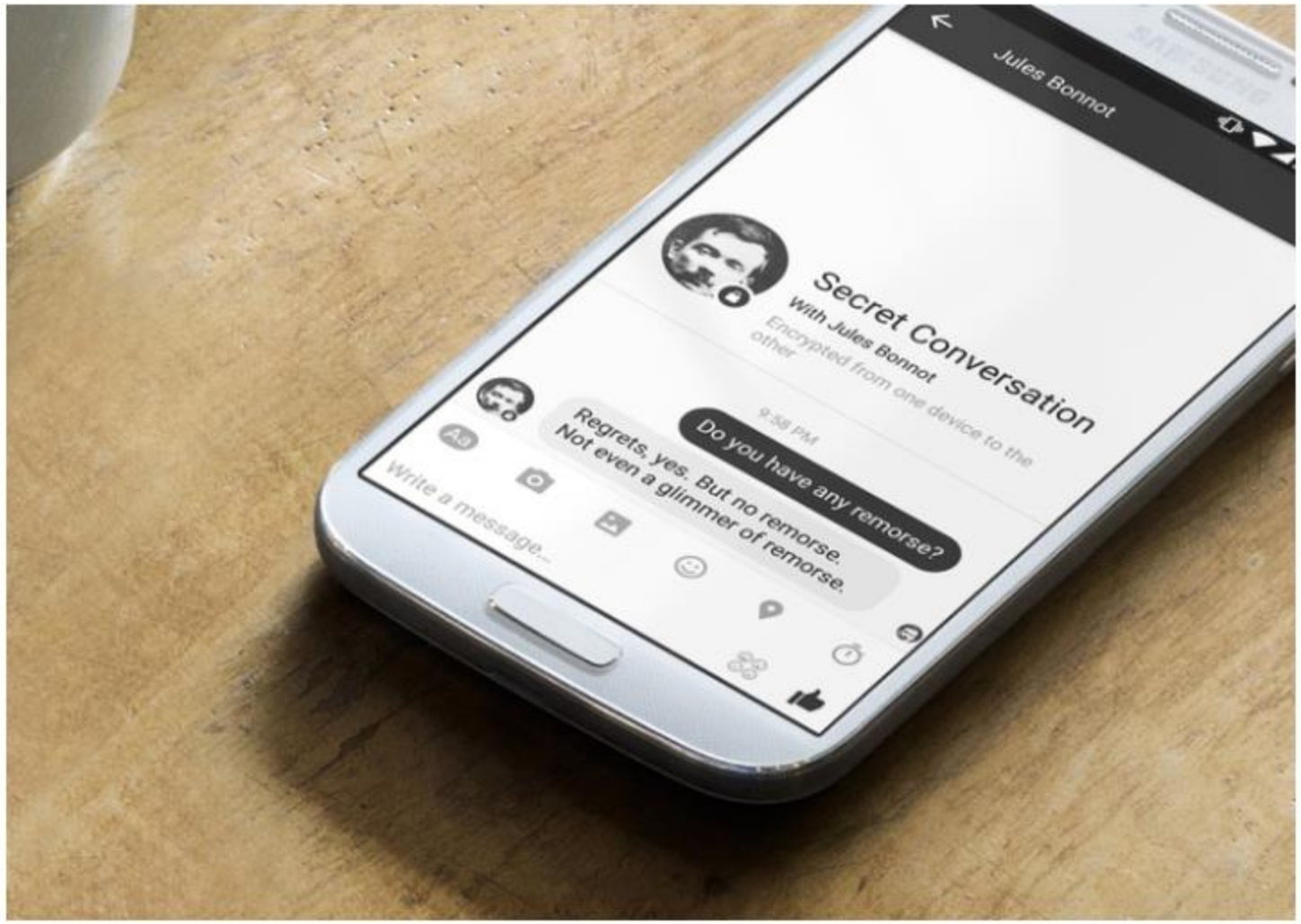



cly available

Open W

# Facebook Messenger deploys Signal Protocol for end to end encryption

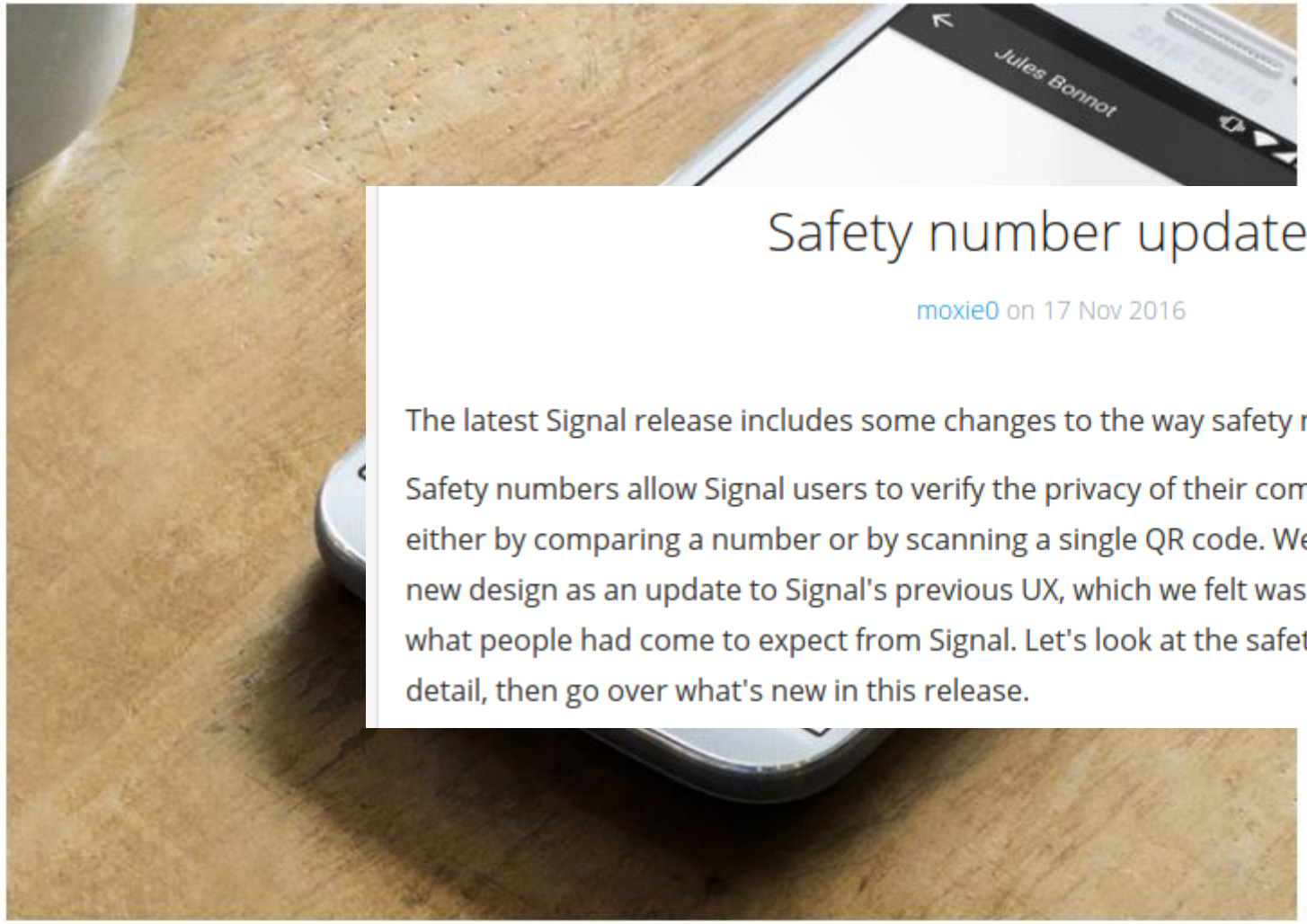
moxie0 on 08 Jul 2016

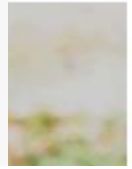


Open W

# Facebook Messenger deploys Signal Protocol for end to end encryption

moxie0 on 08 Jul 2016



# Safety number updates

moxie0 on 17 Nov 2016

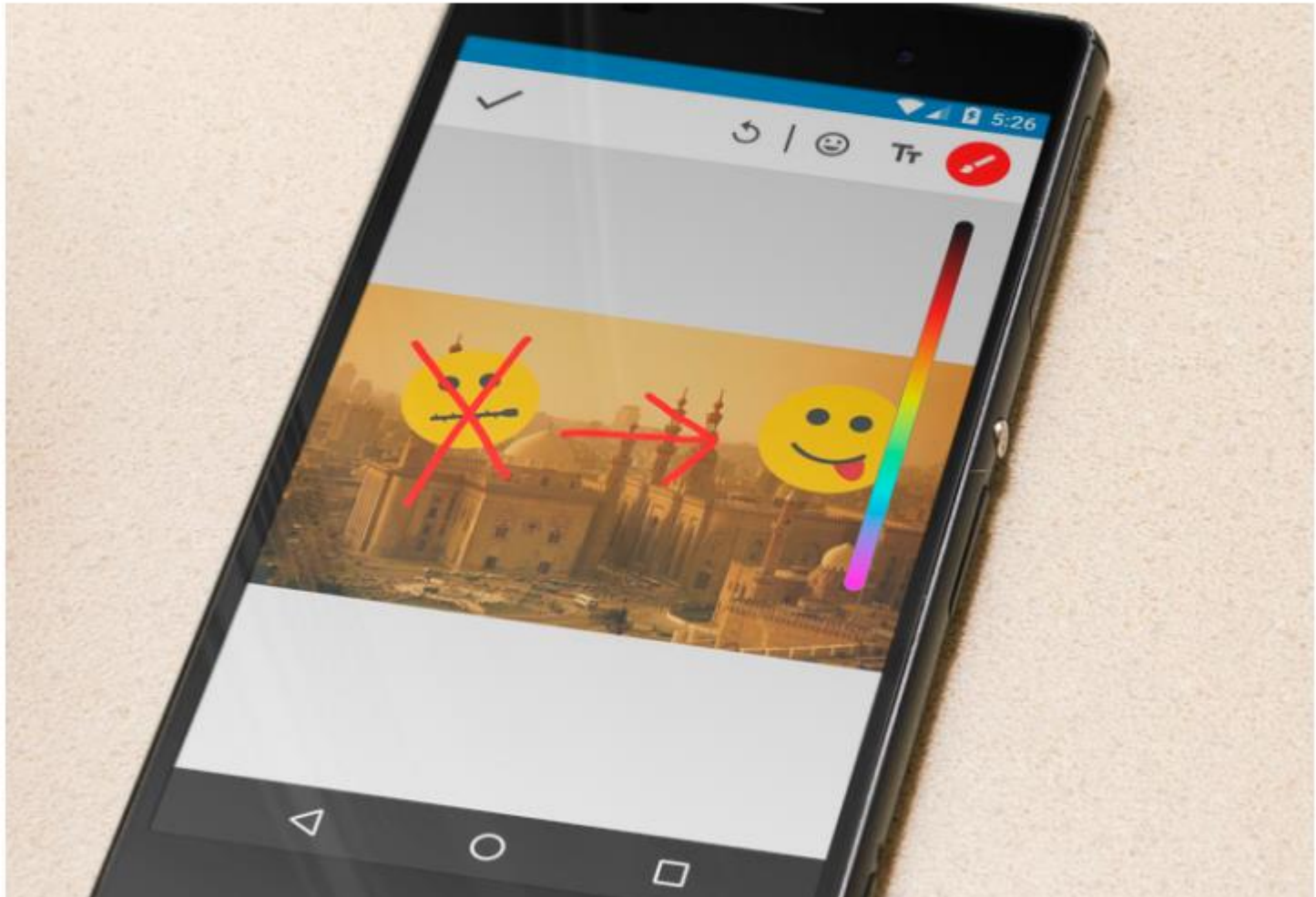
The latest Signal release includes some changes to the way safety numbers work.

Safety numbers allow Signal users to verify the privacy of their communication with a contact, either by comparing a number or by scanning a single QR code. We recently introduced this new design as an update to Signal's previous UX, which we felt was no longer adequate for what people had come to expect from Signal. Let's look at the safety numbers design in more detail, then go over what's new in this release.

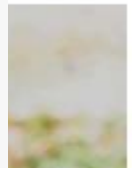
# Doodles, stickers, and censorship circumvention for Signal Android

moxie0 on 21 Dec 2016

The latest Signal for Android release includes support for adding doodles, stickers, and text to images.




ol for end

per updates

7 Nov 2016

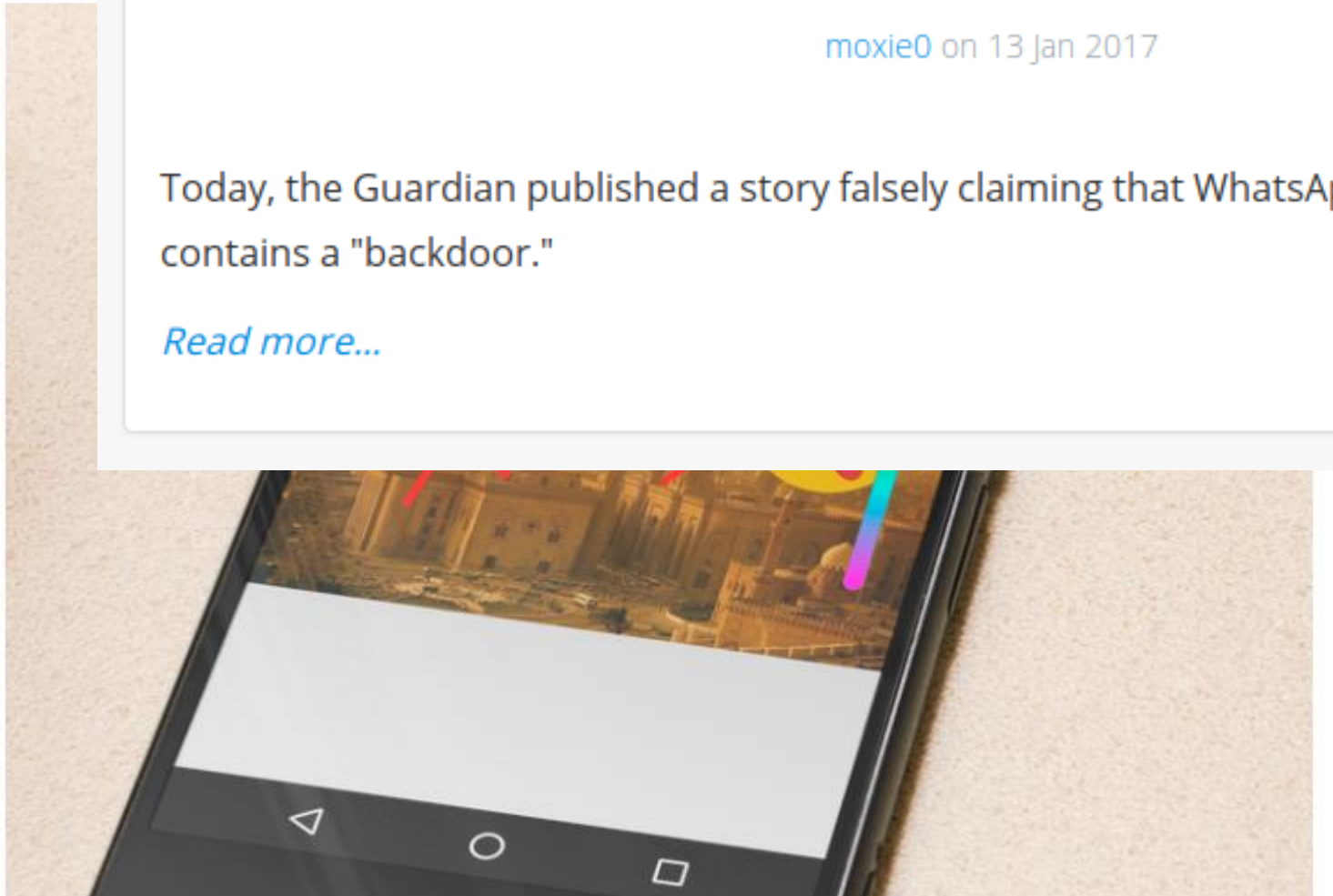
to the way safety numbers work.

rivacy of their communication with a contact,
single QR code. We recently introduced this
, which we felt was no longer adequate for
t's look at the safety numbers design in more

# Doodles, stickers, and censorship circumvention for Signal Android

moxie0 on 21 Dec 2016

The lat
image



# There is no WhatsApp 'backdoor'

moxie0 on 13 Jan 2017

Today, the Guardian published a story falsely claiming that WhatsApp's end to end encryption contains a "backdoor."

*Read more...*

ol for end

ontact,
d this
, which we felt was no longer adequate for
t's look at the safety numbers design in more

# Usability vs. Security

# WhatsApp vulnerability allows snooping on encrypted messages

**Exclusive**: Privacy campaigners criticise WhatsApp vulnerability as a 'huge threat to freedom of speech' and warn it could be exploited by government agencies

A security vulnerability that can be used to allow Facebook and others to intercept and read encrypted messages has been found within its WhatsApp messaging service.

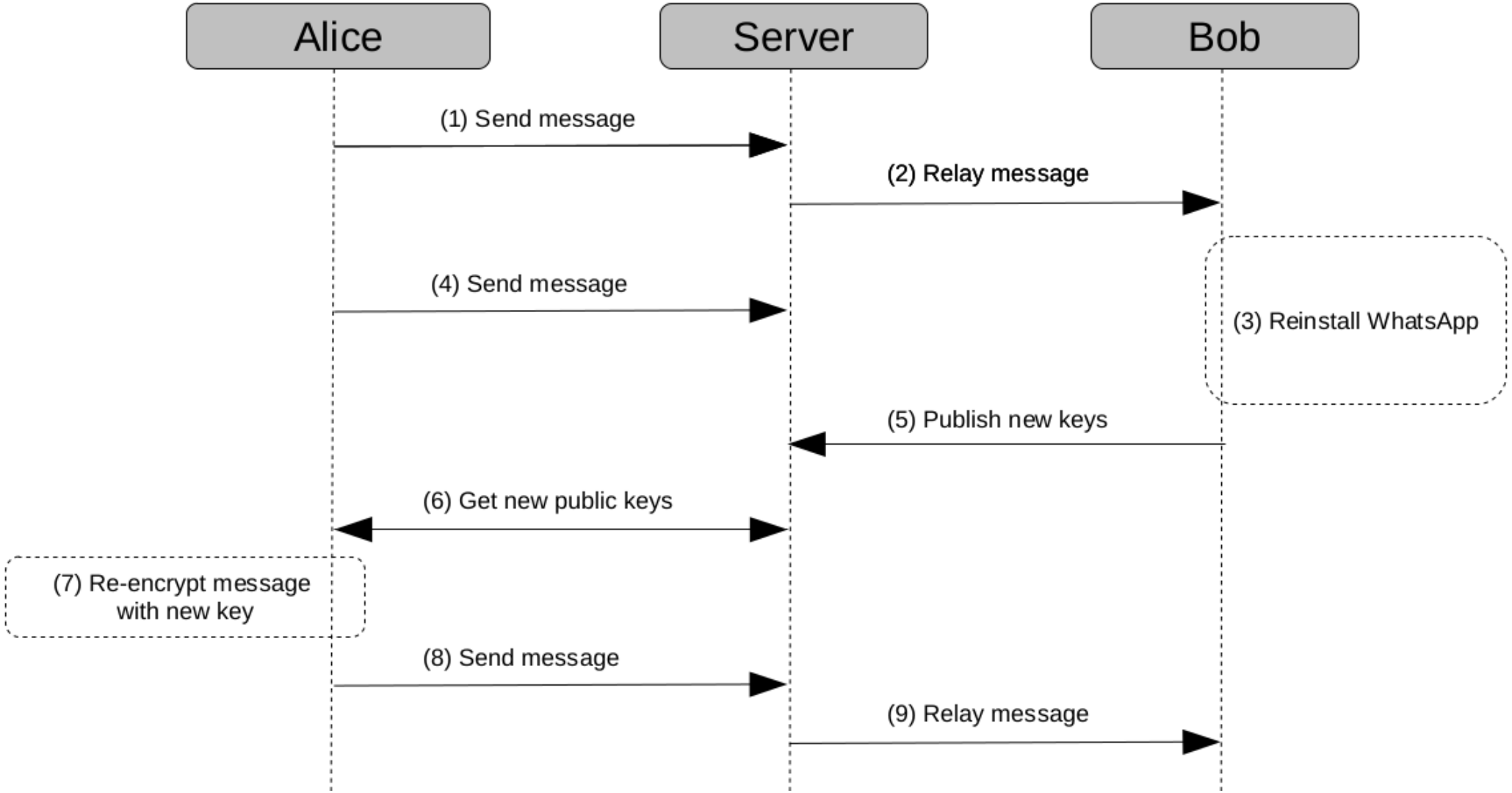
Facebook claims that no one can intercept WhatsApp messages, not even the company and its staff, ensuring privacy for its billion-plus users. But new research shows that the company could in fact read some messages due to the way WhatsApp has implemented its end-to-end encryption protocol.

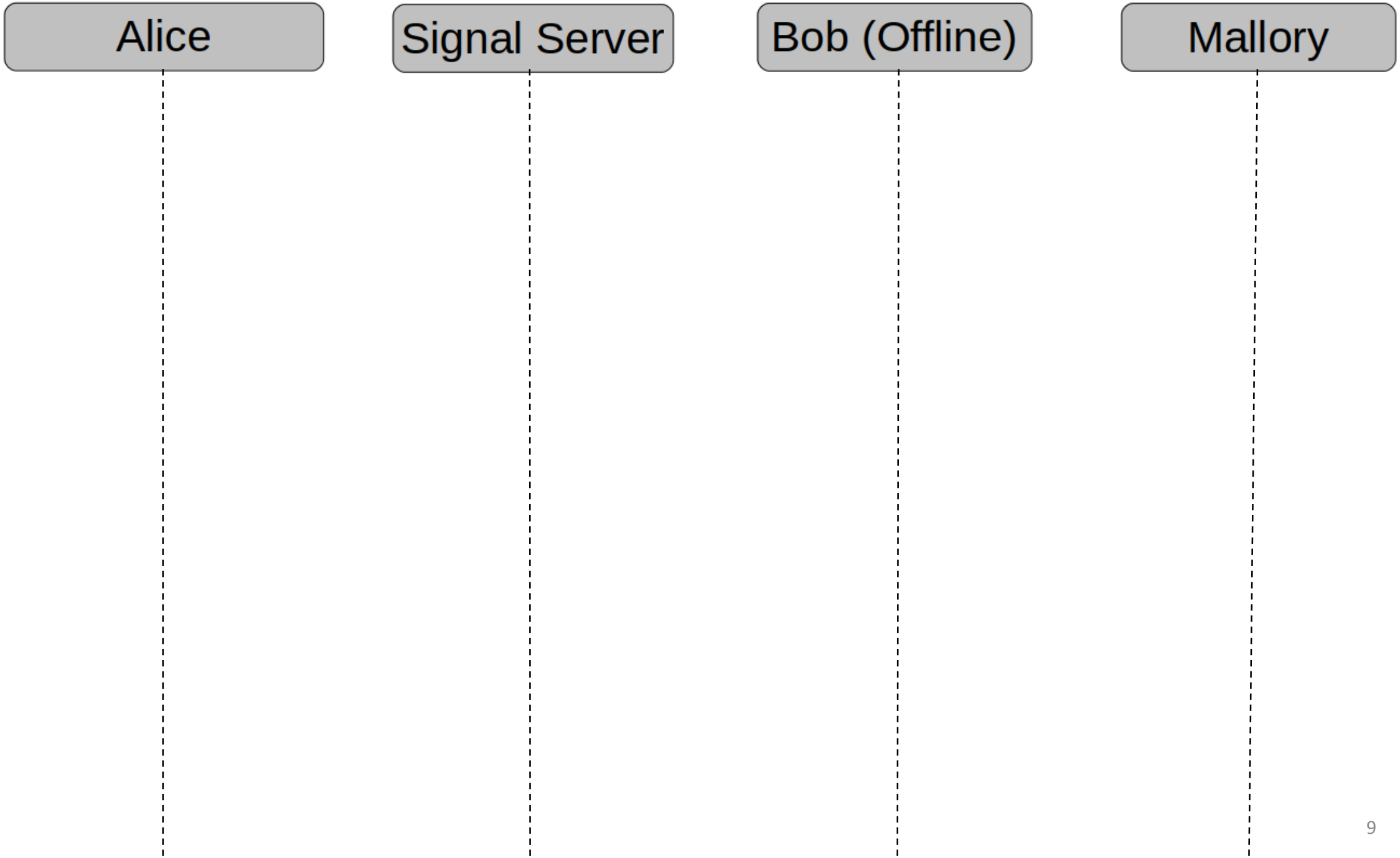
Privacy campaigners said the vulnerability is a "huge threat to freedom of speech" and warned it could be used by government agencies as a backdoor to snoop on users who believe their messages to be secure.

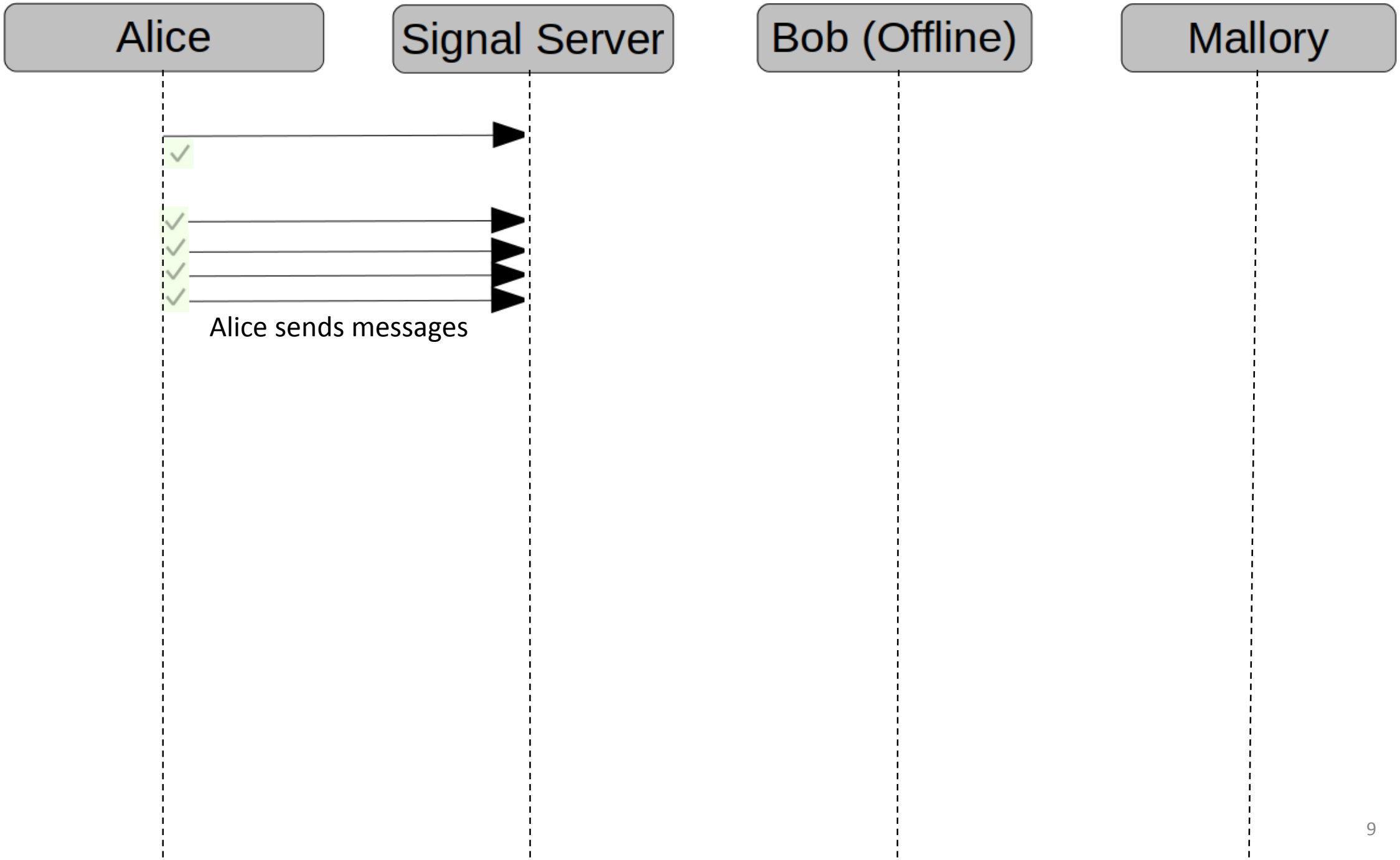


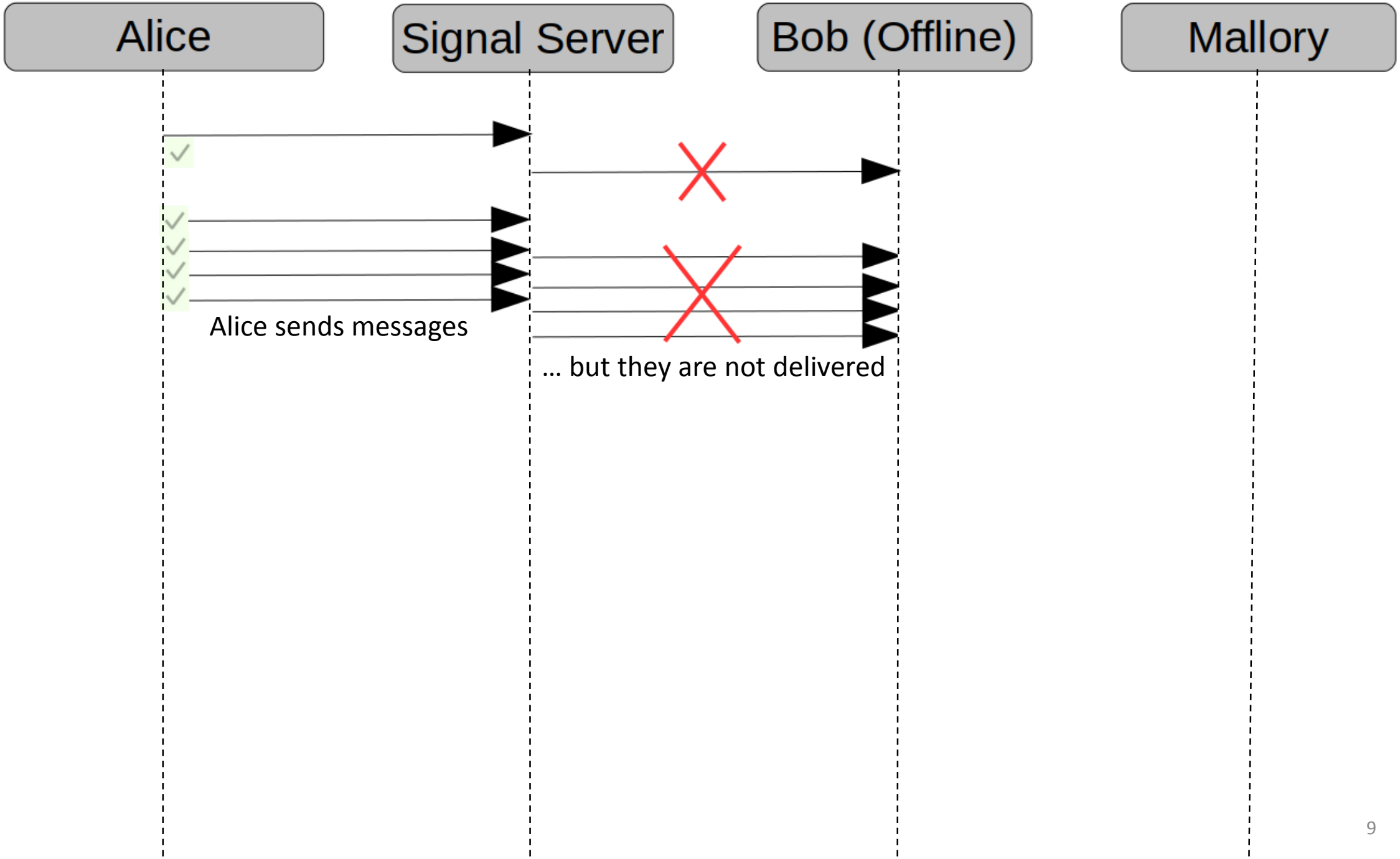
https://www.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages

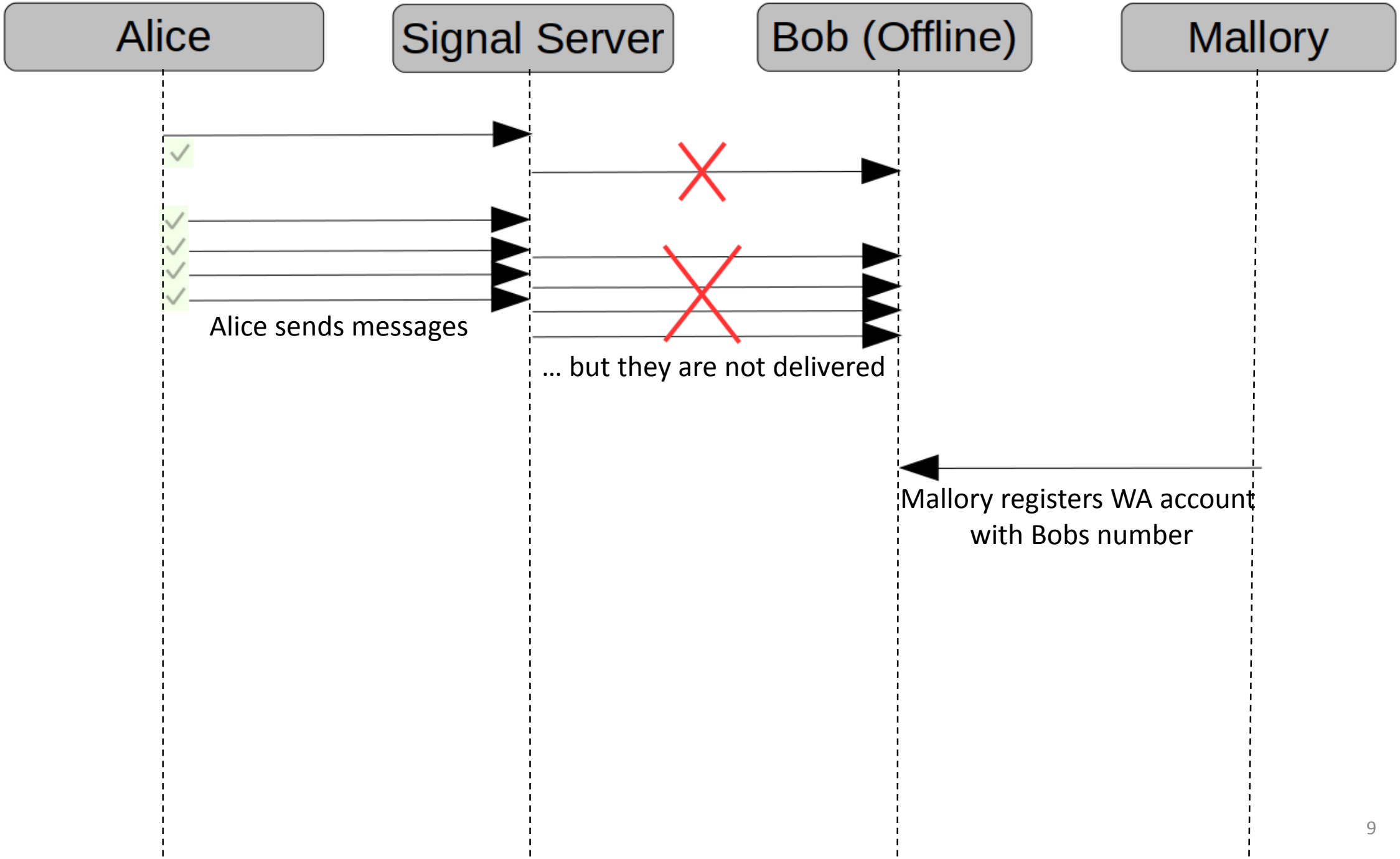
# Usability Feature or Backdoor?

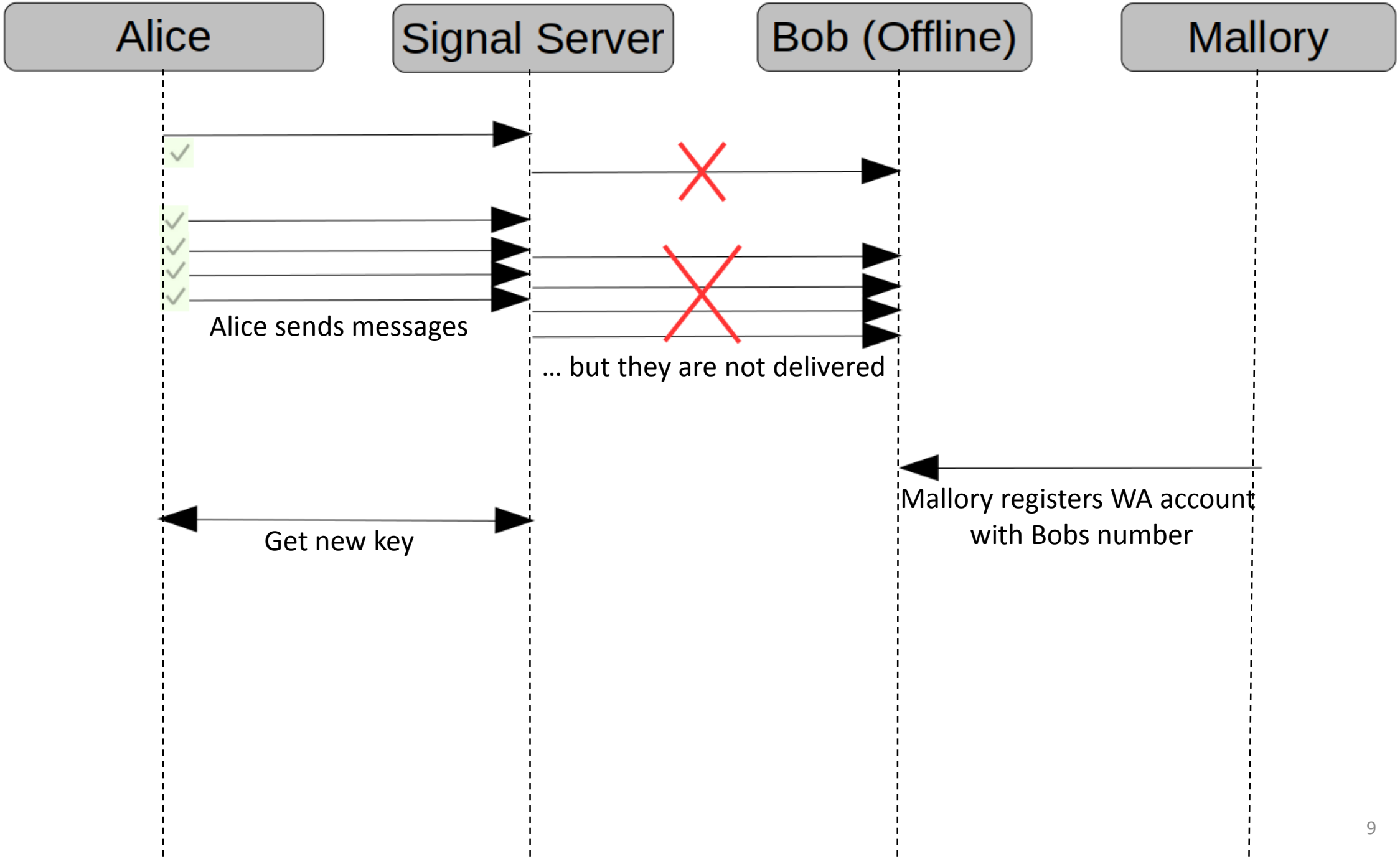


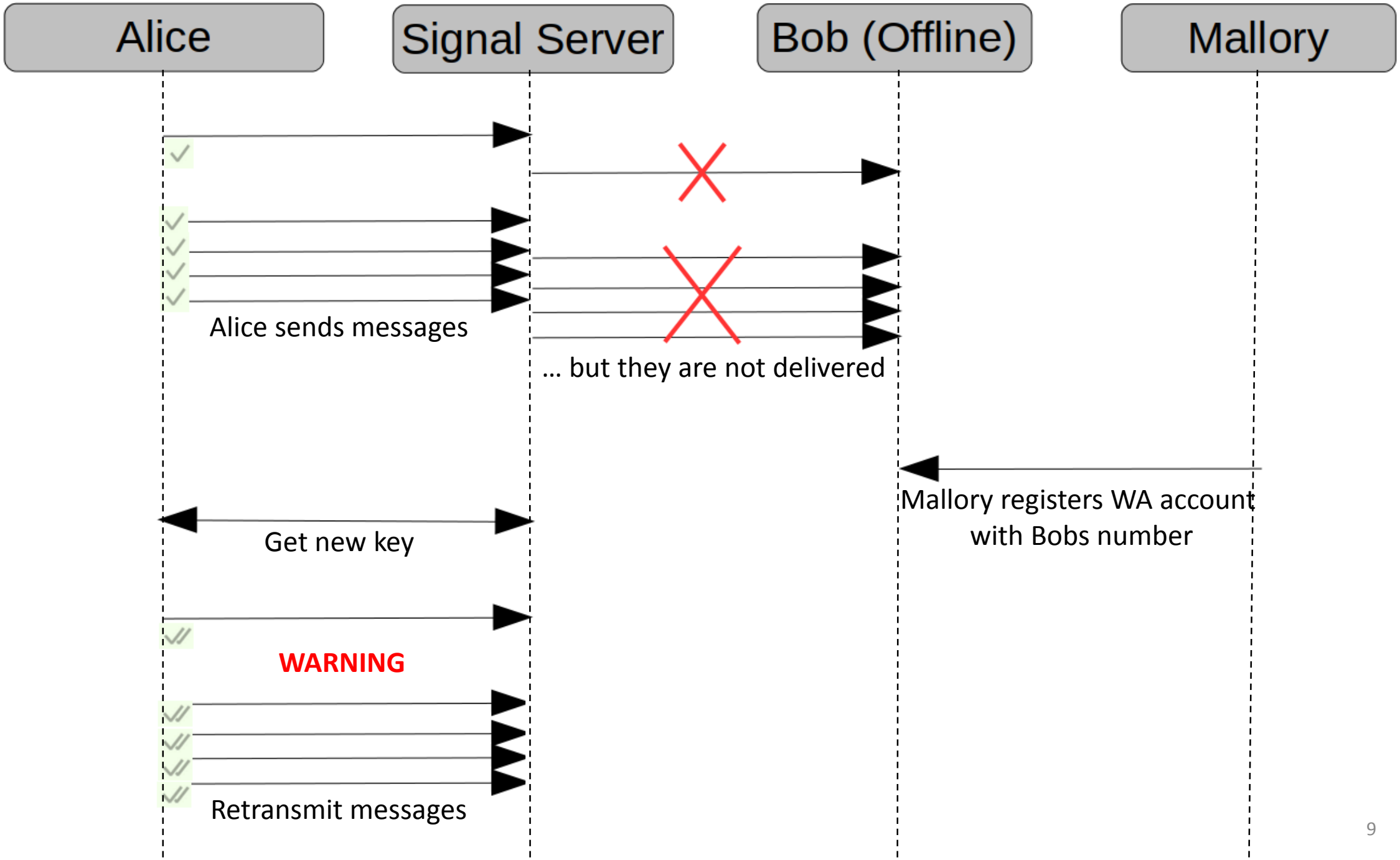

Alice
Signal Server
Bob (Offline)
Mallory

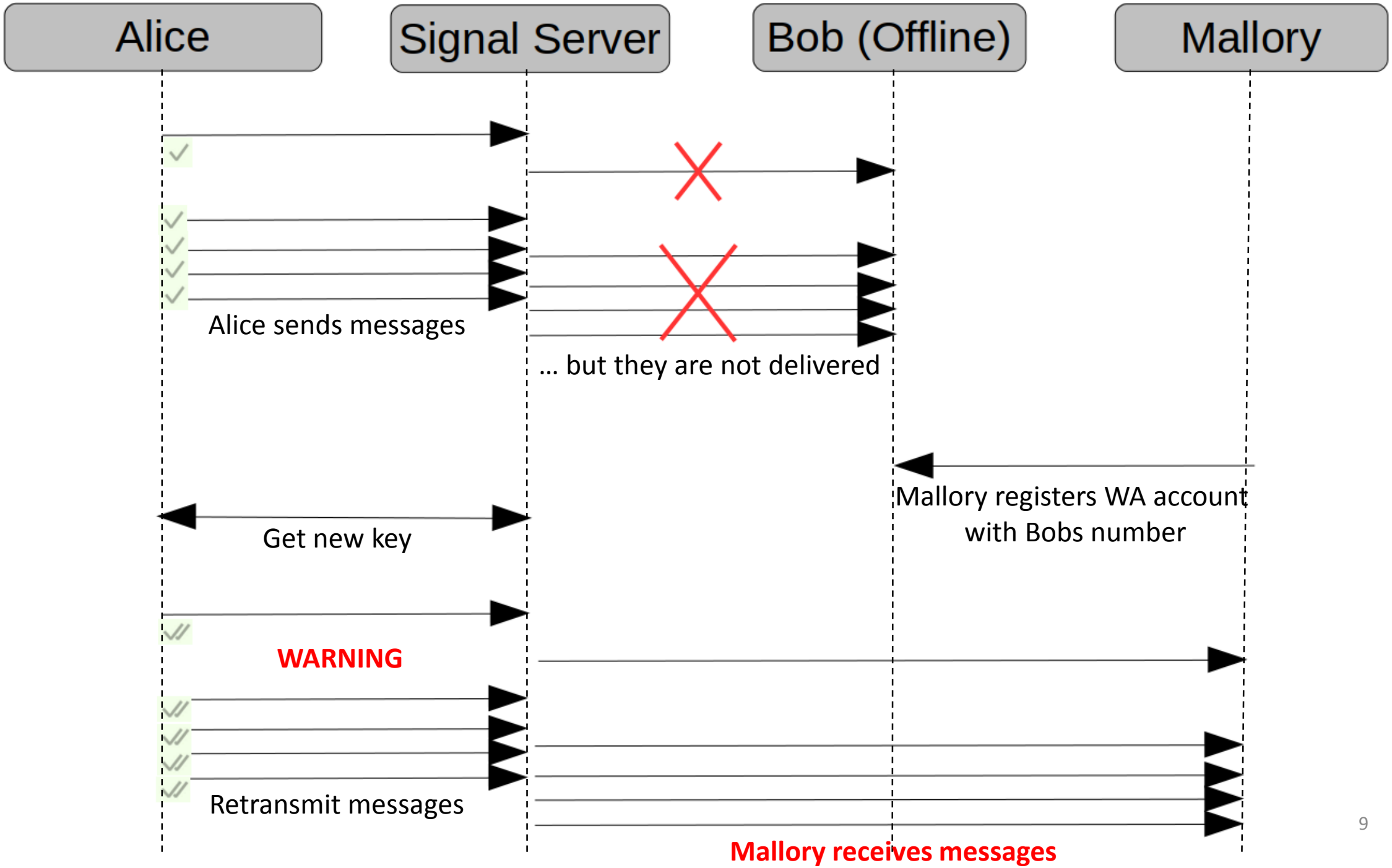

Alice
Signal Server
Bob (Offline)
Mallory
Alice sends messages


Alice
Signal Server
Bob (Offline)
Mallory
Alice sends messages
… but they are not delivered


Alice
Signal Server
Bob (Offline)
Mallory
Alice sends messages
… but they are not delivered
Mallory registers WA account
with Bobs number

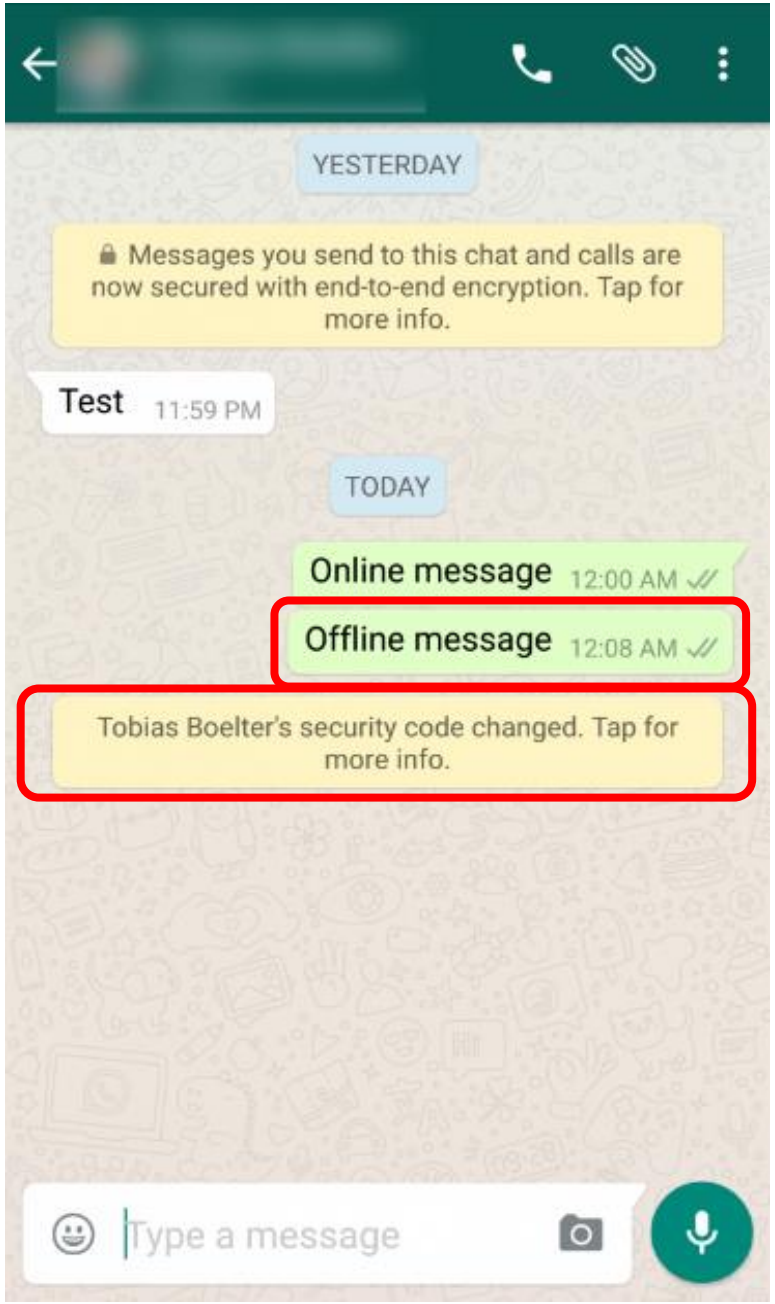

Alice
Signal Server
Bob (Offline)
Mallory
Alice sends messages
… but they are not delivered
Mallory registers WA account
with Bobs number
Get new key


Alice
Signal Server
Bob (Offline)
Mallory
Alice sends messages
… but they are not delivered
Mallory registers WA account
with Bobs number
Get new key
WARNING
Retransmit messages


Alice
Signal Server
Bob (Offline)
Mallory
Alice sends messages
… but they are not delivered
Mallory registers WA account
with Bobs number
Get new key
WARNING
Retransmit messages
Mallory receives messages

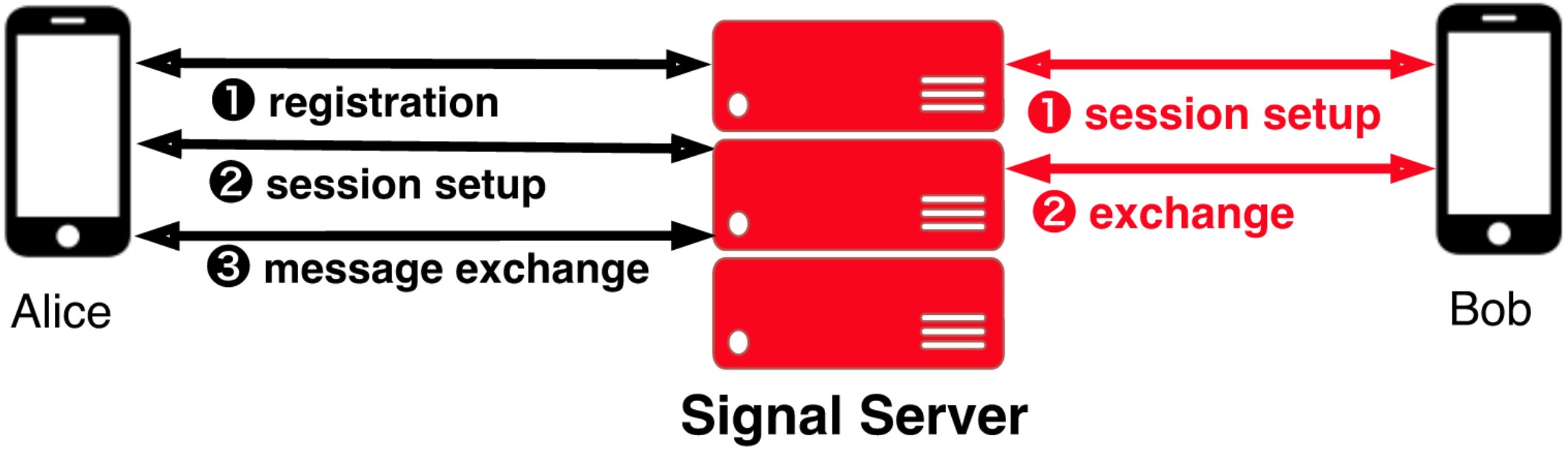

YESTERDAY
Messages you send to this chat and calls are now secured with end-to-end encryption. Tap for more info.
Test 11:59 PM
TODAY
Online message 12:00 AM
Offline message 12:08 AM
Type a message


YESTERDAY
Messages you send to this chat and calls are now secured with end-to-end encryption. Tap for more info.
Test 11:59 PM
TODAY
Online message 12:00 AM
Offline message 12:08 AM
Type a message

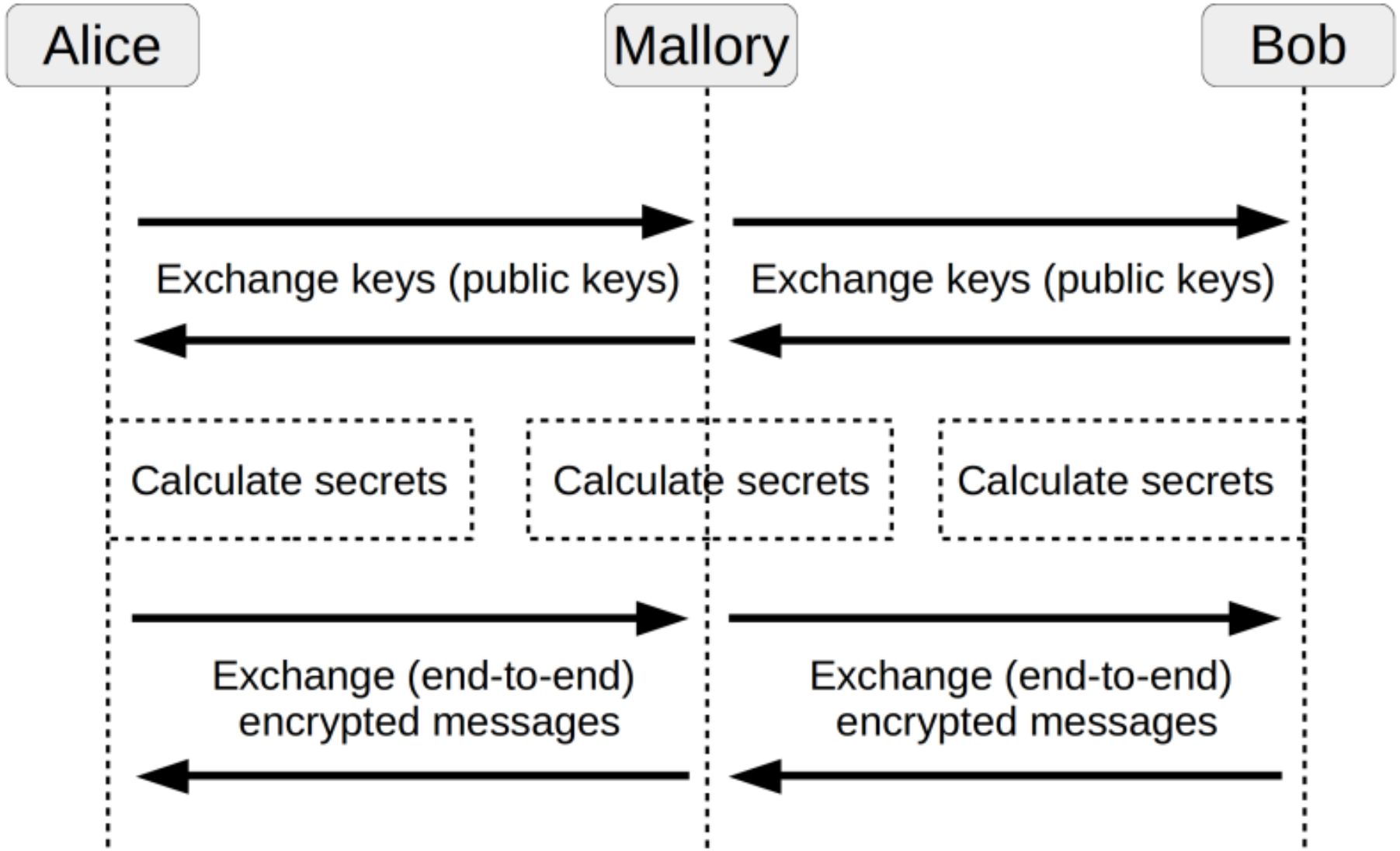

YESTERDAY
Messages you send to this chat and calls are now secured with end-to-end encryption. Tap for more info.
Test 11:59 PM
TODAY
Online message 12:00 AM
Offline message 12:08 AM
Tobias Boelter's security code changed. Tap for more info.
Type a message

# Signal Usability Study

# Usability Study | Threat Model



# Revision | MitM



# Usability Study | Tasks

# Usability Study | Tasks

1. Send messages to communication partner

# Usability Study | Tasks

1. Send messages to communication partner
2. Configure master password

# Usability Study | Tasks

1. Send messages to communication partner
2. Configure master password
3. Create backup of local data & restore backup

# Usability Study | Tasks

1. Send messages to communication partner
2. Configure master password
3. Create backup of local data & restore backup
4. Send messages again → MitM

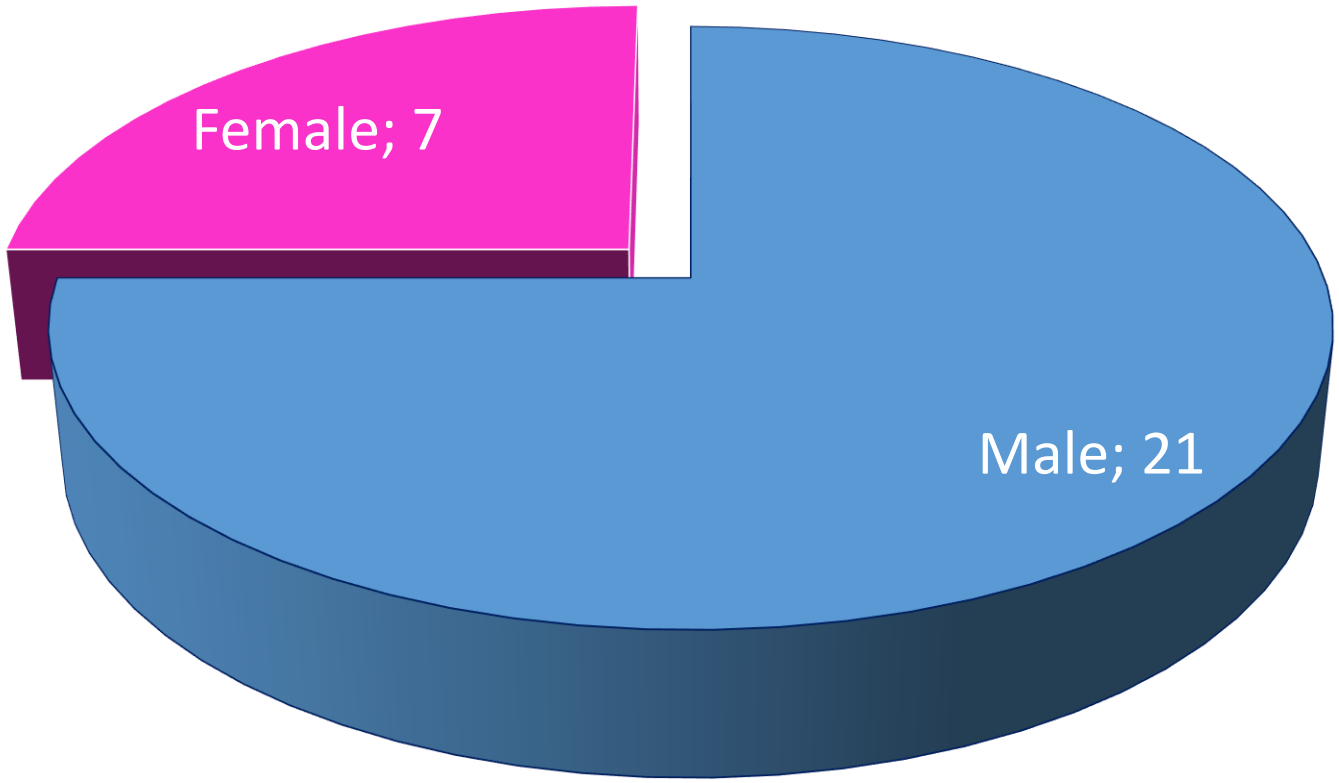
# Usability Study | Tasks

1. Send messages to communication partner
2. Configure master password
3. Create backup of local data & restore backup
4. Send messages again → MitM
5. Verify the identity of the other party

# Usability Study | Tasks

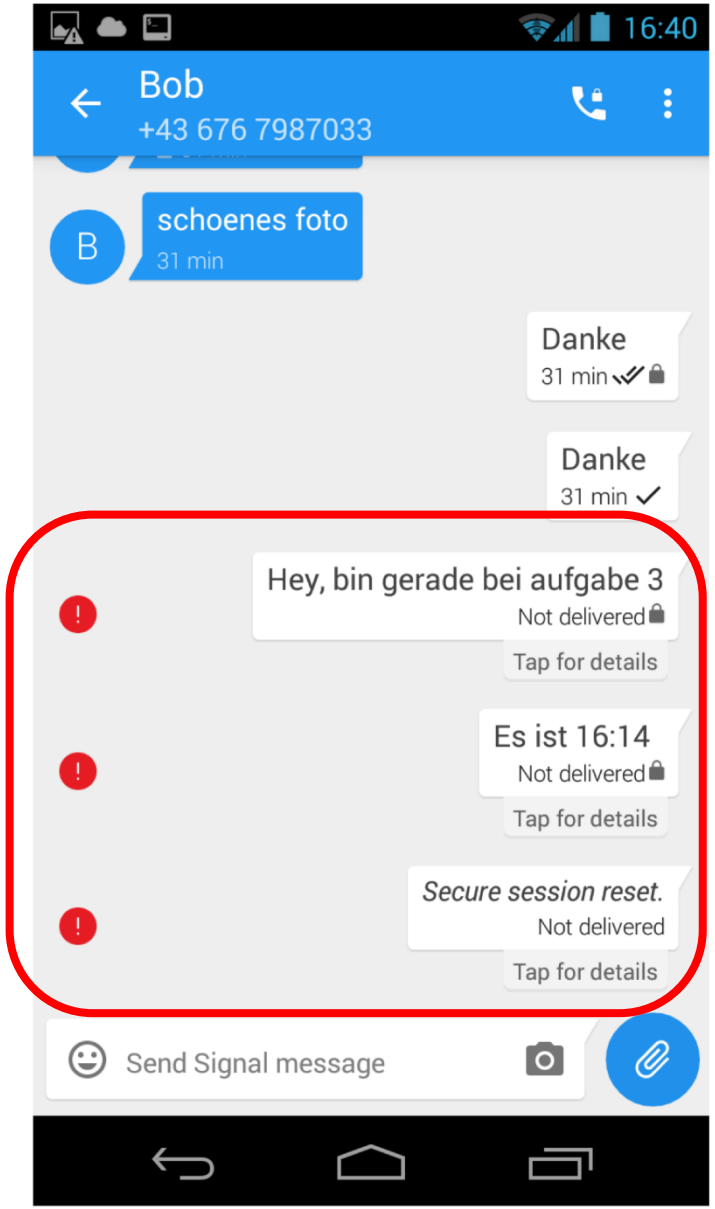
1. Send messages to communication partner
2. Configure master password
3. Create backup of local data & restore backup
4. Send messages again → MitM
5. Verify the identity of the other party
6. Interview: What happened?

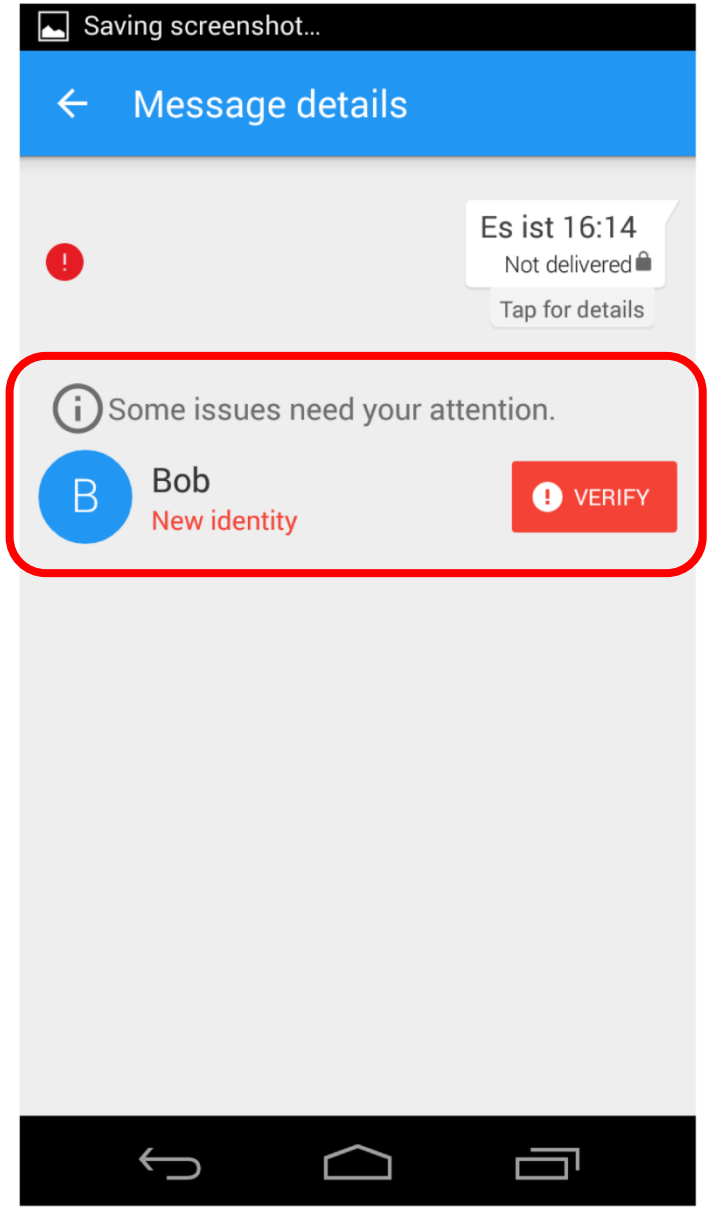
# Usability Study | Participants

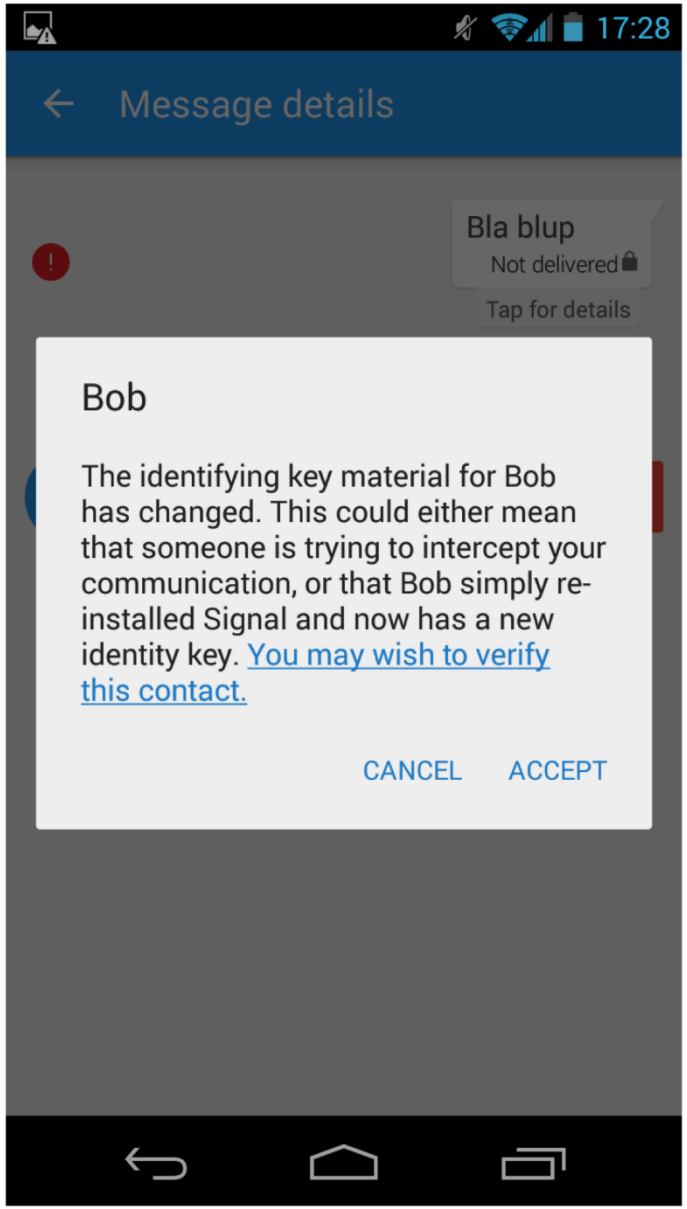


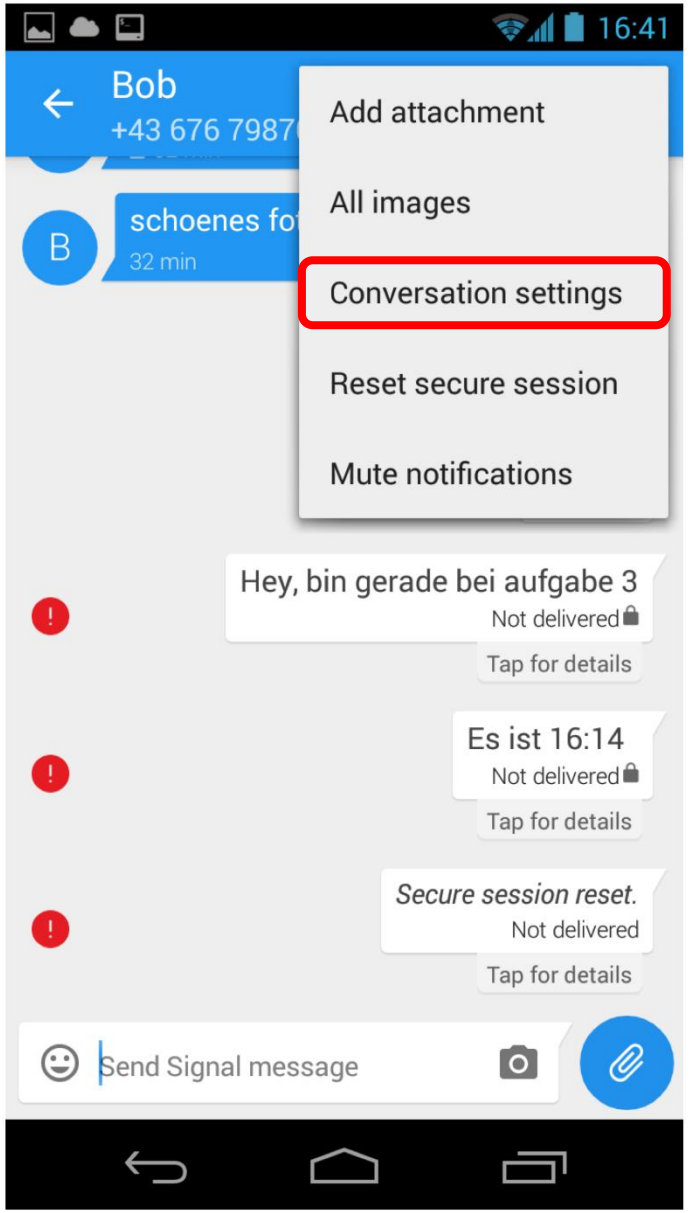
# Usability Study | Participants

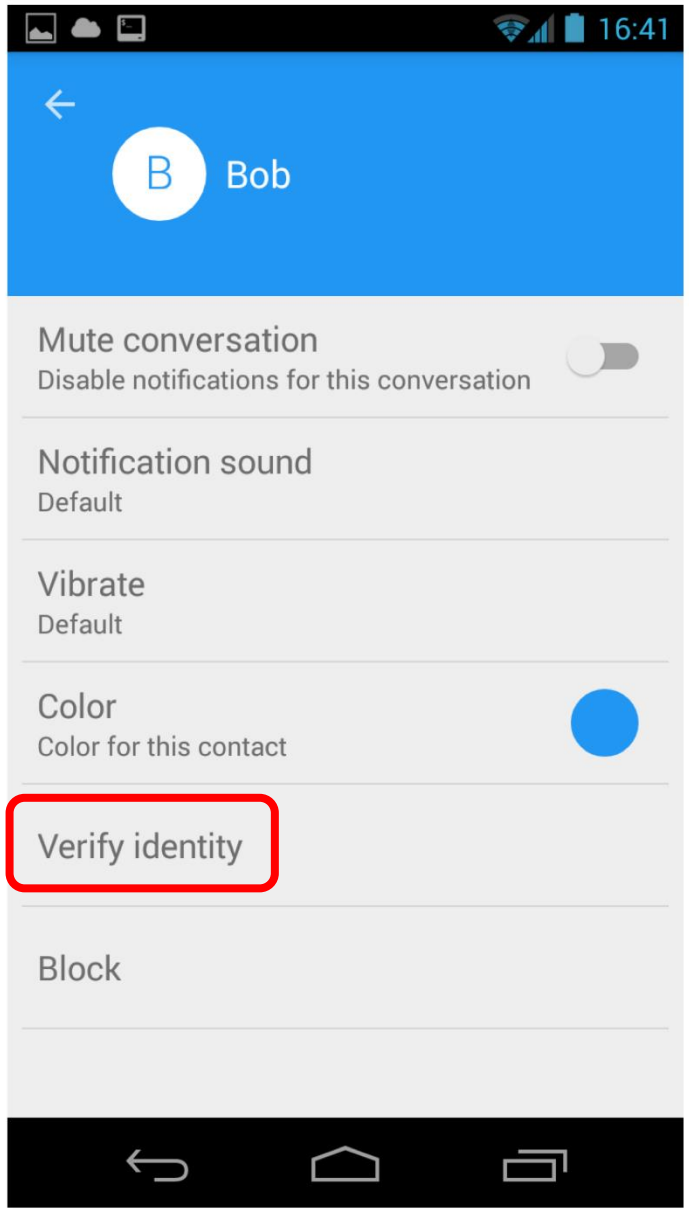
- Age
  - 18 – 35 years
- Knowledge about privacy and security
  - 7 no knowledge
  - 17 some knowledge
  - 4 a lot of knowledge
  - No experts
- Background
  - Most of them used WhatsApp
  - One used Signal

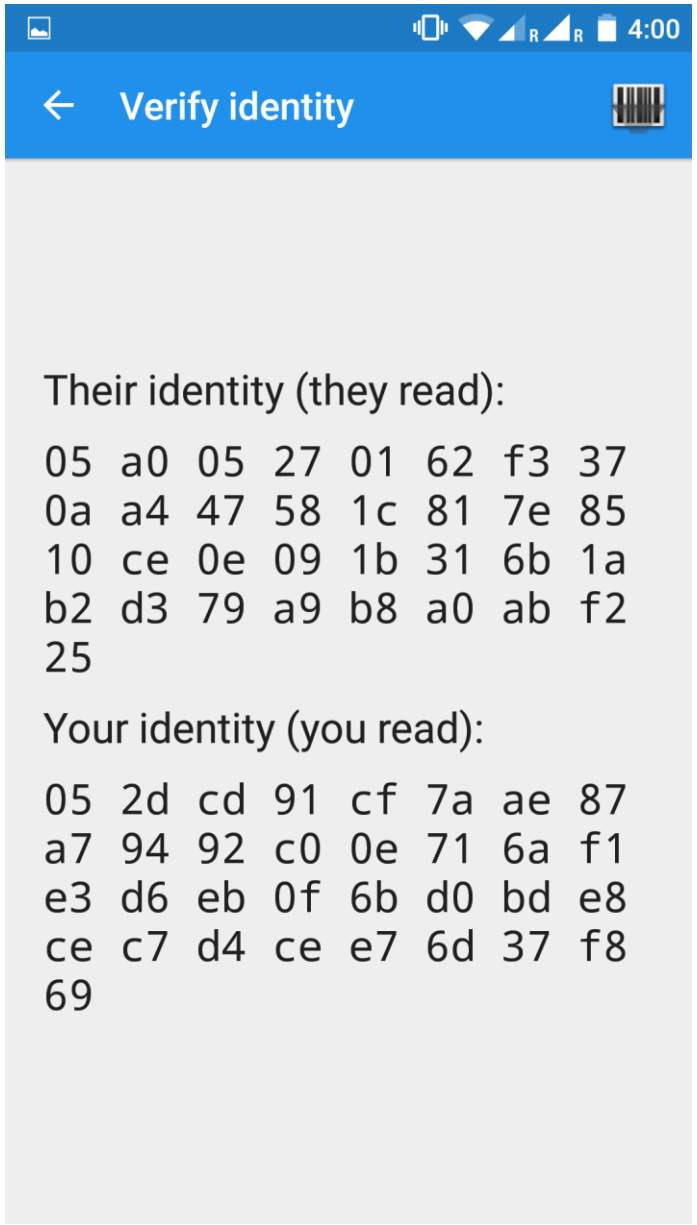

16:40
Bob
+43 676 7987033
B
schoenes foto
31 min
Danke
31 min
Danke
31 min
Hey, bin gerade bei aufgabe 3
Not delivered
Tap for details
Es ist 16:14
Not delivered
Tap for details
Secure session reset.
Not delivered
Tap for details
Send Signal message

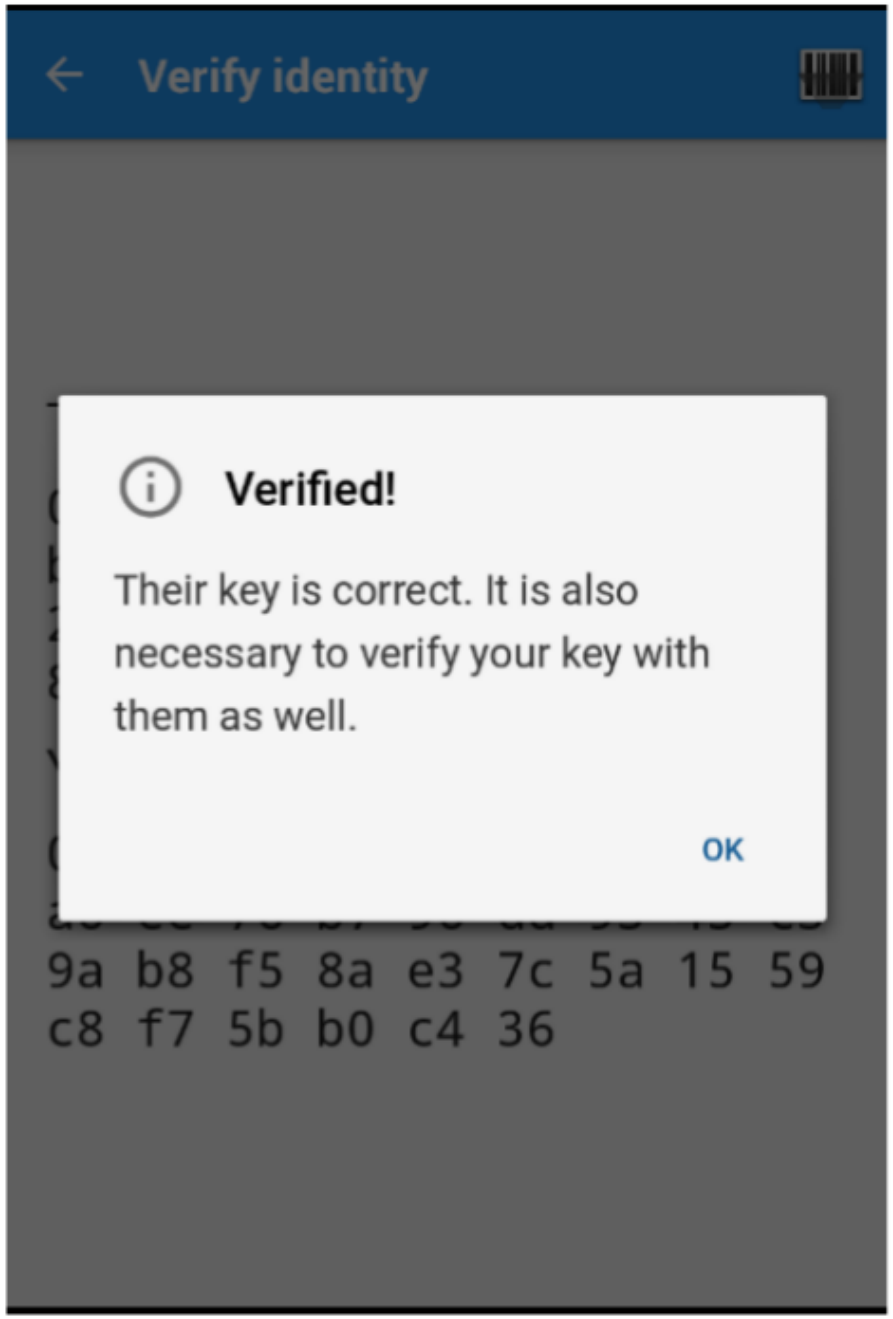

Saving screenshot...
Message details
Es ist 16:14
Not delivered
Tap for details
Some issues need your attention.
B
Bob
New identity
VERIFY

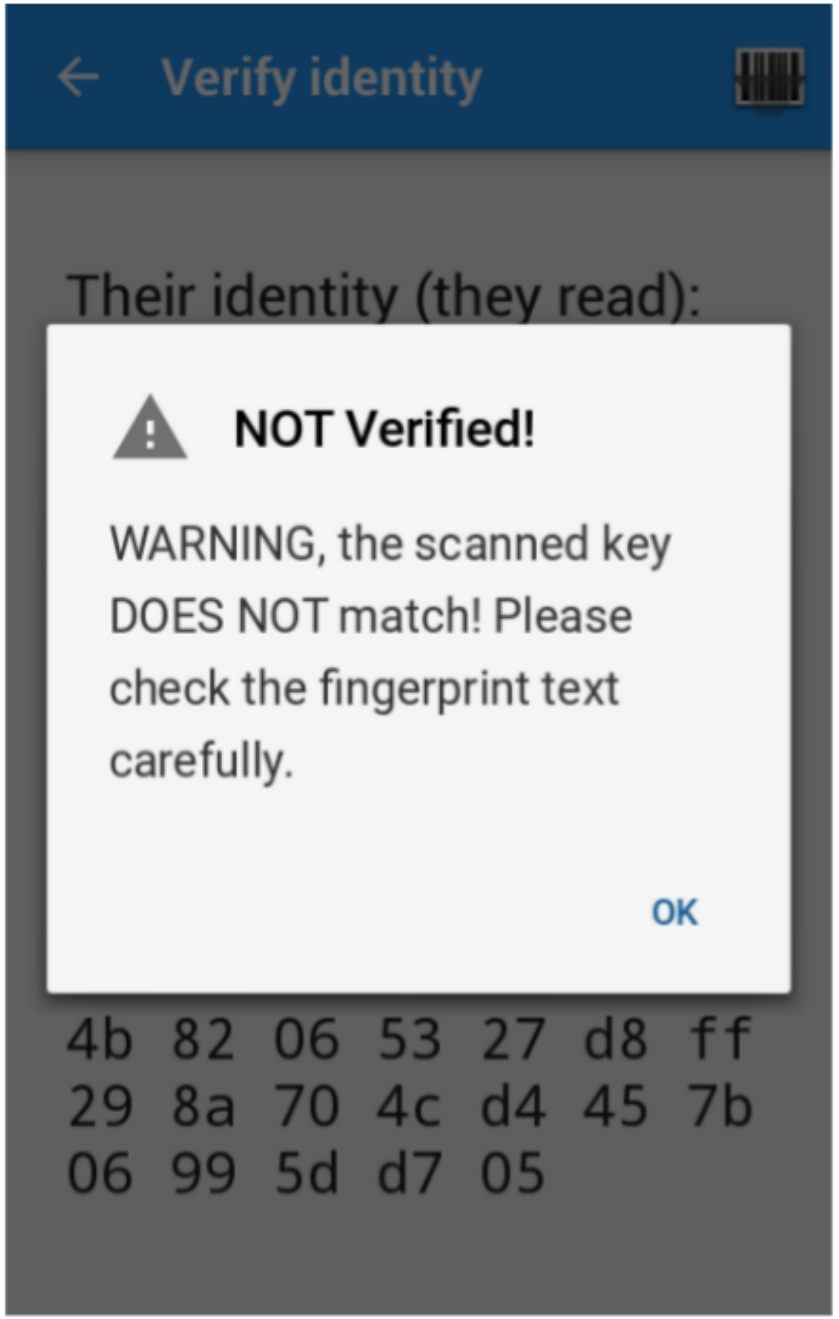

17:28
Message details
Bla blup
Not delivered
Tap for details
Bob
The identifying key material for Bob has changed. This could either mean that someone is trying to intercept your communication, or that Bob simply re-installed Signal and now has a new identity key. You may wish to verify this contact.
CANCEL
ACCEPT


16:41
Bob
+43 676 7987
Add attachment
All images
Conversation settings
Reset secure session
Mute notifications
B
schoenes fo
32 min
Hey, bin gerade bei aufgabe 3
Not delivered
Tap for details
Es ist 16:14
Not delivered
Tap for details
Secure session reset.
Not delivered
Tap for details
Send Signal message

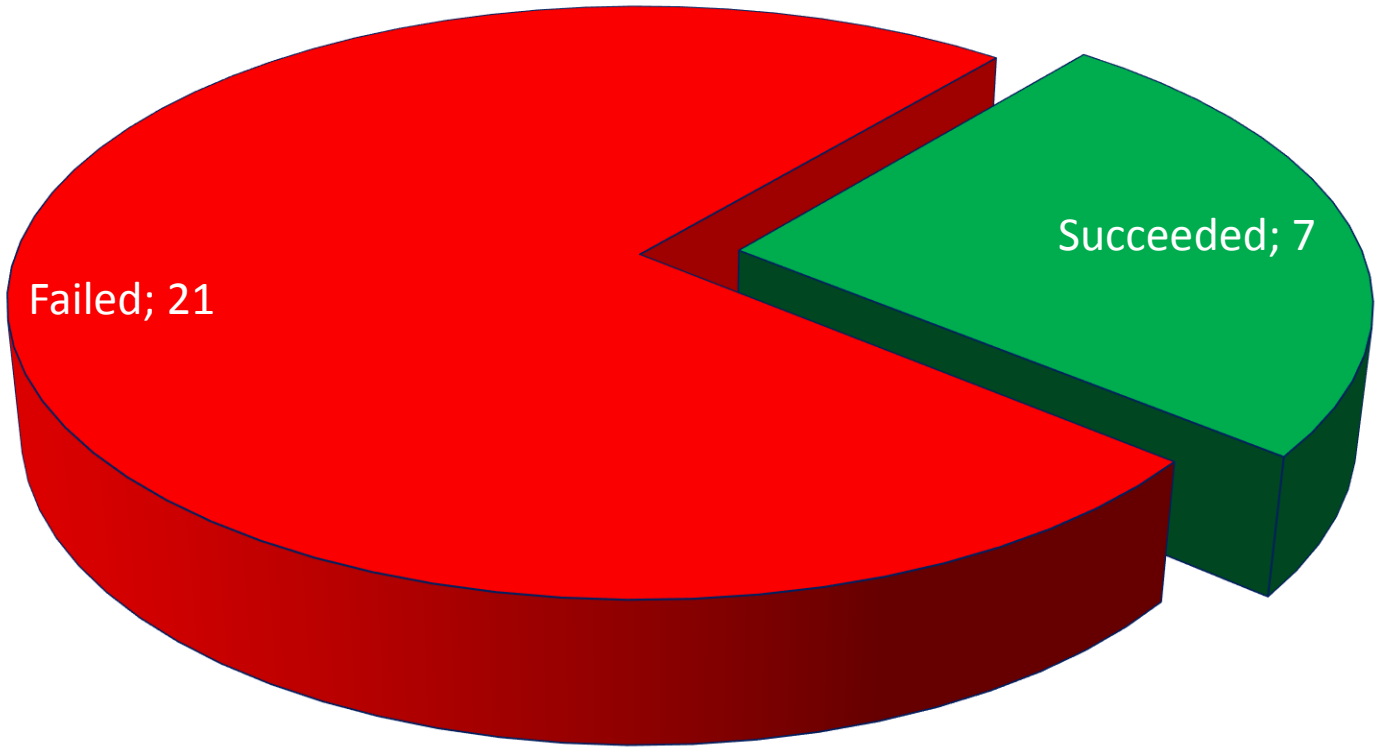

16:41
B
Bob
Mute conversation
Disable notifications for this conversation
Notification sound
Default
Vibrate
Default
Color
Color for this contact
Verify identity
Block


4:00
Verify identity
Their identity (they read):
05 a0 05 27 01 62 f3 37
0a a4 47 58 1c 81 7e 85
10 ce 0e 09 1b 31 6b 1a
b2 d3 79 a9 b8 a0 ab f2
25
Your identity (you read):
05 2d cd 91 cf 7a ae 87
a7 94 92 c0 0e 71 6a f1
e3 d6 eb 0f 6b d0 bd e8
ce c7 d4 ce e7 6d 37 f8
69


Verify identity
Verified!
Their key is correct. It is also necessary to verify your key with them as well.
OK
9a b8 f5 8a e3 7c 5a 15 59
c8 f7 5b b0 c4 36

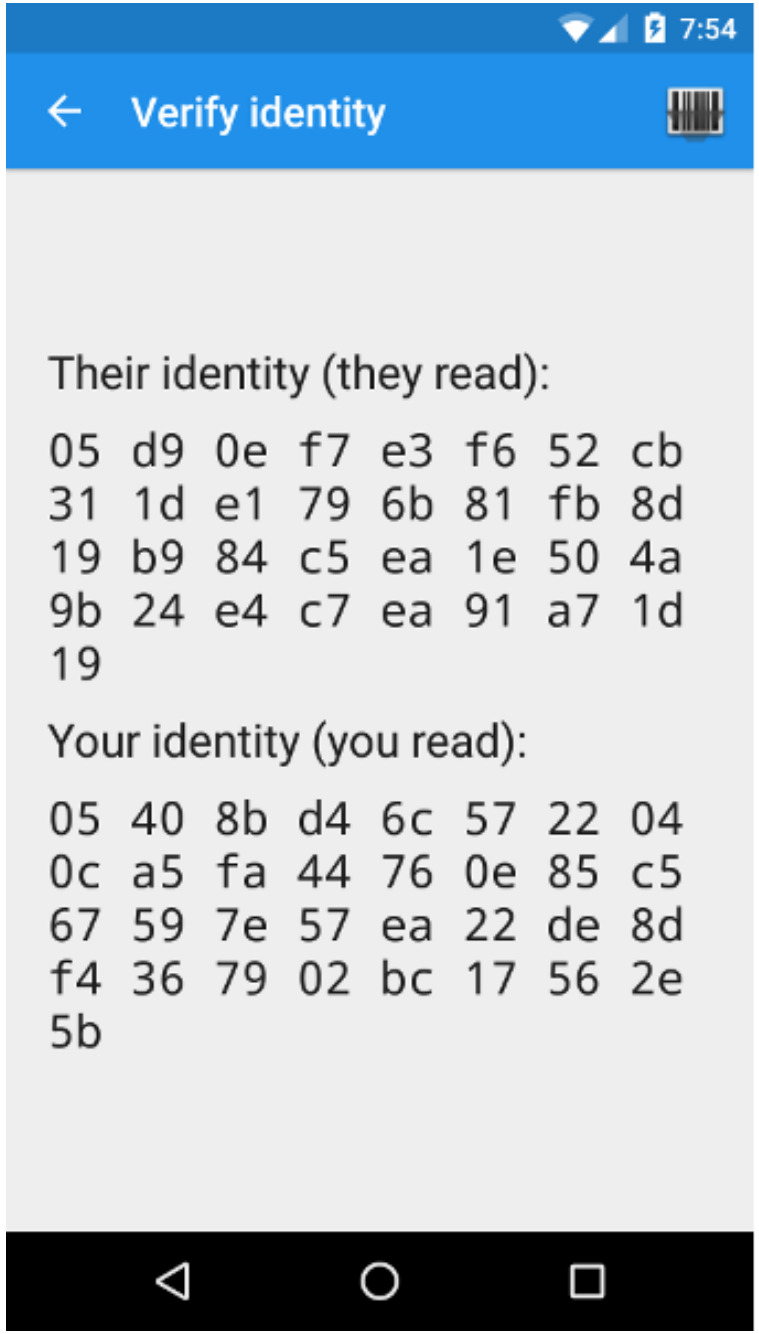

Verify identity
Their identity (they read):
NOT Verified!
WARNING, the scanned key DOES NOT match! Please check the fingerprint text carefully.
OK
4b 82 06 53 27 d8 ff
29 8a 70 4c d4 45 7b
06 99 5d d7 05

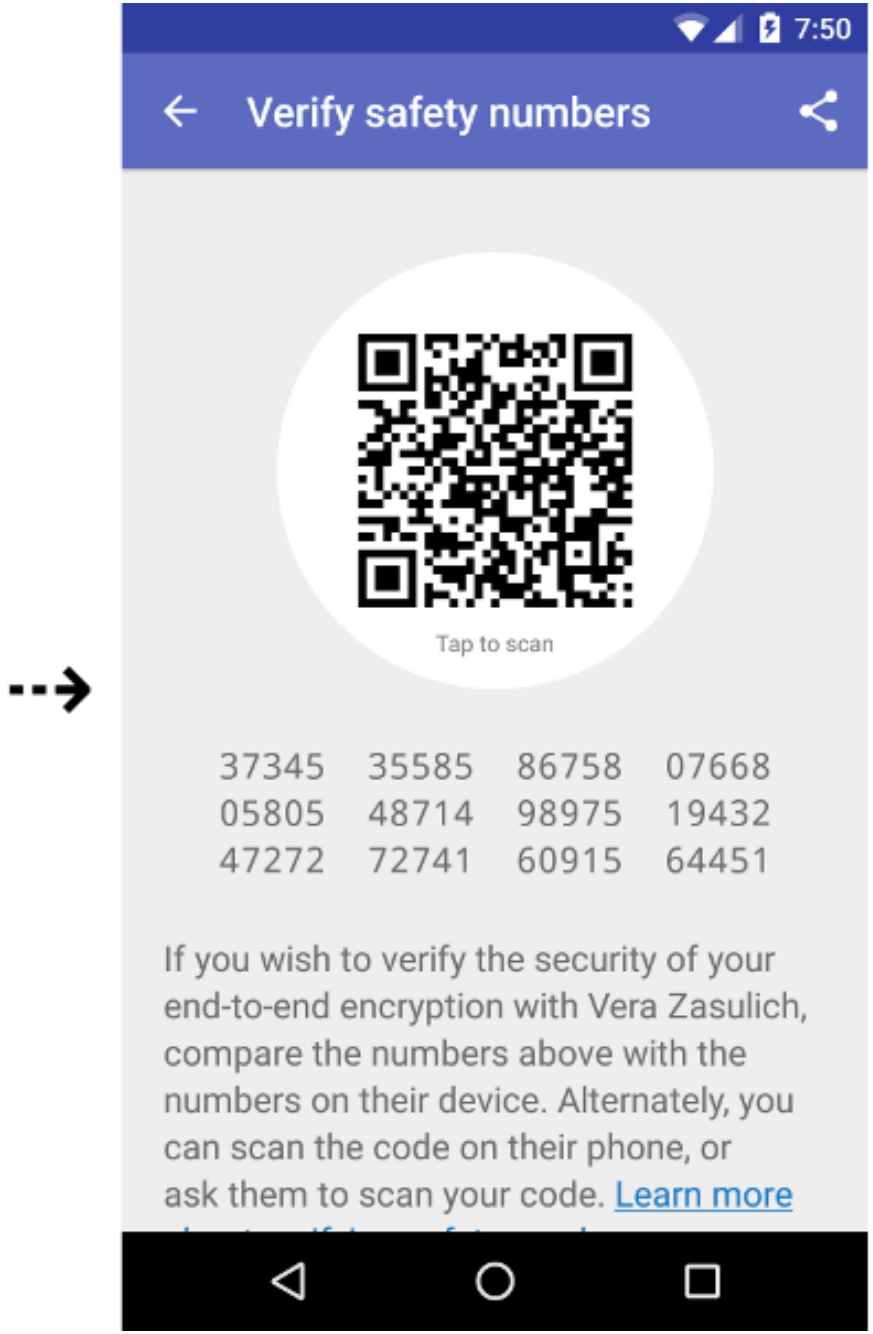
# Usability Study | Results



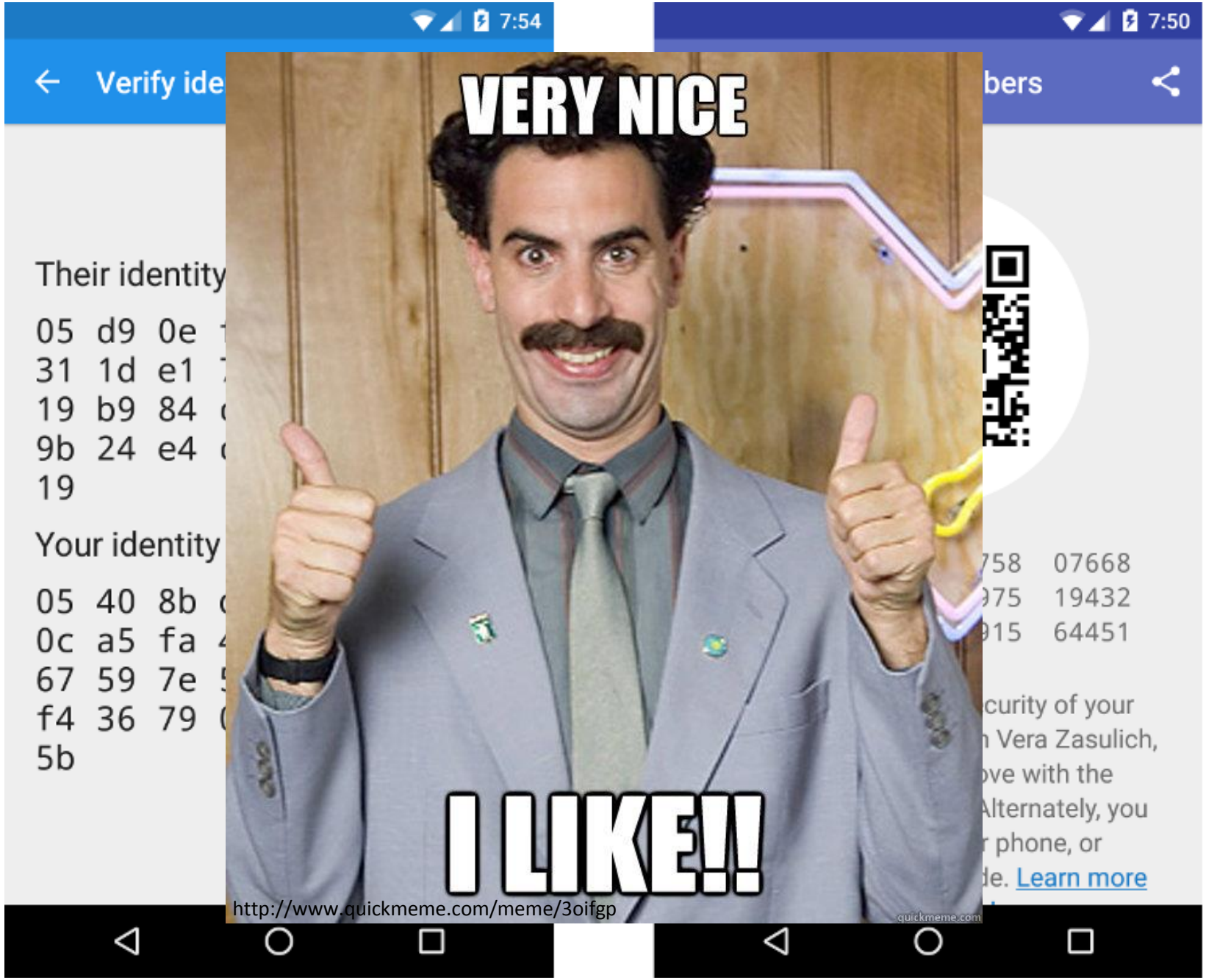
# Signal Usability | Recommendations

- “Verfiy“ Button should be renamed
- Redesign verification page
- More informative “Help” pages
- Verification status



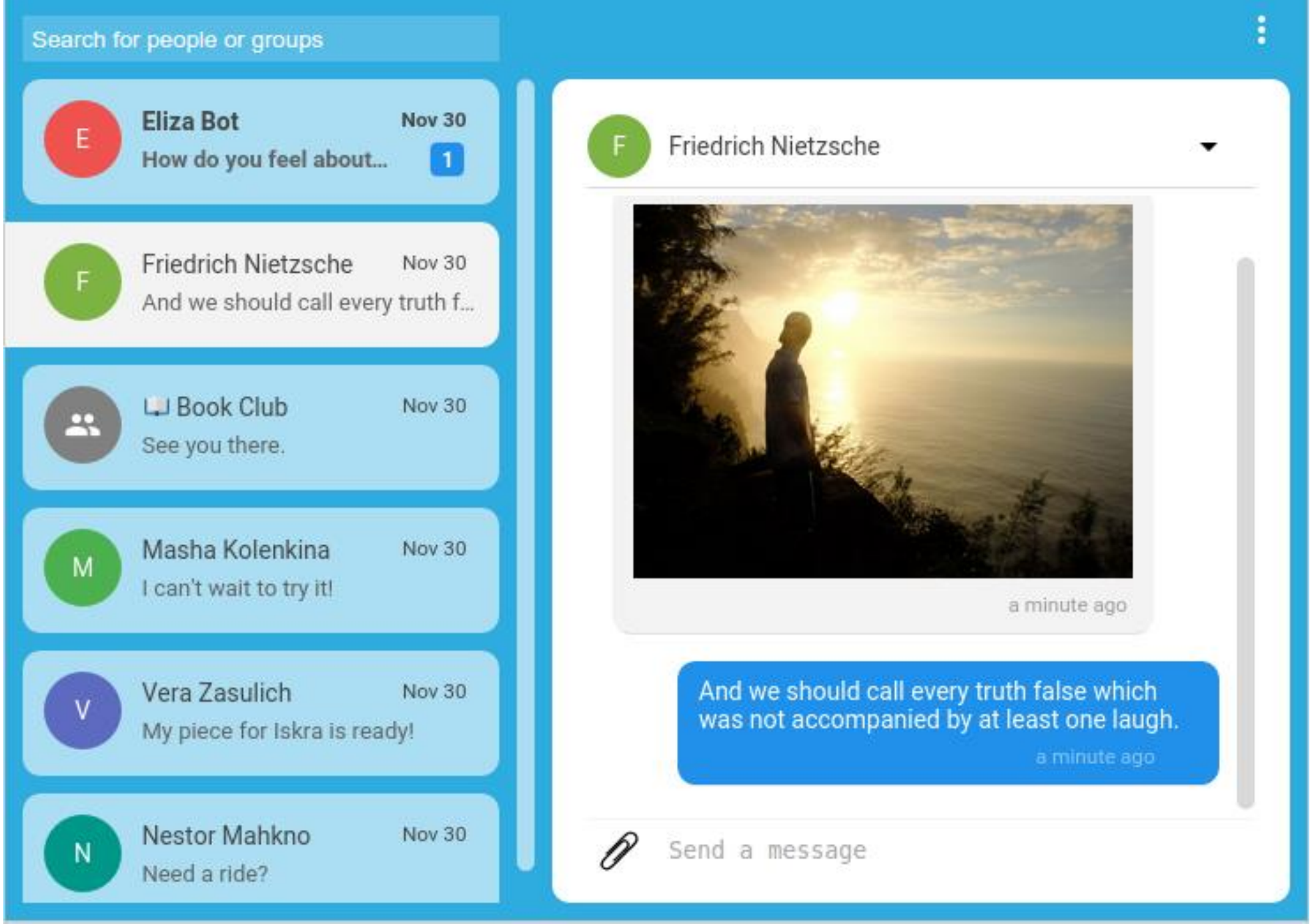

https://whispersystems.org/blog/safety-number-updates/




https://whispersystems.org/blog/safety-number-updates/

# Desktop Messengers

# Signal Desktop

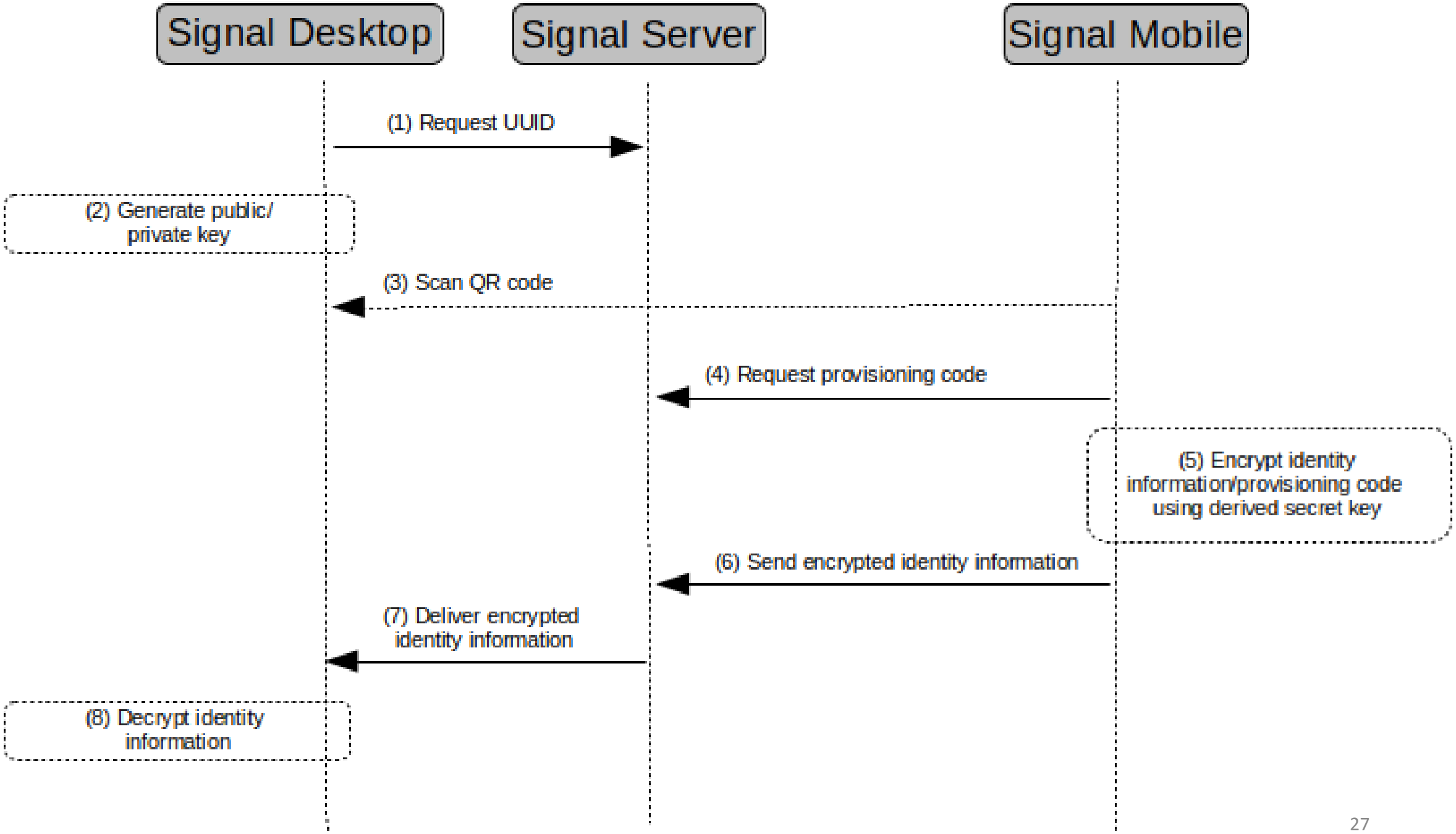


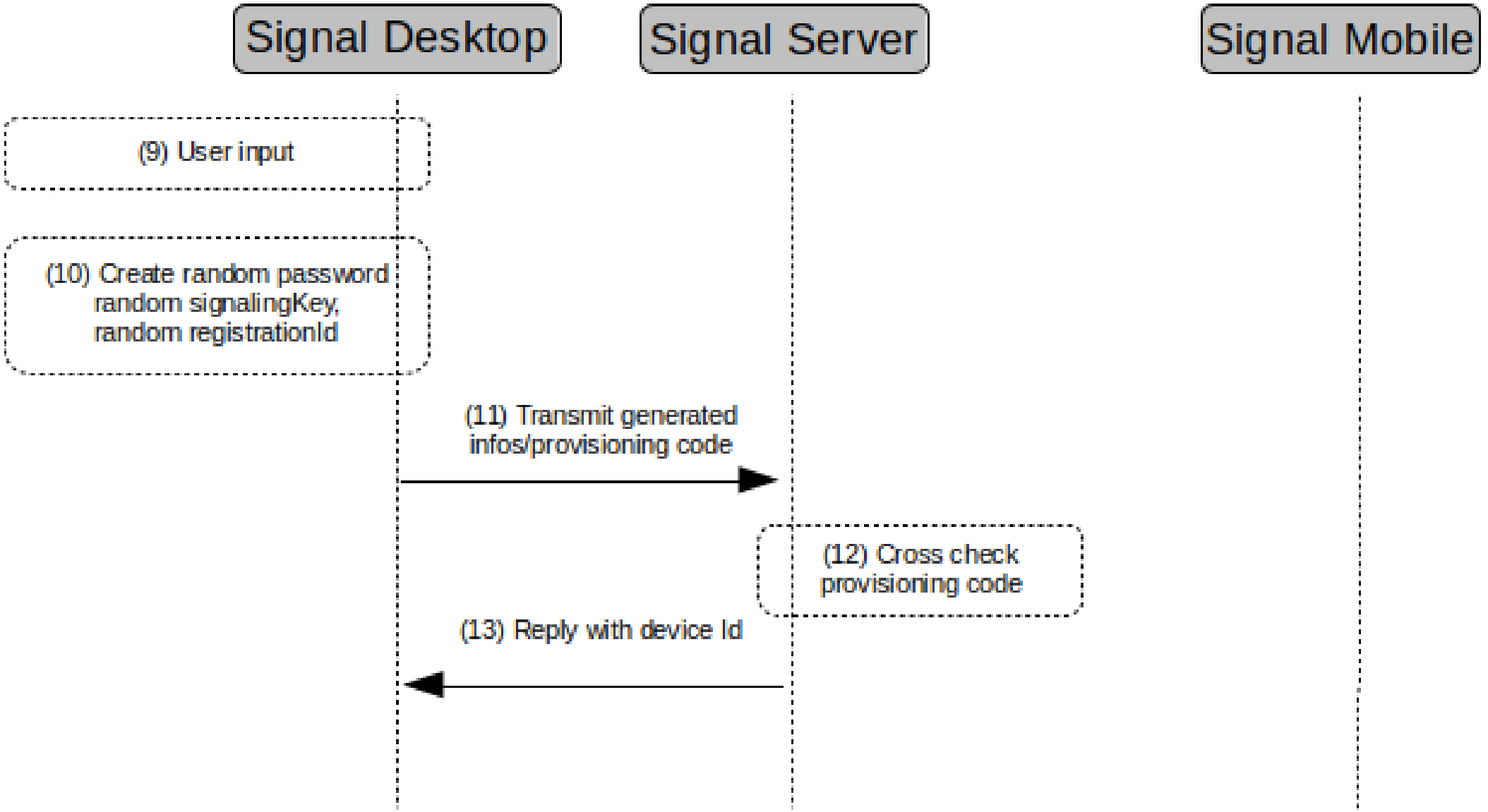

https://whispersystems.org/blog/images/signal-desktop-screenshot.png

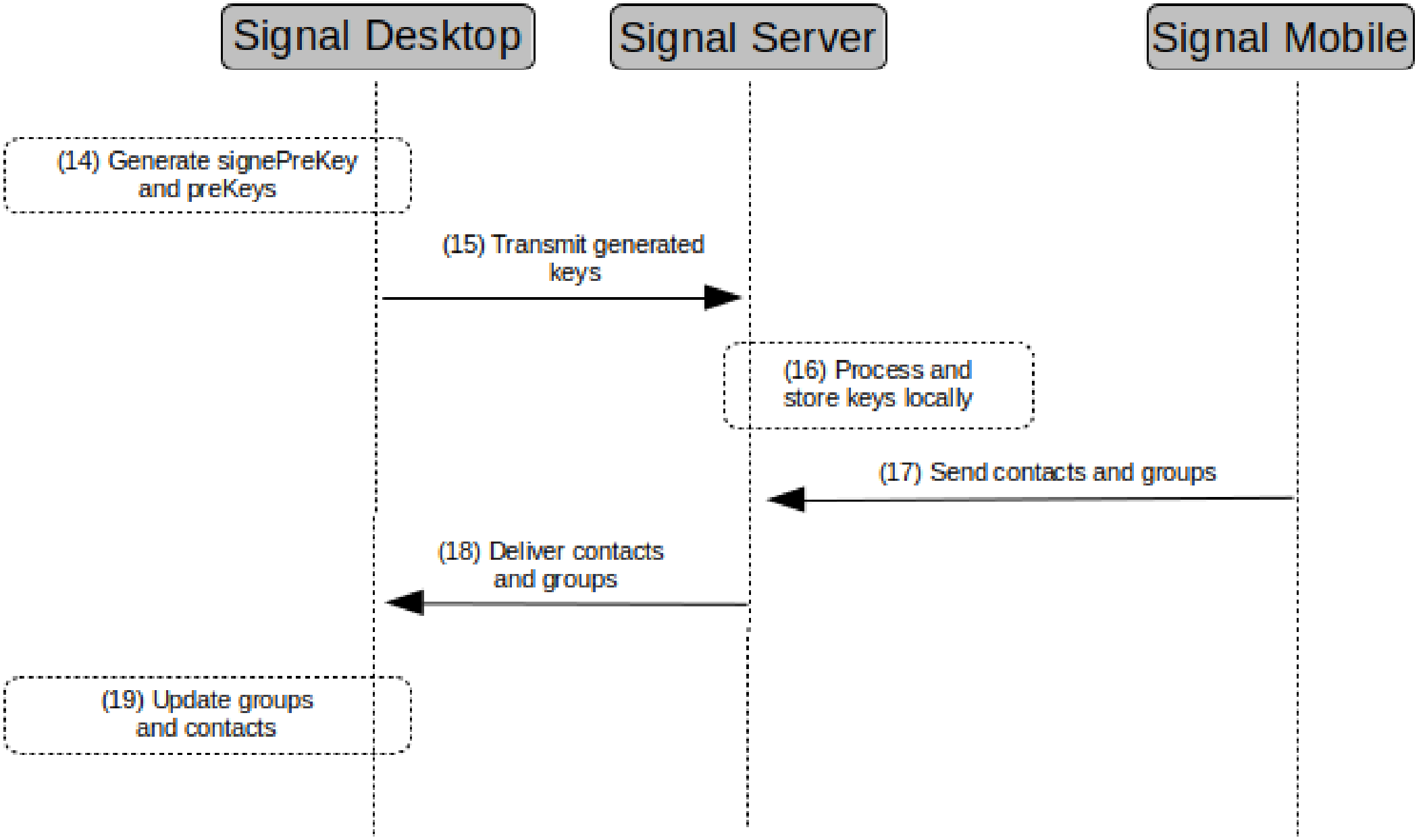
# Signal Desktop | Characteristics

- Standalone
- Chrome extension
- Uses QR code to exchange necessary information which is needed for calculating secrets
- Open Source

# Signal Desktop | Device Linking


Signal Desktop
Signal Server
Signal Mobile
(1) Request UUID
(2) Generate public/ private key
(3) Scan QR code
(4) Request provisioning code
(5) Encrypt identity information/provisioning code using derived secret key
(6) Send encrypted identity information
(7) Deliver encrypted identity information
(8) Decrypt identity information


Signal Desktop
Signal Server
Signal Mobile
(9) User input
(10) Create random password
random signalingKey,
random registrationId
(11) Transmit generated
infos/provisioning code
(12) Cross check
provisioning code
(13) Reply with device Id


Signal Desktop
Signal Server
Signal Mobile
(14) Generate signePreKey and preKeys
(15) Transmit generated keys
(16) Process and store keys locally
(17) Send contacts and groups
(18) Deliver contacts and groups
(19) Update groups and contacts

# Signal Desktop | Synching

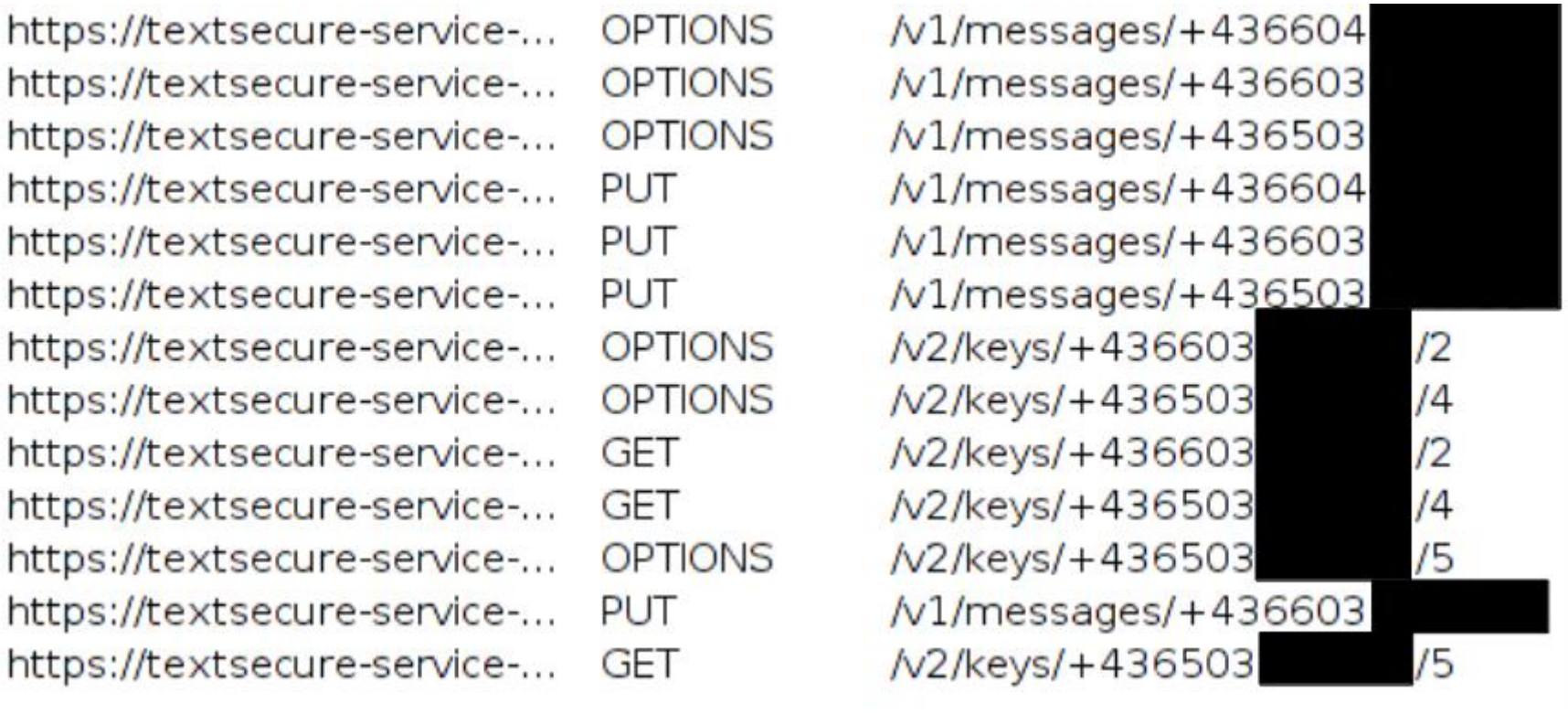
- After linking, Signal syncs contacts and group-memberships to Signal Desktop
- Done via a normal Signal message → Recipient is the **device_id**

# Signal Desktop | Synching

- After linking, Signa nberships to Signal Desktop
- Done via a normal he **device_id**

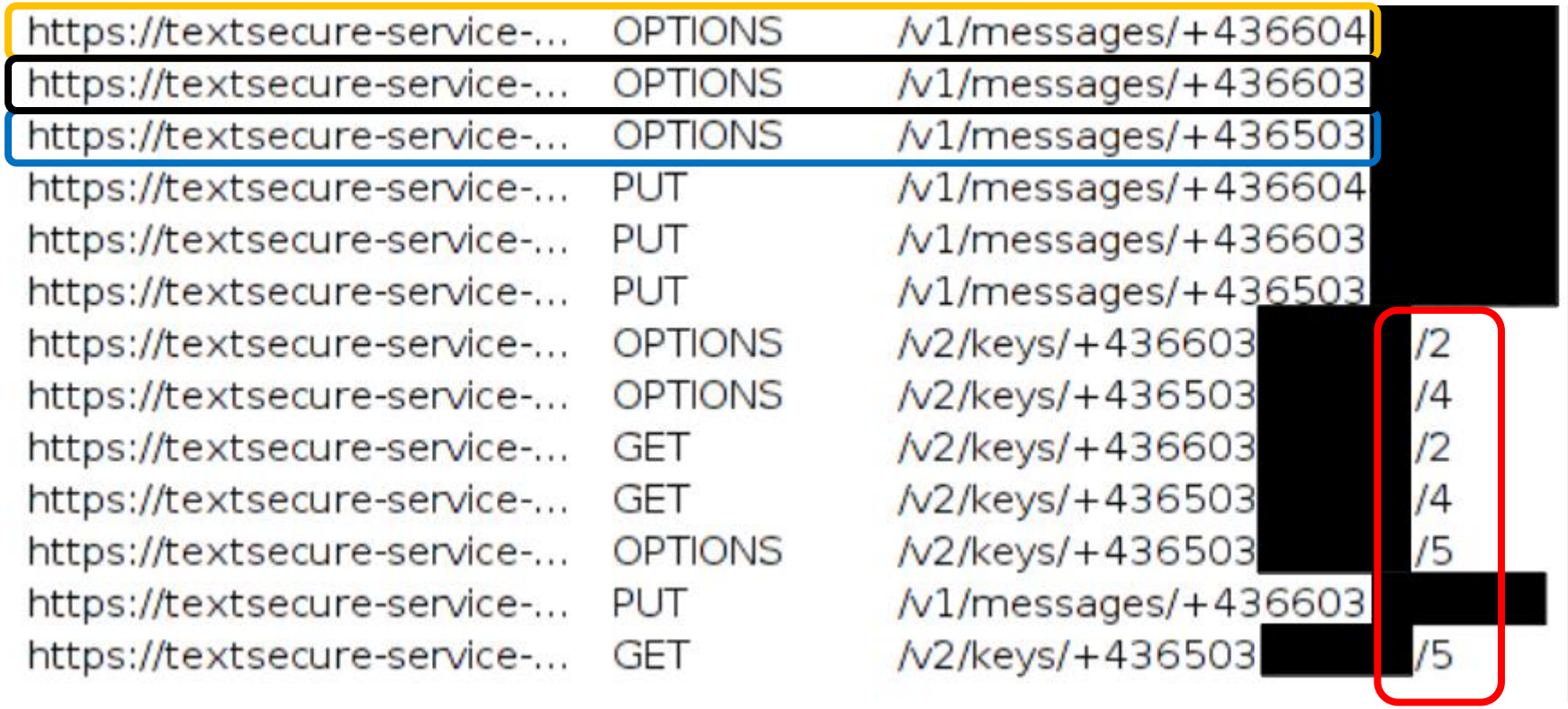
# Signal Desktop | Info Leak

- Known problem – Hard to mitigate
- Signal Desktop leaks phone numbers + device_ids

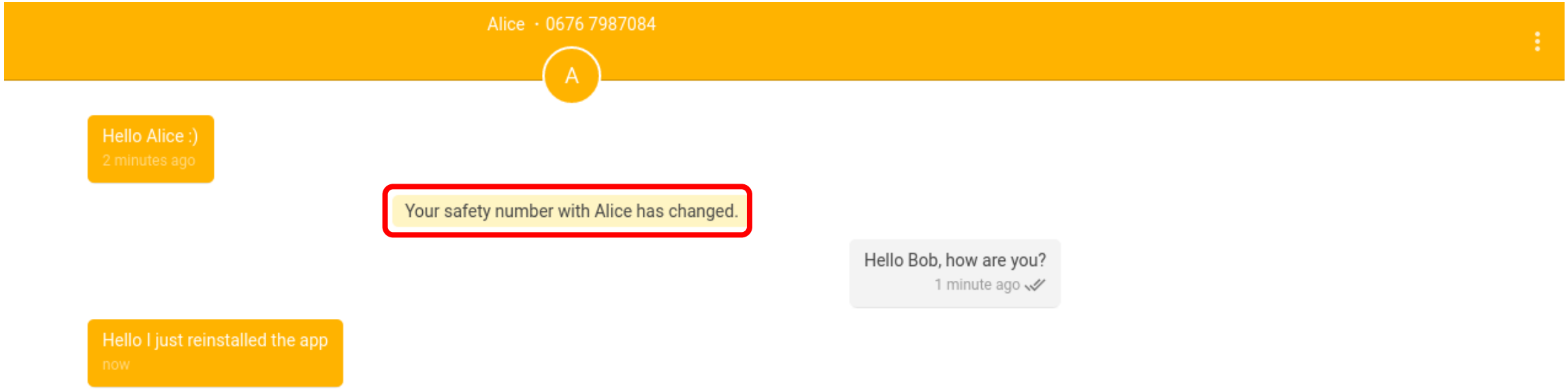


# Signal Desktop | Info Leak

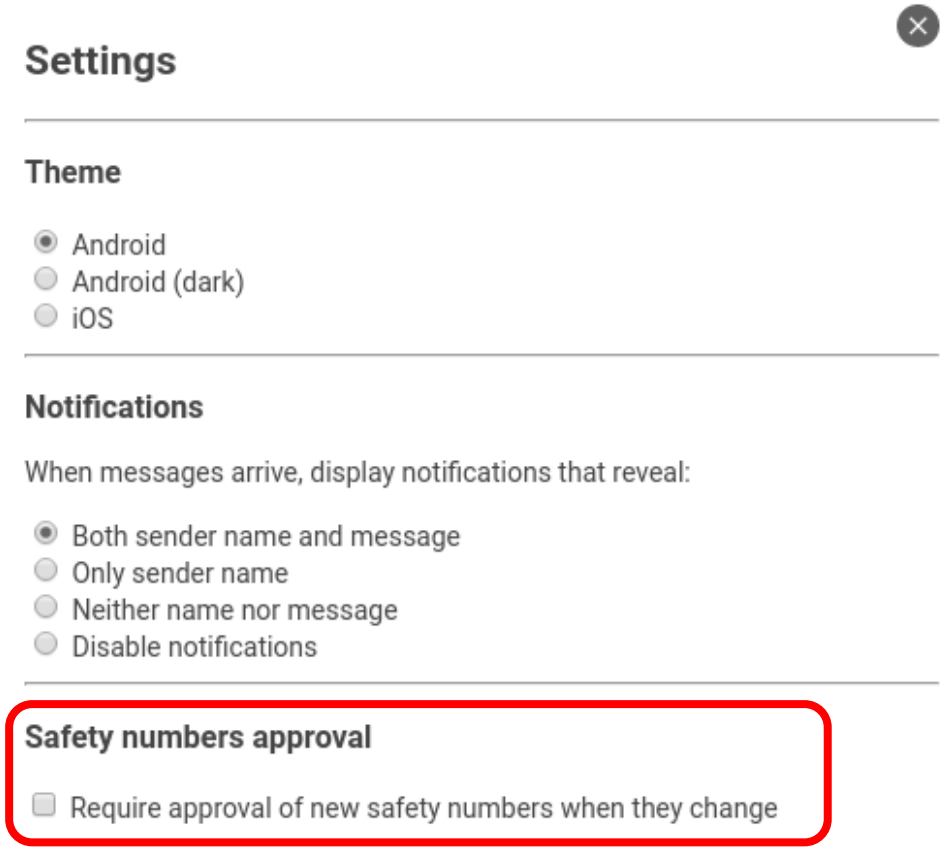
- Known problem – Hard to mitigate
- Signal Desktop leaks phone numbers + device_ids



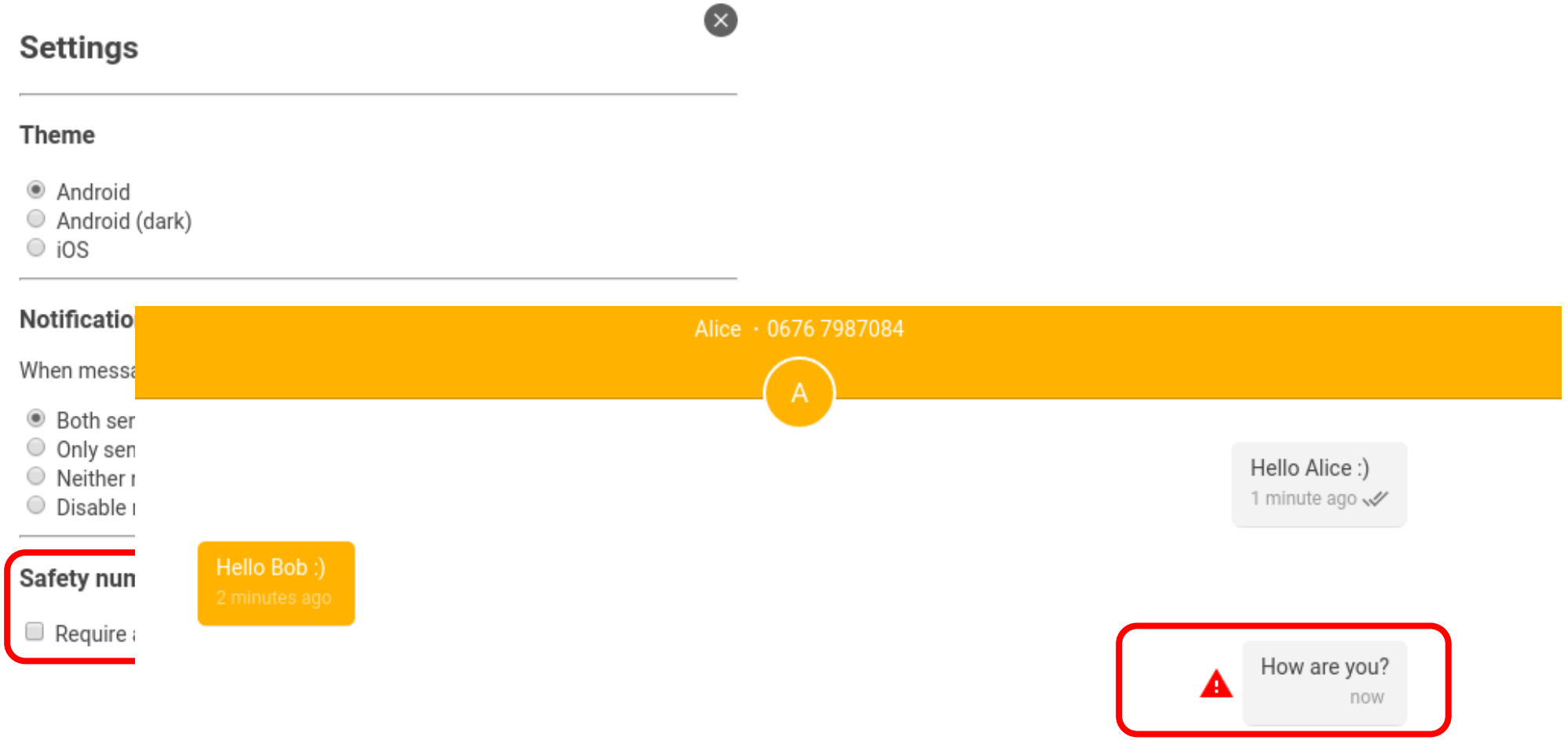
# Signal Desktop | MitM



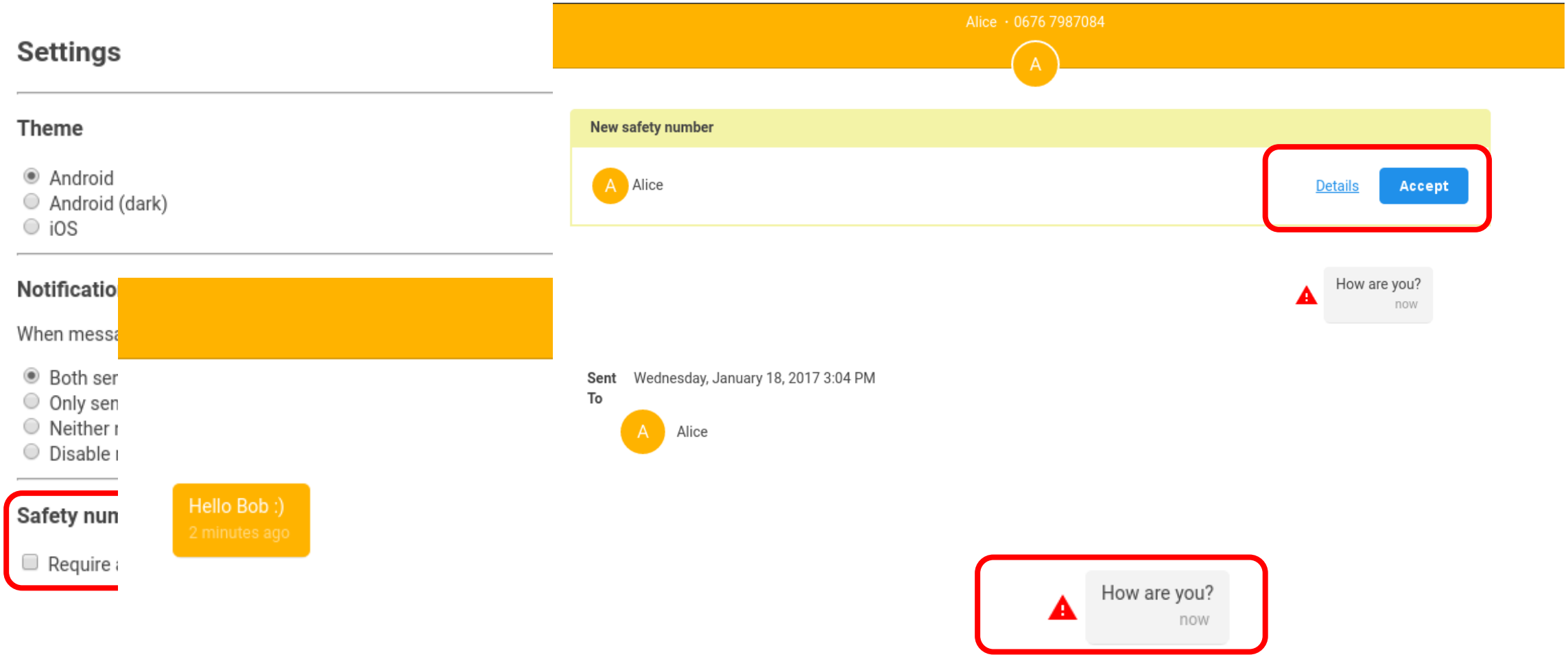
# Signal Desktop | MitM



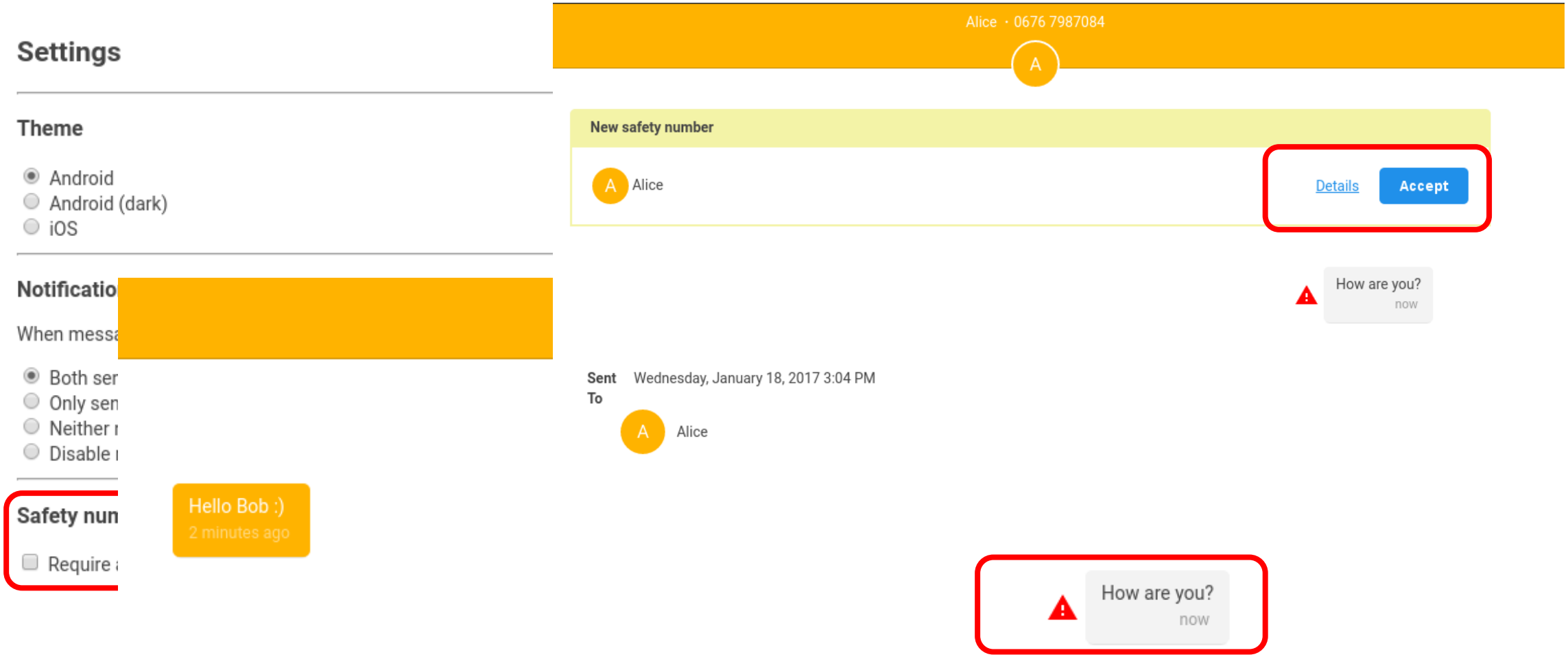
# Signal Desktop | MitM



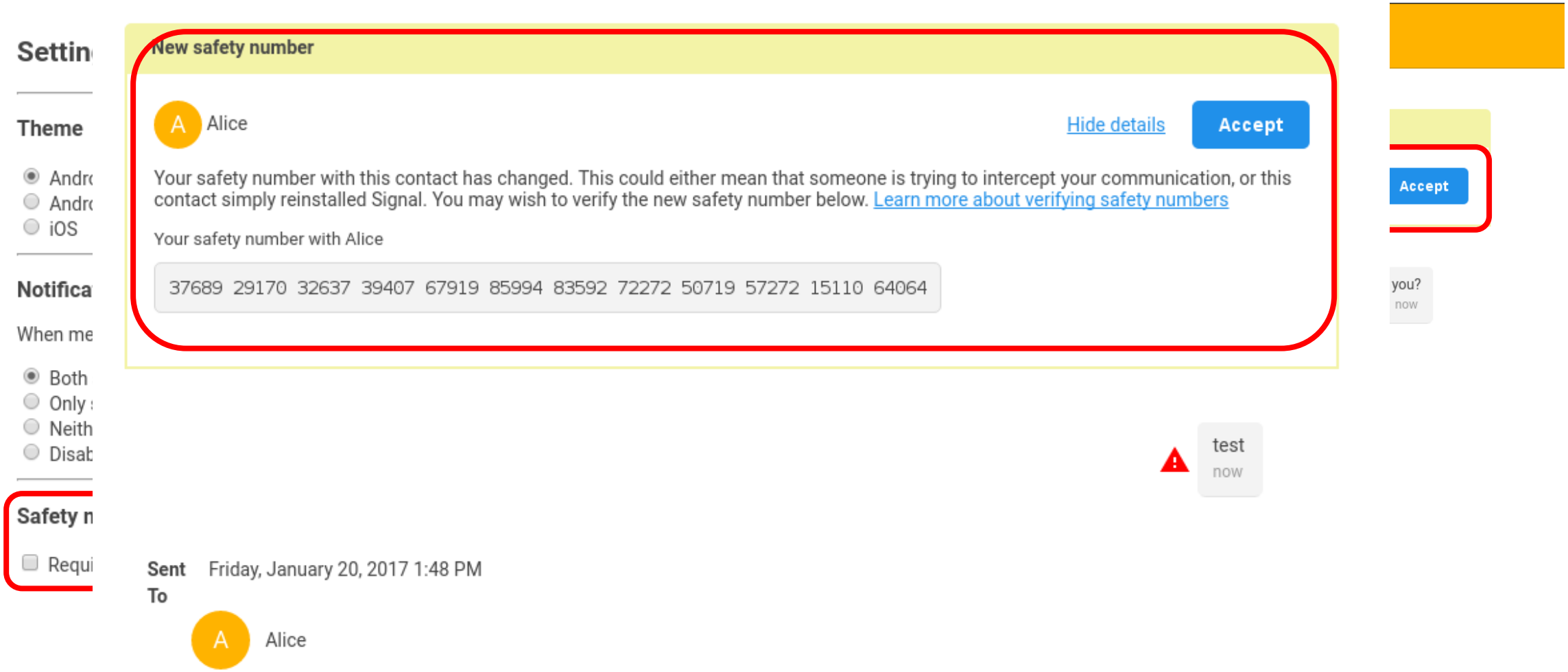
# Signal Desktop | MitM



# Signal Desktop | MitM

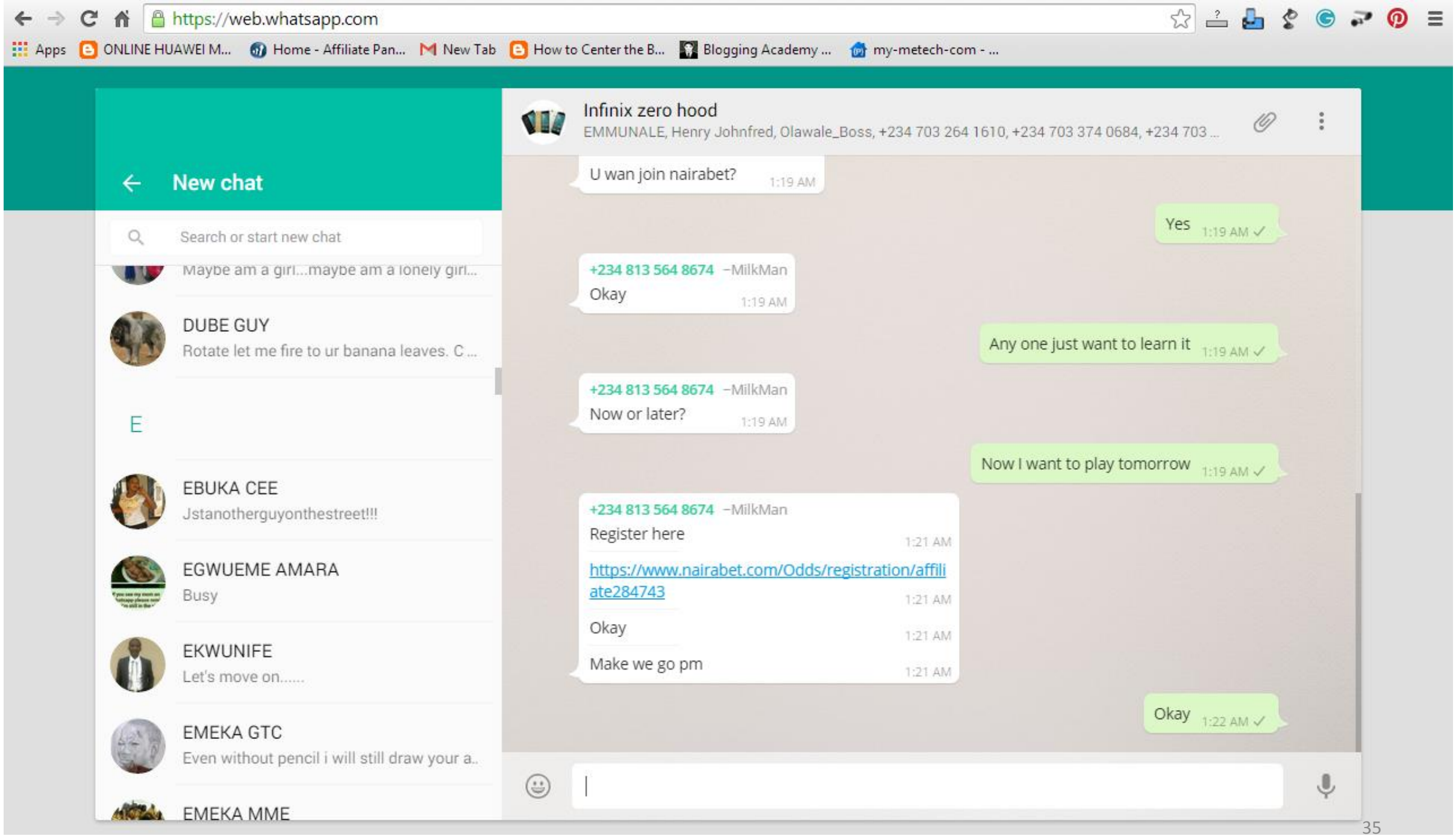


# Signal Desktop | MitM



# Signal Desktop

# WhatsApp Web



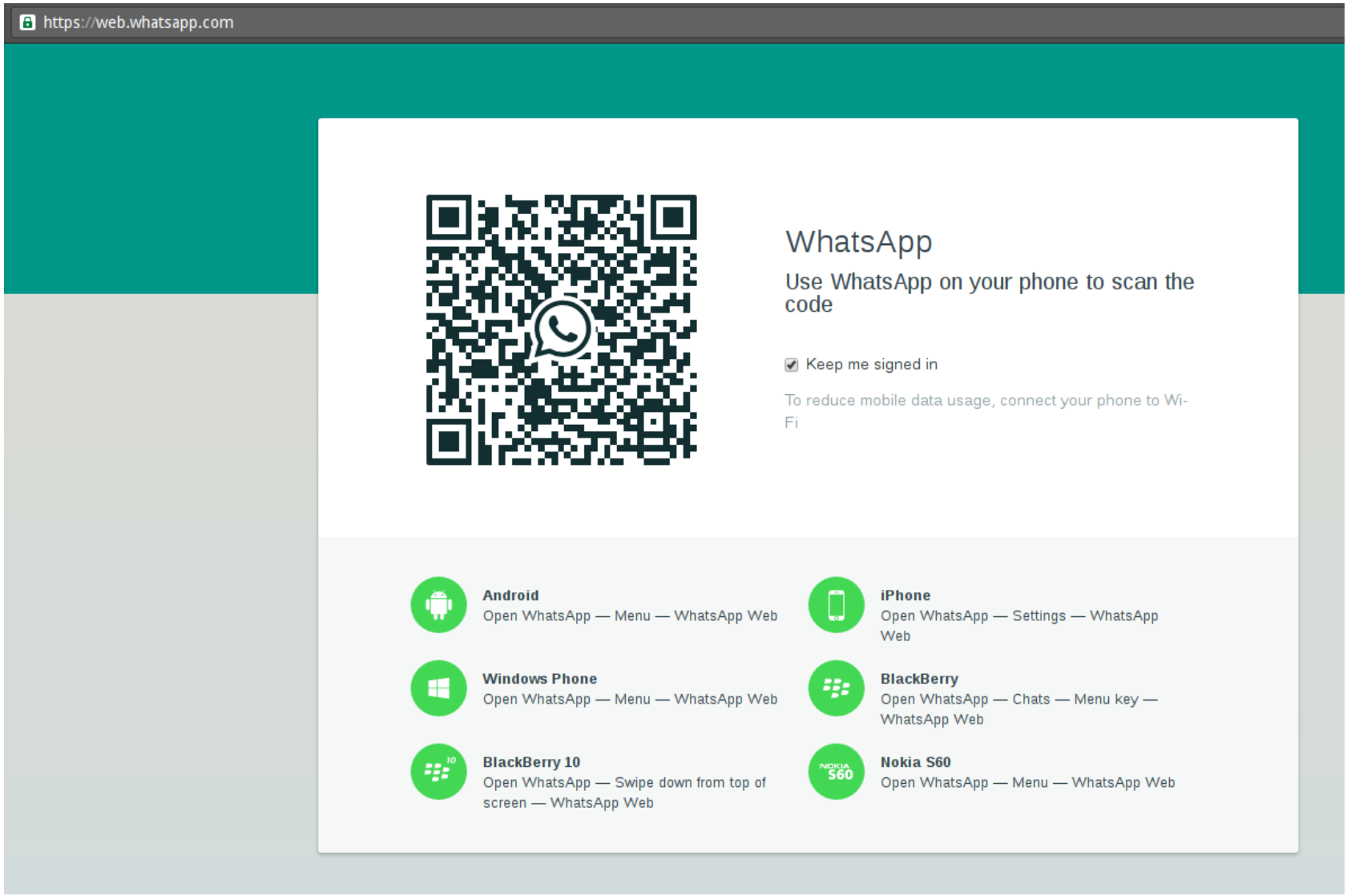


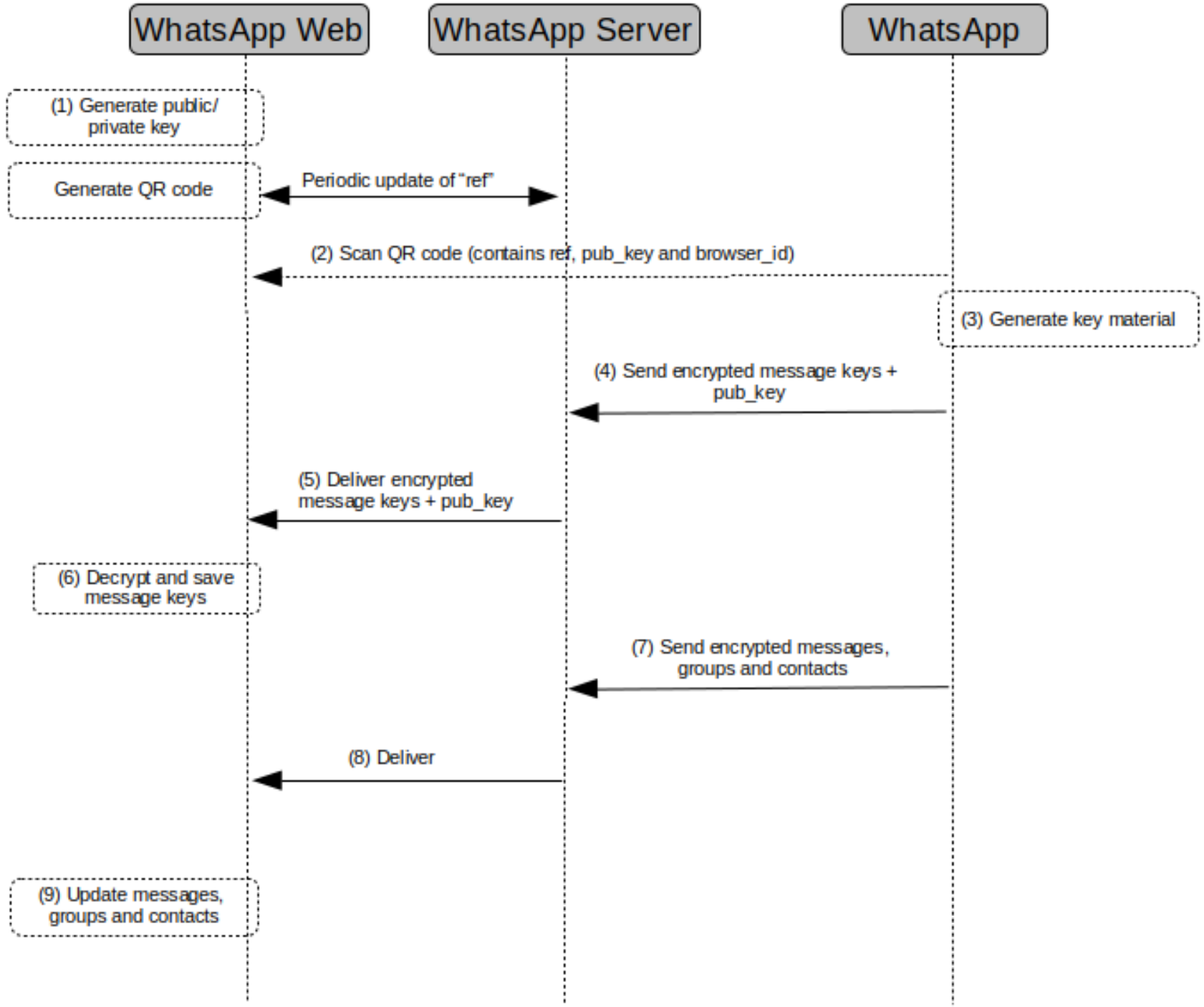

https://4.bp.blogspot.com/-vqobDIixh6s/VMRIo_jC-YI/AAAAAAAABHM/XfTbK8FIn5w/s1600/Screenshot%2B(28).png

# WhatsApp Web | Characteristics

- Mobile dependent
- Web application
- Uses QR code to exchange necessary information which is needed for calculating secrets
- Closed Source
- Privacy concerns

# WhatsApp Web | Device Linking




WhatsApp Web
WhatsApp Server
WhatsApp
(1) Generate public/ private key
Generate QR code
Periodic update of "ref"
(2) Scan QR code (contains ref, pub_key and browser_id)
(3) Generate key material
(4) Send encrypted message keys + pub_key
(5) Deliver encrypted message keys + pub_key
(6) Decrypt and save message keys
(7) Send encrypted messages, groups and contacts
(8) Deliver
(9) Update messages, groups and contacts

# WhatsApp Web | Synchronisation & encryption

- WhatsApp mobile uploads chats to WhatsApp Web
  - Images are stored encrypted on WhatsApp server – decrypted locally within the web application

# WhatsApp Web | Synchronisation & encryption

- WhatsApp mobile uploads chats to WhatsApp Web
  - Images are stored encrypted on WhatsApp server – decrypted locally within the web application

| | | |
|---|---|---|
| 1484148051.--170,["admin","Conn","reref"] | 41 | 16:20:5… |
| 1484148051.--170,{"status":200,"ref":"1@pfjBPPyHLV83XkDejTlMxP7Fvsm+XiAqabzPDG/vNRaRXctaib/iGUyY","ttl":20000} | 110 | 16:20:5… |
| s1,["Conn",{"ref":"1@pfjBPPyHLV83XkDejTlMxP7Fvsm+XiAqabzPDG/vNRaRXctaib/iGUyY","wid":"436767987084@c.us","connected":true,"is… | 1228 | 16:20:5… |
| s2,["Stream","update",false,"0.2.2730"] | 39 | 16:20:5… |
| s3,["Props",{"bucket":"b","gifSearch":"giphy","SPAM":true,"SET_BLOCK":true,"MESSAGE_INFO":true,"media":64,"maxSubject":25,"maxParticip… | 206 | 16:20:5… |
| Binary Frame (Opcode 2) | 136 | 16:20:5… |
| Binary Frame (Opcode 2) | 2272 | 16:20:5… |
| Binary Frame (Opcode 2) | 5712 | 16:20:5… |
| Binary Frame (Opcode 2) | 488 | 16:20:5… |
| Binary Frame (Opcode 2, mask) | 75 | 16:20:5… |
| Binary Frame (Opcode 2, mask) | 75 | 16:20:5… |

# WhatsApp Web | Synchronisation & encryption

- For encryption between WhatsApp Web and WhatsApp mobile, a symmetric key is used

# WhatsApp Web | Synchronisation & encryption

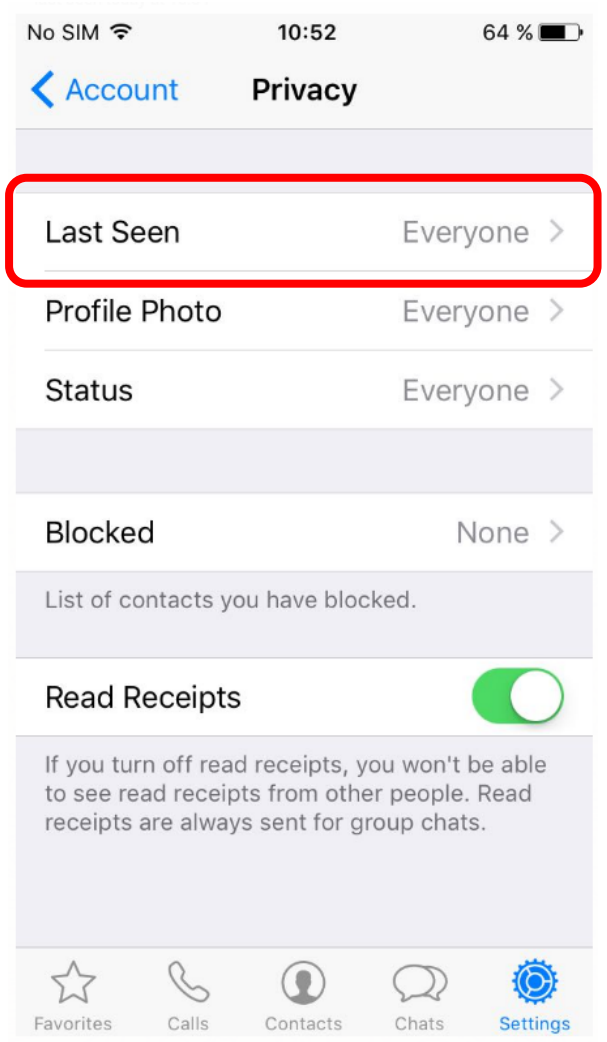
- For encryption between WhatsApp Web and WhatsApp mobile, a symmetric key is used

| Key | Value |
|---|---|
| +CAd4xh20auNT5DOX9hqIg== | [{"id":"uM7Jk0OboVsrscR+l1aqgg=="}] |
| /NPzuwAjediyAQdJEV2OVQ== | false |
| 0MHj6jtKAT3eh8tyMklEJA== | false |
| 2/WKoyBWLT5kHHX095H6aQ== | [{"id":"global_mute","expiration":0}] |
| WABrowserId | "tHARqzk8QOFqAyXVtJ7Tjg==" |
| WASecretBundle | {"encKey":"CtivaoyUf1Kmms5bSe16Eisy7pOo+FRt1rbZwFJnPO8=","macKey":"9NFv92BZhBsR/Nbcu7NZ6Hsf/pNoxhSC0DB… |
| WAToken1 | "6WPSDXywG1HLcerONiV7zVzJ14ETrYN1tQumhjEXEco=" |
| WAToken2 | "1@YGHUxUnzTQjhpCZd08hp5BXz7czAFA2yWgE6pVdql1LrhJXSRh9Din6Npfiq1upqa853ICSPfIW1dw==" |
| debugCursor | 478 |
| i3t7+MdlIkCYTWMBBi6iPA== | [{"id":"defaultPreference","wallpaperColor":"default_chat_wallpaper"}] |
| kt2B7iEPy76k8XB3W/1CtA== | false |
| logout-token | "1@B3bXu/2XY3tVZGw36wAZ2LauwrtMxNPd5Xl51zycjbDU/olljFn7i6v97LSeibnsfpi4hFvSyPD3Lz2blyFeHiEUA6ao9Zt4TIX+I… |
| remember-me | true |
| storage_test | storage_test |
| ver | 1 |
| whatsapp-mutex | "x189703616:init_1487778912397" |

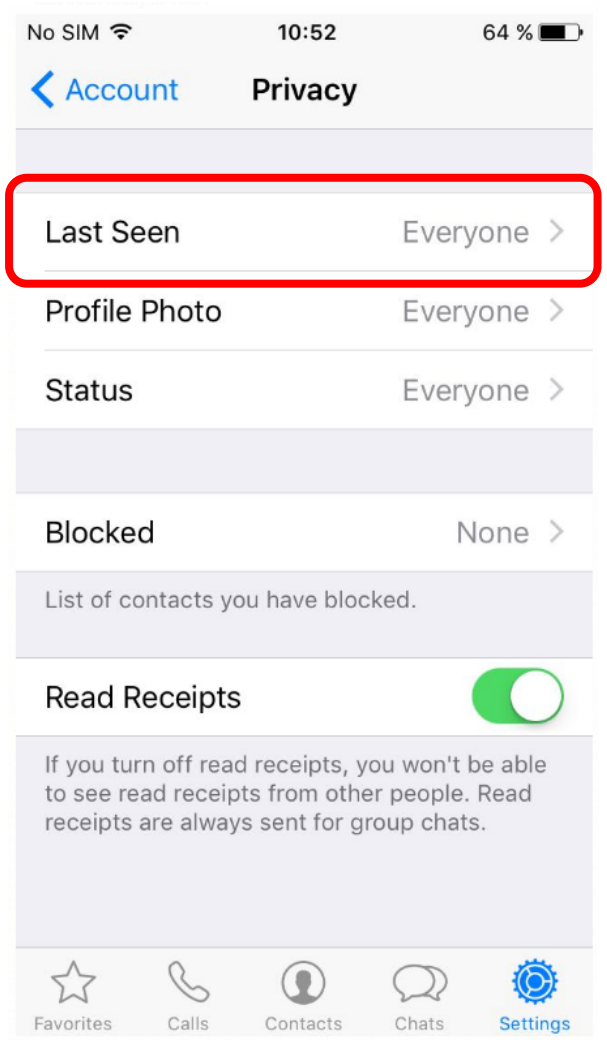
# WhatsApp | Default Settings and Privacy Concerns

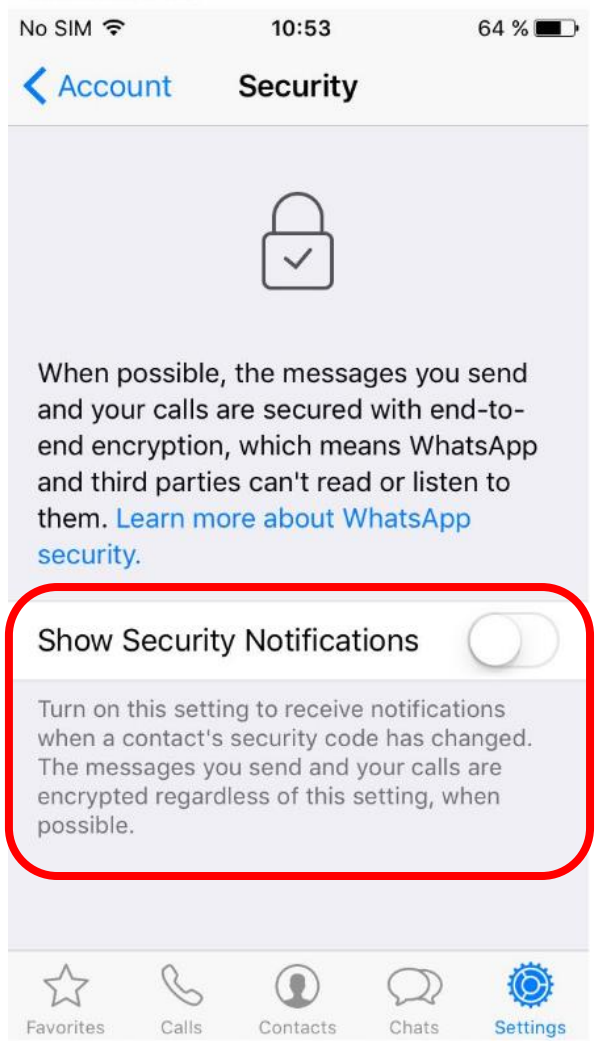
# WhatsApp | Default Settings and Privacy Concerns

# WhatsApp | Default Settings and Privacy Concerns

# WhatsApp | Default Settings and Privacy Concerns

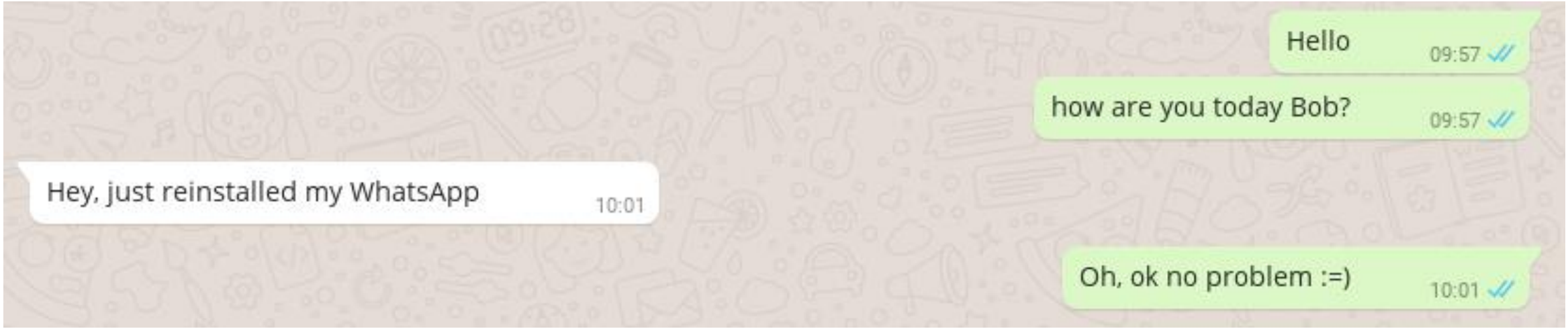



# WhatsApp | Default Settings and Privacy Concerns

WhatsApp sends

- Battery level
  - Plugged in or not?
- Location (Country)
- Language settings
- Exact WhatsApp version
- Exact phone model
- Exact OS info
- Crash messages (without notification)

# WhatsApp Web | MitM

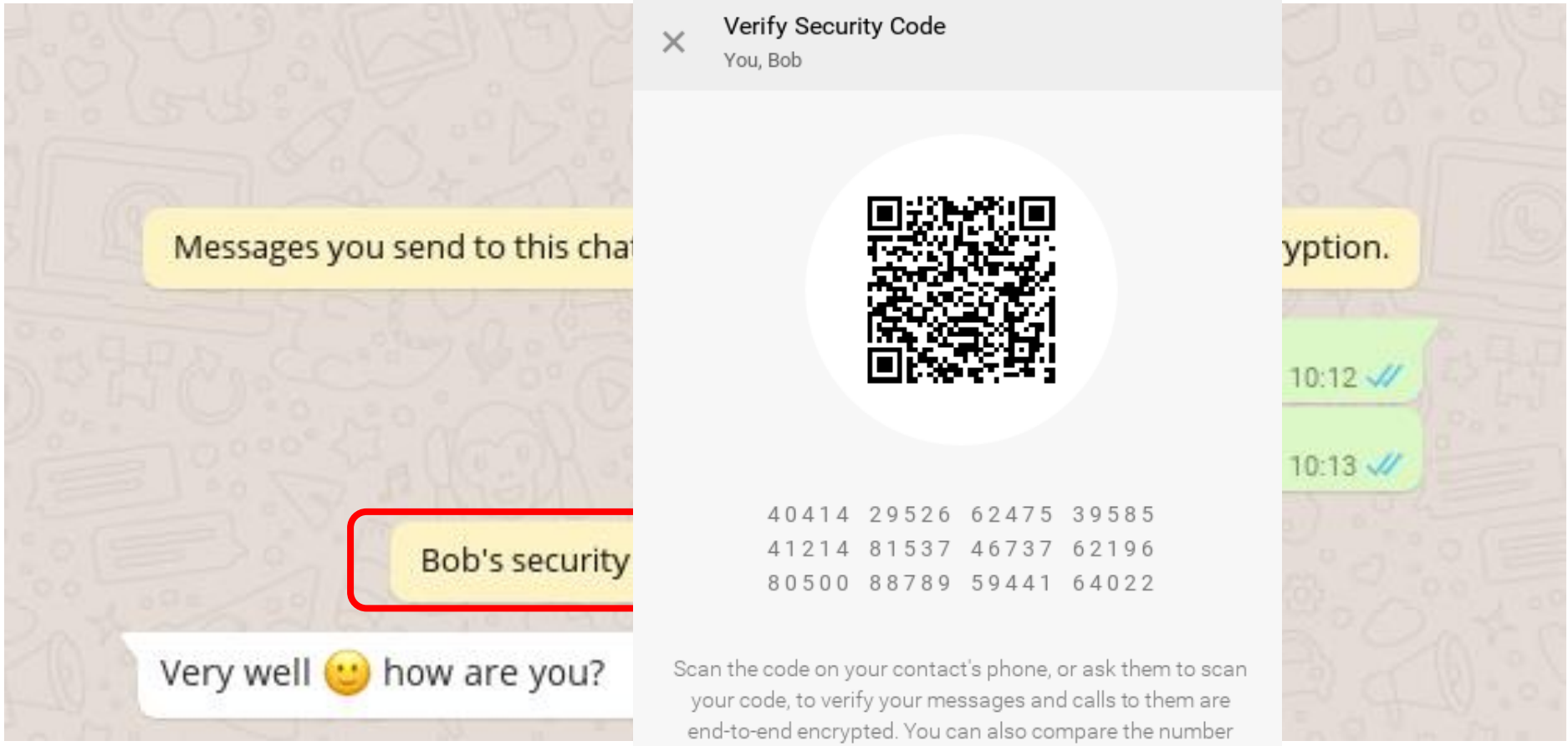


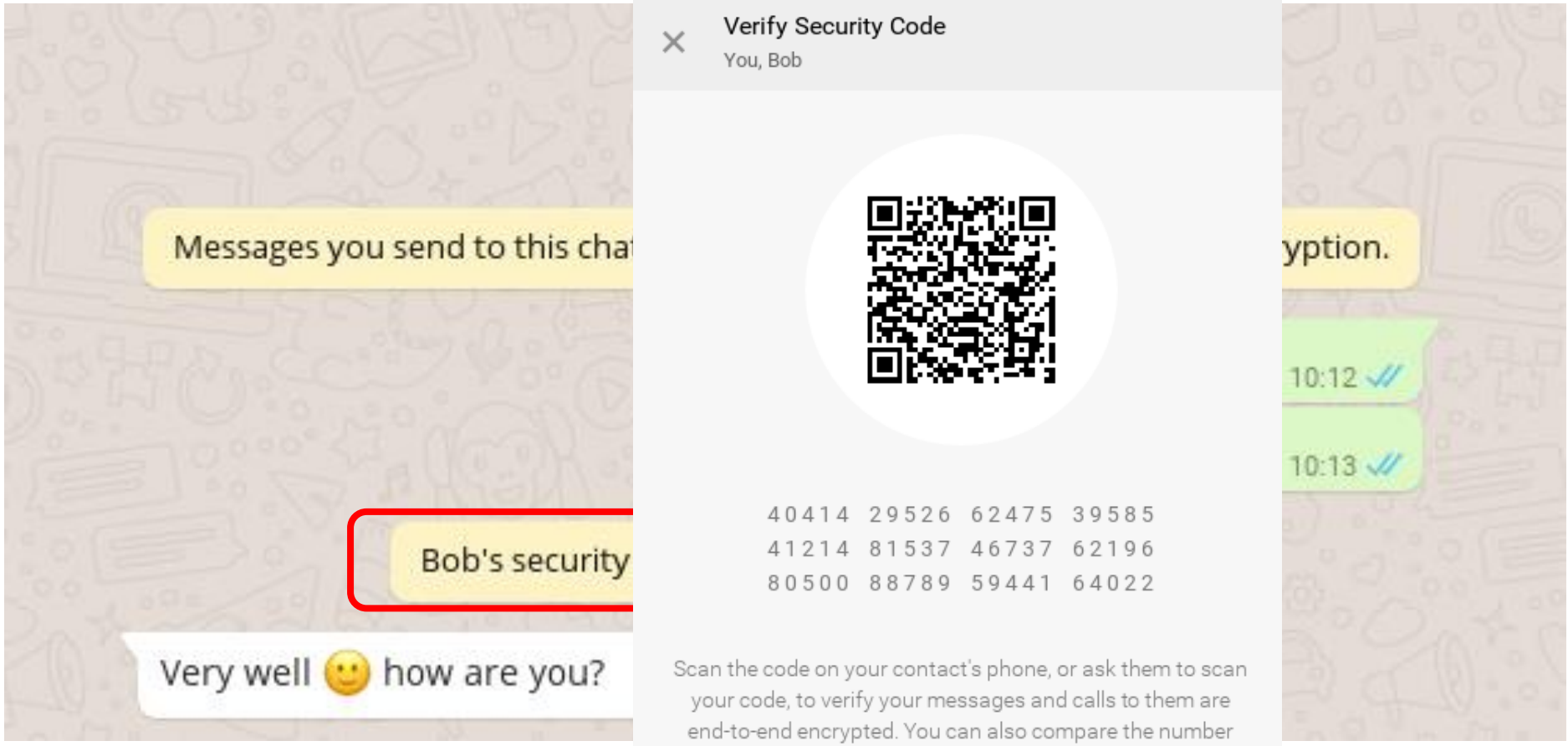
# WhatsApp Web | MitM




http://www.laughaton.com/uploads/images/11923-Attack.jpg


TODAY
Messages you send to this chat and calls are secured with end-to-end encryption.
Hey bob!
10:12
how is it going?
10:13
Bob's security code changed. Click for more info.
Very well how are you?
10:17


Messages you send to this cha
yption.
10:12
10:13
Bob's security
Very well how are you?
Verify Security Code
You, Bob
40414 29526 62475 39585
41214 81537 46737 62196
80500 88789 59441 64022
Scan the code on your contact's phone, or ask them to scan your code, to verify your messages and calls to them are end-to-end encrypted. You can also compare the number above to verify. This is optional. Learn more
SCAN CODE
UPLOAD CODE

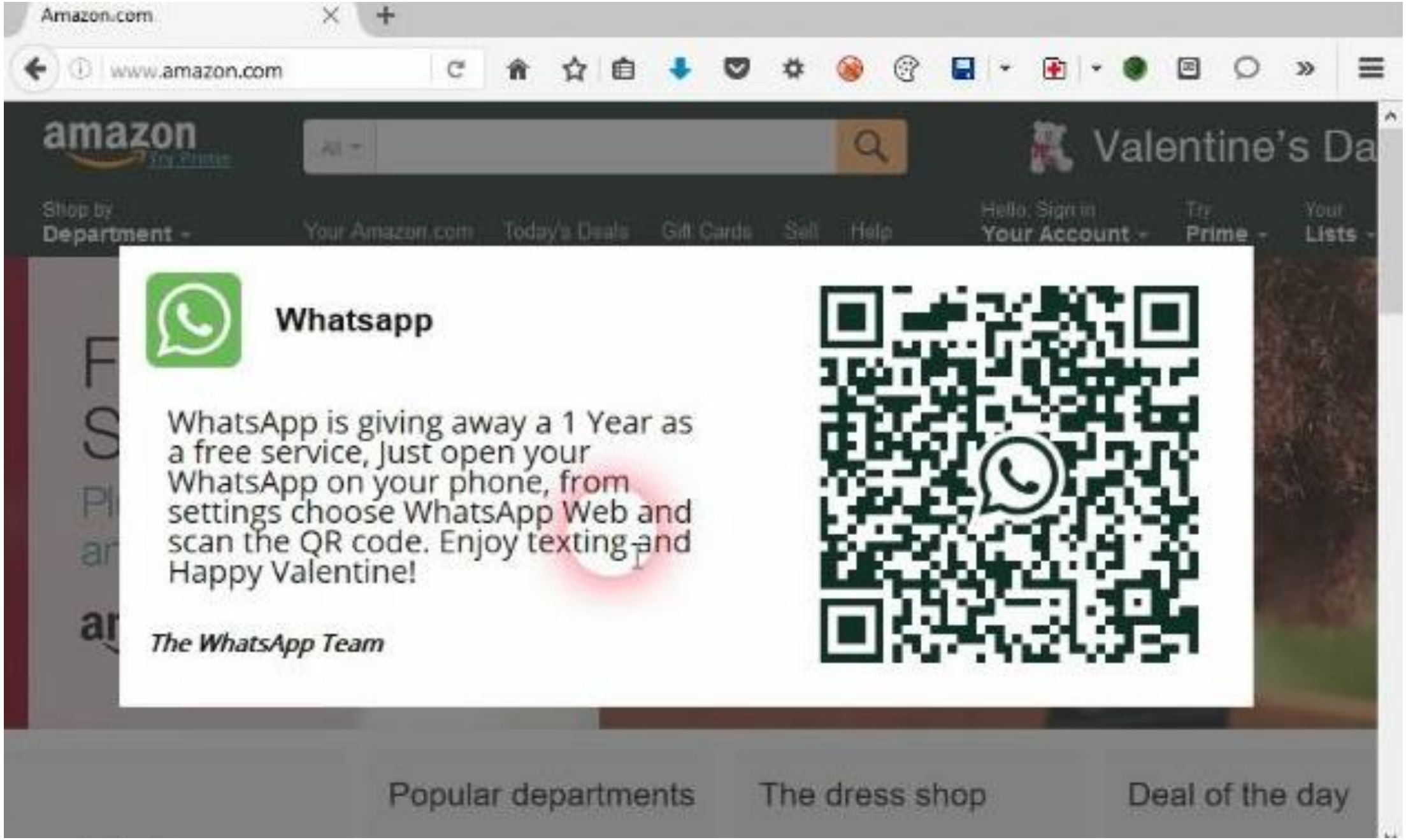



# Non-blocking! – Messages are sent anyway!

# General Issues

# Cross-Site-Scripting

- Both desktop messengers are mainly built out of JavaScript
- Attacker would be able to steal messages
- WhatsApp Web vs. Signal Desktop
  - Signal Desktop stores private identity key locally
  - WhatsApp Web never has access to the private identity key
- Probably easier to exploit within WhatsApp Web






https://www.seekurity.com/blog/wp-content/uploads/2016/11/PhishingPopup.jpg




https://www.seekurity.com/blog/wp-content/uploads/2016/11/PhishingPopup.jpg

# Storage

- WhatsApp uses the local browser cache
  - Stored in clear text
- Signal uses IndexedDB
  - Persistent client-side database which comes with HTML5
  - No way of encrypting Signal Desktop messages (like in the mobile application)

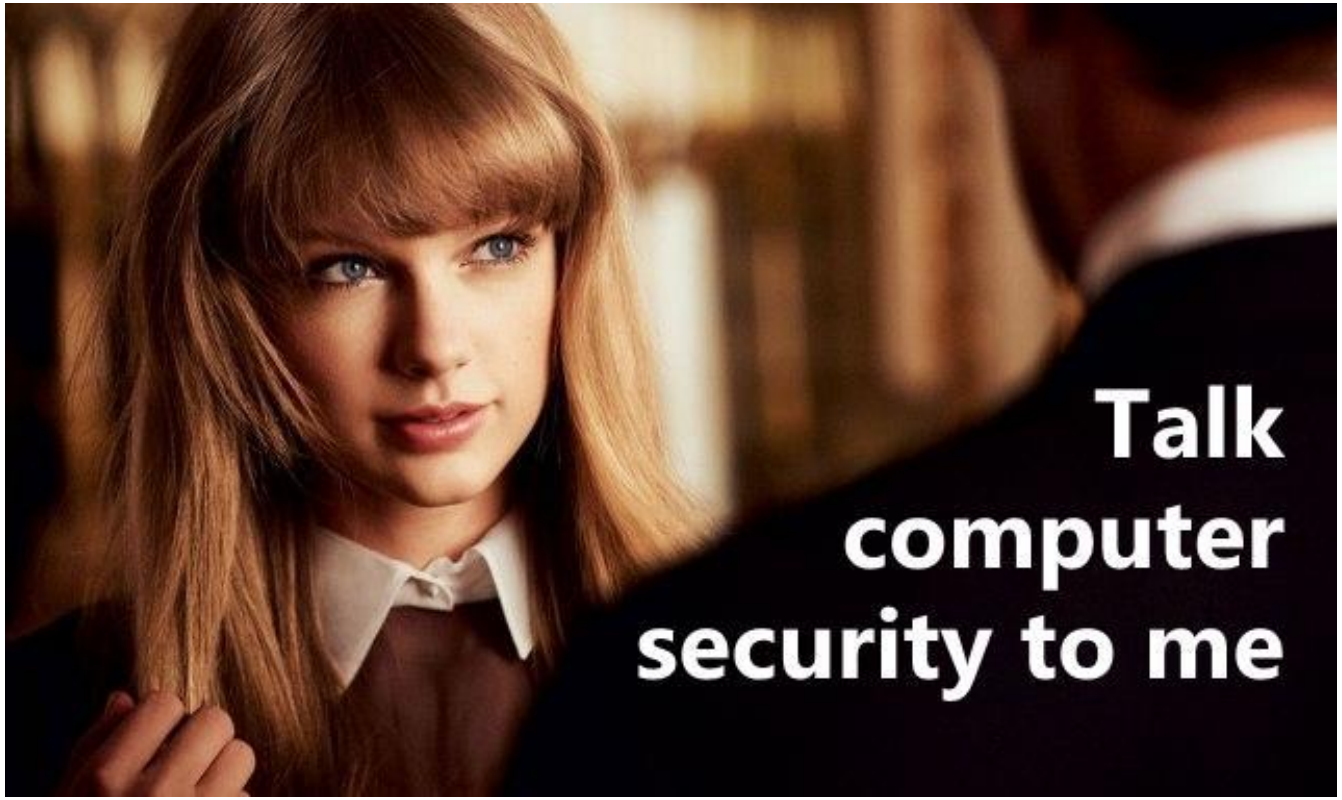
# Conclusion

- Signal Protocol most widely used E2E encryption protocol for messengers
- WhatsApp focuses on usability
  - Security notifications disabled by default
  - Retransmission problem
- Signal focuses on security
  - Security notifications enabled by default
  - More warnings can irritate users
- Providers can **ALWAYS MITM** users when keys are not verified

# Conclusion

- Both desktop variants store messages in cleartext on the disk
- Privacy
  - WhatsApp makes money out of **YOUR** data
  - Signal focuses on privacy

We as security focused people prefer Signal over WhatsApp, but this is not a big surprise ☺




# Q&A

@slashcrypto @pycycle
https://slashcrypto.org for the slides



http://i3.kym-cdn.com/photos/images/newsfeed/000/937/387/d9b.jpg