ChatSecure

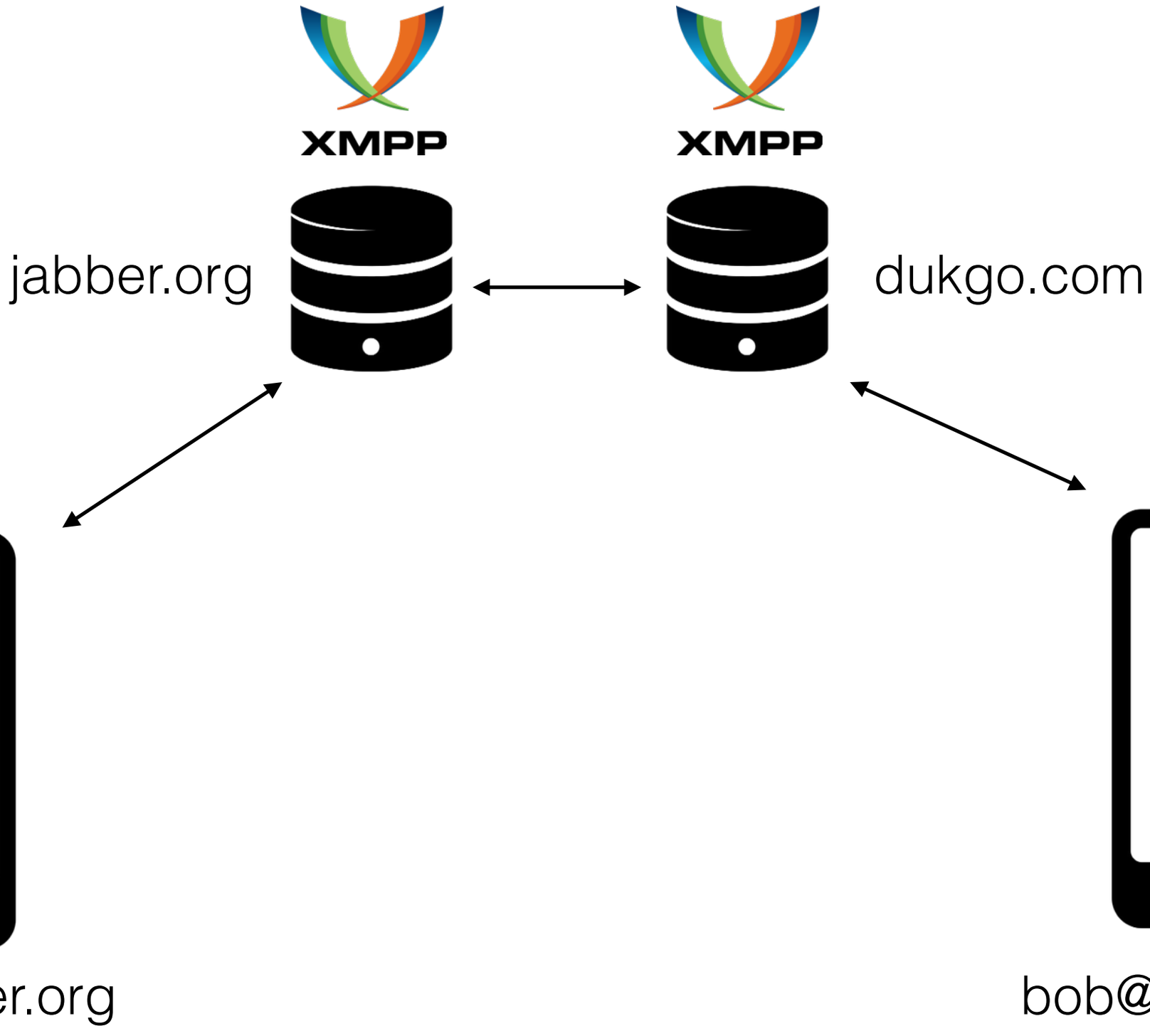
Free and open source OTR encrypted chat over XMPP
for iOS and Android.

@ChatSecure chatsecure.org

What is ChatSecure?

- Free and open source mobile chat application
- XMPP Compatible (Google Talk, Facebook, Jabber)
- OTR encryption
- Available for iOS and Android

XMPP Overview



Why XMPP?

- Decentralized
- Standardized
- Extensible
- Widespread implementation on desktop and mobile
- Supported by Google, Facebook (for now…)

Why not XMPP?

- Not designed for mobile
- No widely implemented standard for push messaging
- These limitations are especially problematic on iOS

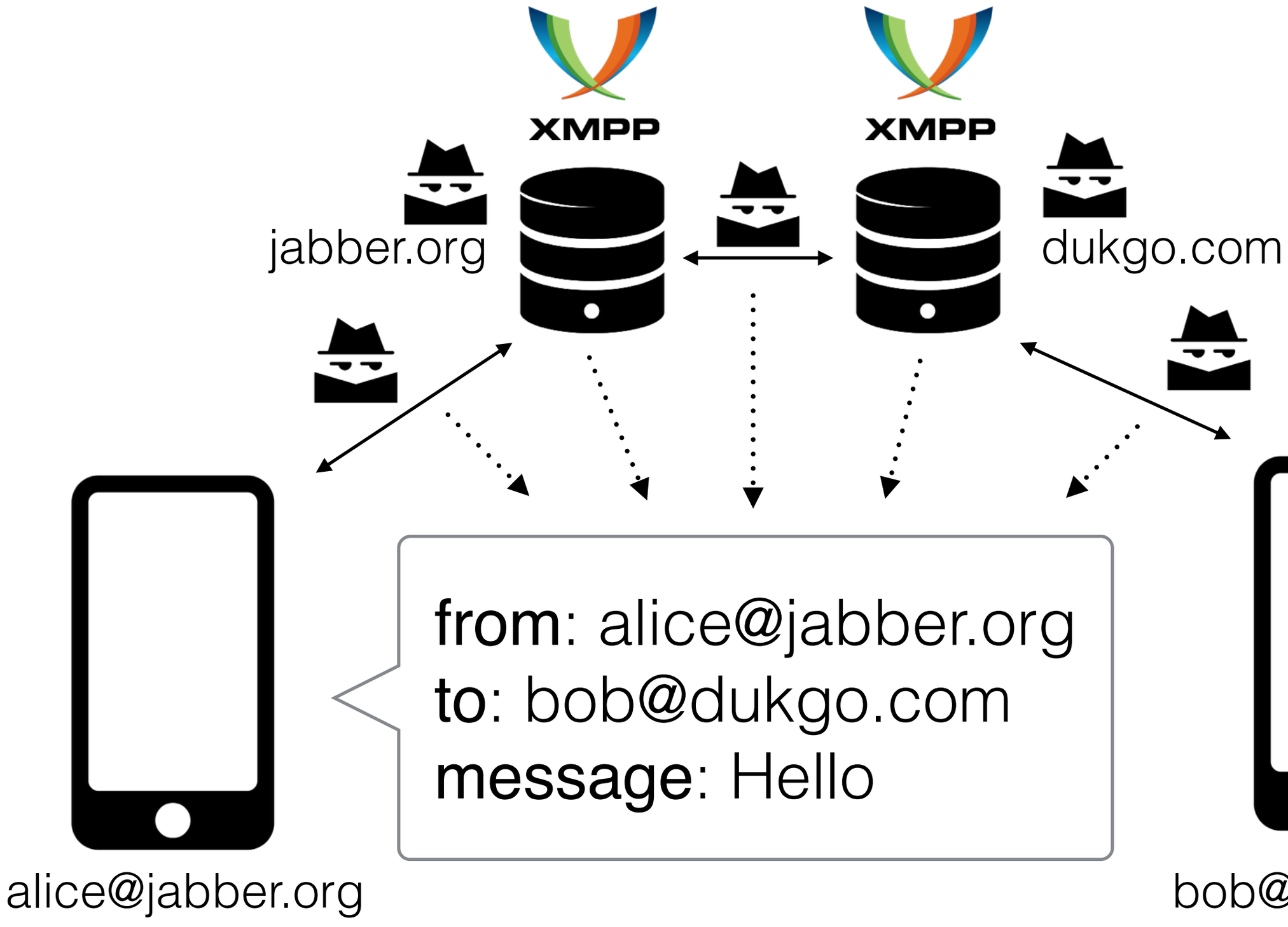
What is OTR?

- **Encryption**: No one can read your messages.
- **Authentication**: You know who you're talking to.
- **Perfect forward secrecy**: If your private key is compromised, your previous conversations are still safe.
- **Deniability**: Encrypted logs don't prove authorship.

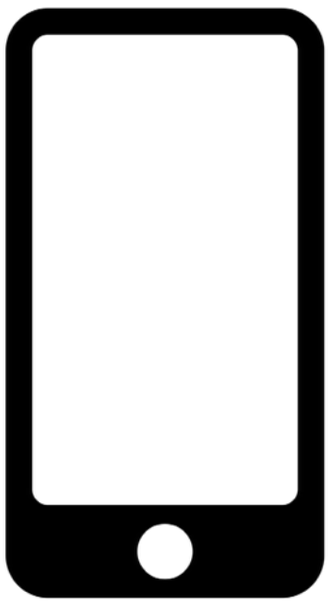
Why OTR?

- Designed by cryptographers Ian Goldberg and Nikita Borisov
- Widely implemented
- Around since 2004
- Implementations in Java (otr4j), C (libotr), bindings for Obj-C (OTRKit)

Without OTR


XMPP
XMPP
jabber.org
dukgo.com
from: alice@jabber.org
to: bob@dukgo.com
message: Hello
alice@jabber.org
bob@dukgo.com

With OTR



alice@jabber.org

from: alice@jabber.org
to: bob@dukgo.com
message: ?
OTR:AAIDAQAAAAMAAAAEA
AAAwBst9inn2mWrtsl0xuJIbo
11fLGb04G5TtdjTK1JVDlI74y
HMu2VSCbYlOxkOp/
8MCyeY2wREI/w/jC/zaQ/
j5hx9LL4BFFsBeeDdarFrEI/
40STTc0ZUljV5X37iwM2il0tCA
QIfMleSQFS2m13UdwROyVM
tN….

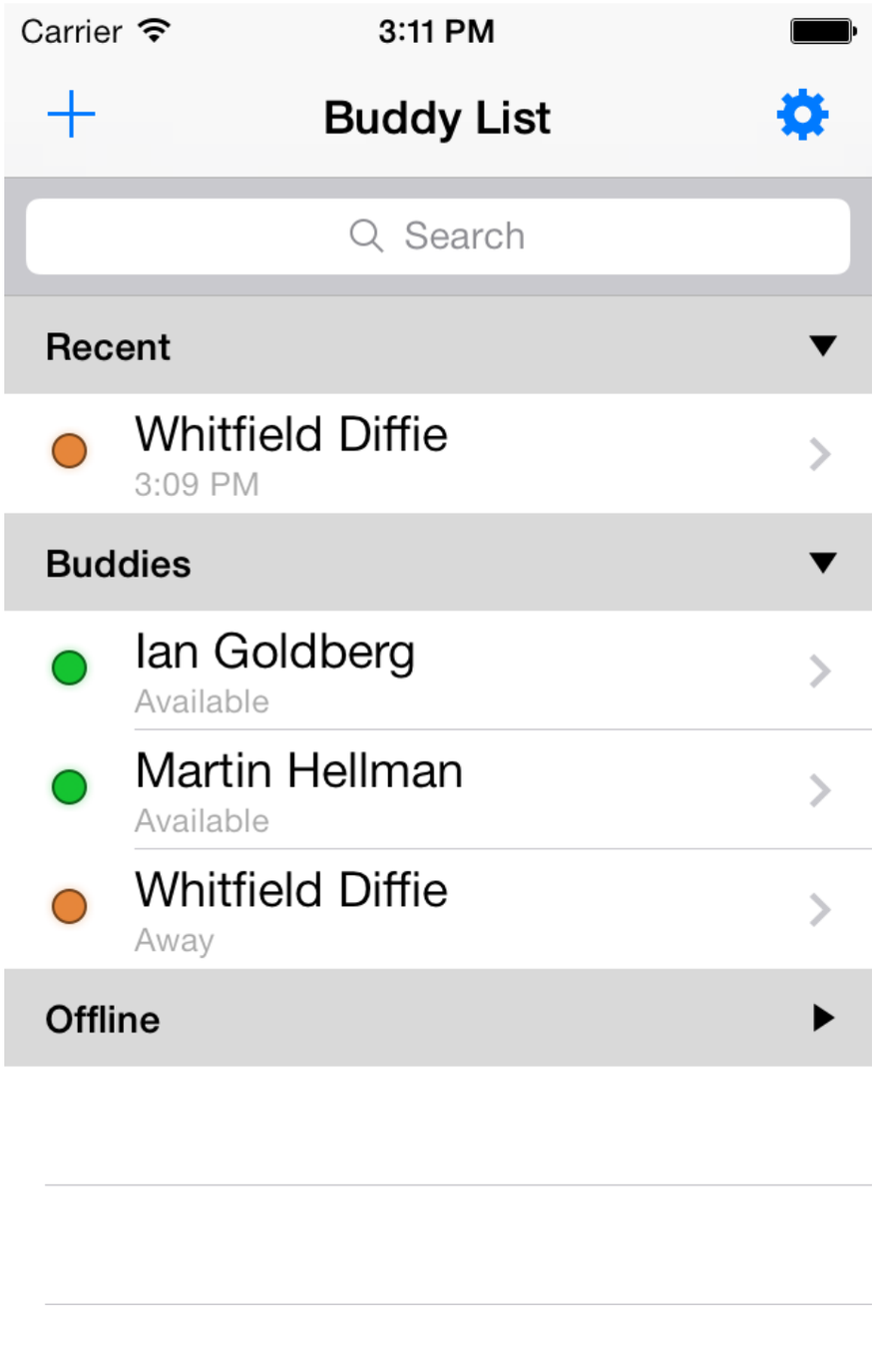
Why not OTR?

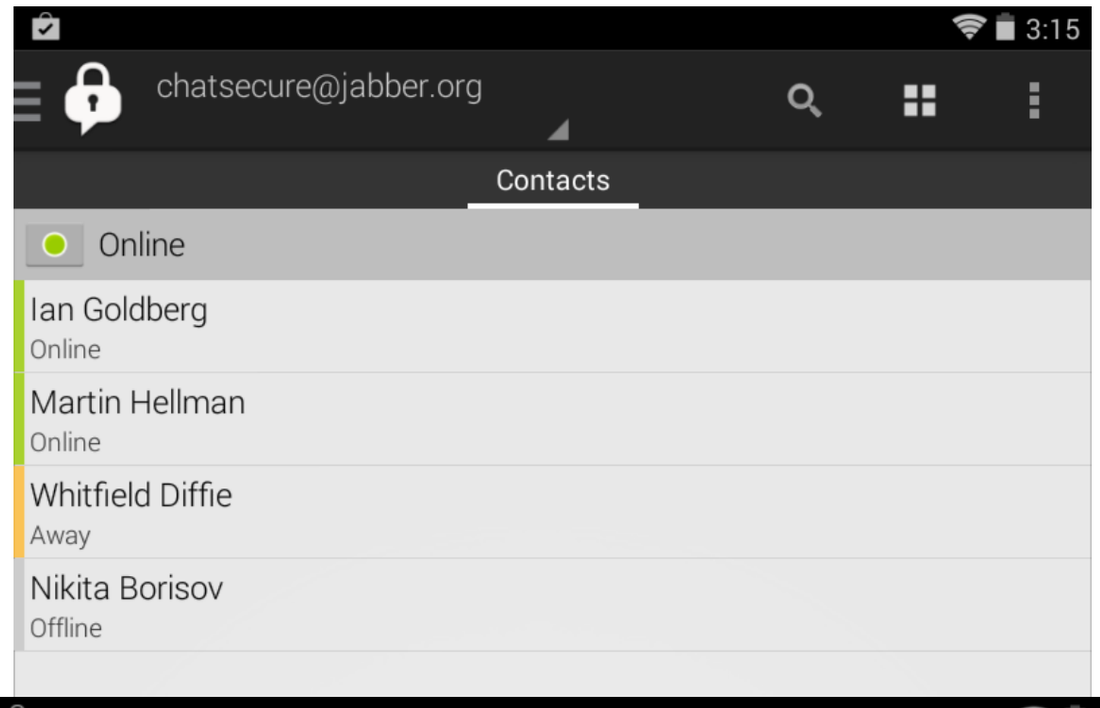
- Designed for synchronous communication (desktop)
- No support for group chats
- Not great on multiple devices, even with OTRv3
- Messages can be lost if sent to wrong client
- No way to sync messages across desktop/mobile

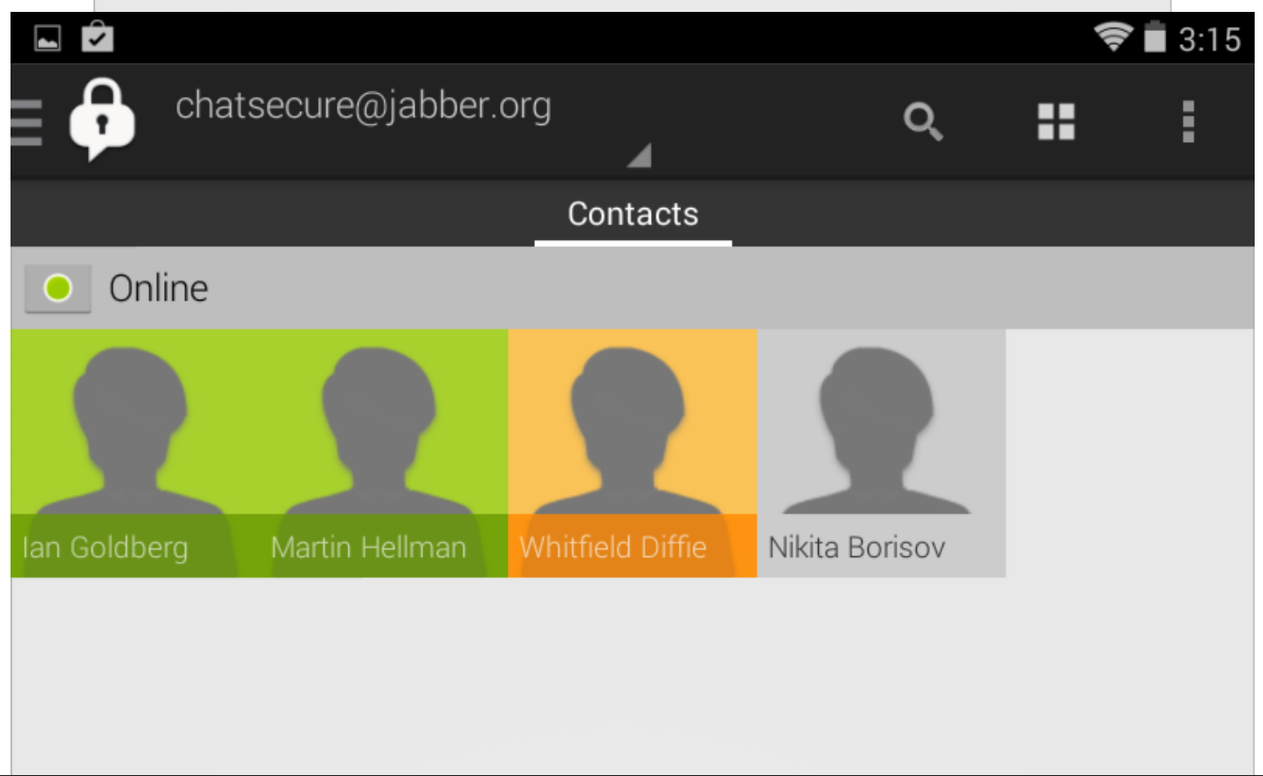
UX Issues

- Buddy lists are old school.
- No one verifies fingerprints.
- No onboarding, confusing for beginners.
- Very limited background support on iOS.
- No push messaging.
- Inconsistent UI between iOS and Android.

Buddy List

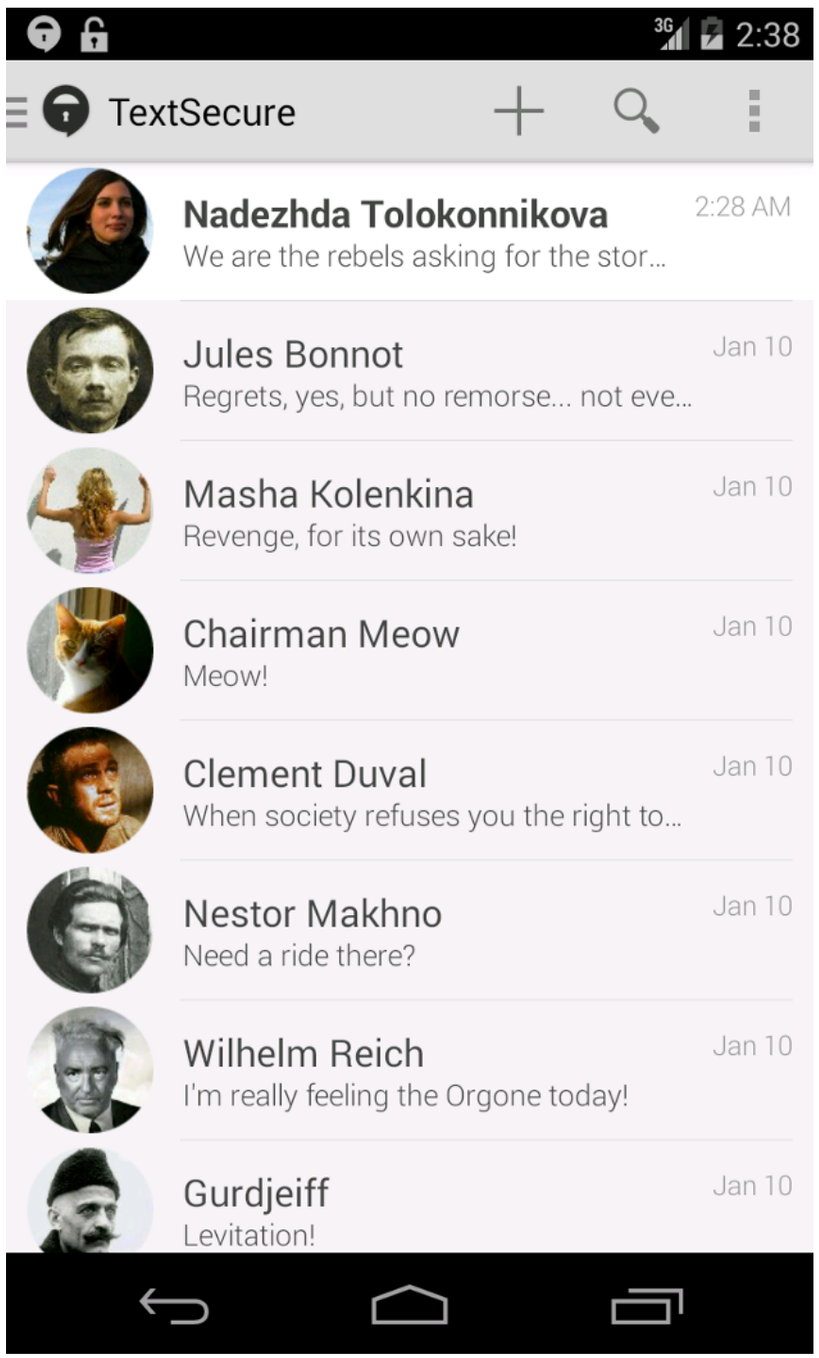

Carrier
3:11 PM
Buddy List
Search
Recent
Whitfield Diffie
3:09 PM
Buddies
Ian Goldberg
Available
Martin Hellman
Available
Whitfield Diffie
Away
Offline


3:15
chatsecure@jabber.org
Contacts
Online
Ian Goldberg
Online
Martin Hellman
Online
Whitfield Diffie
Away
Nikita Borisov
Offline

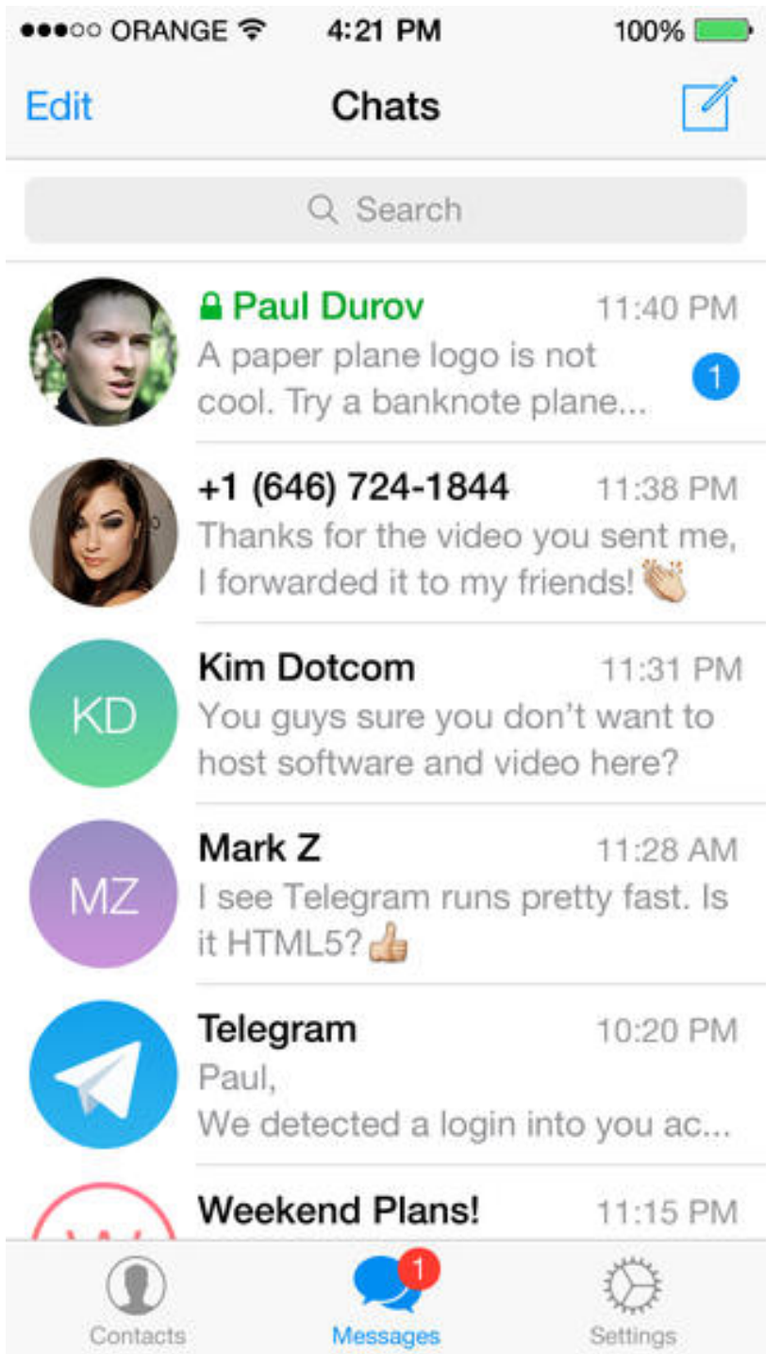

3:15
chatsecure@jabber.org
Contacts
Online
Ian Goldberg
Martin Hellman
Whitfield Diffie
Nikita Borisov

Other Apps

TextSecure

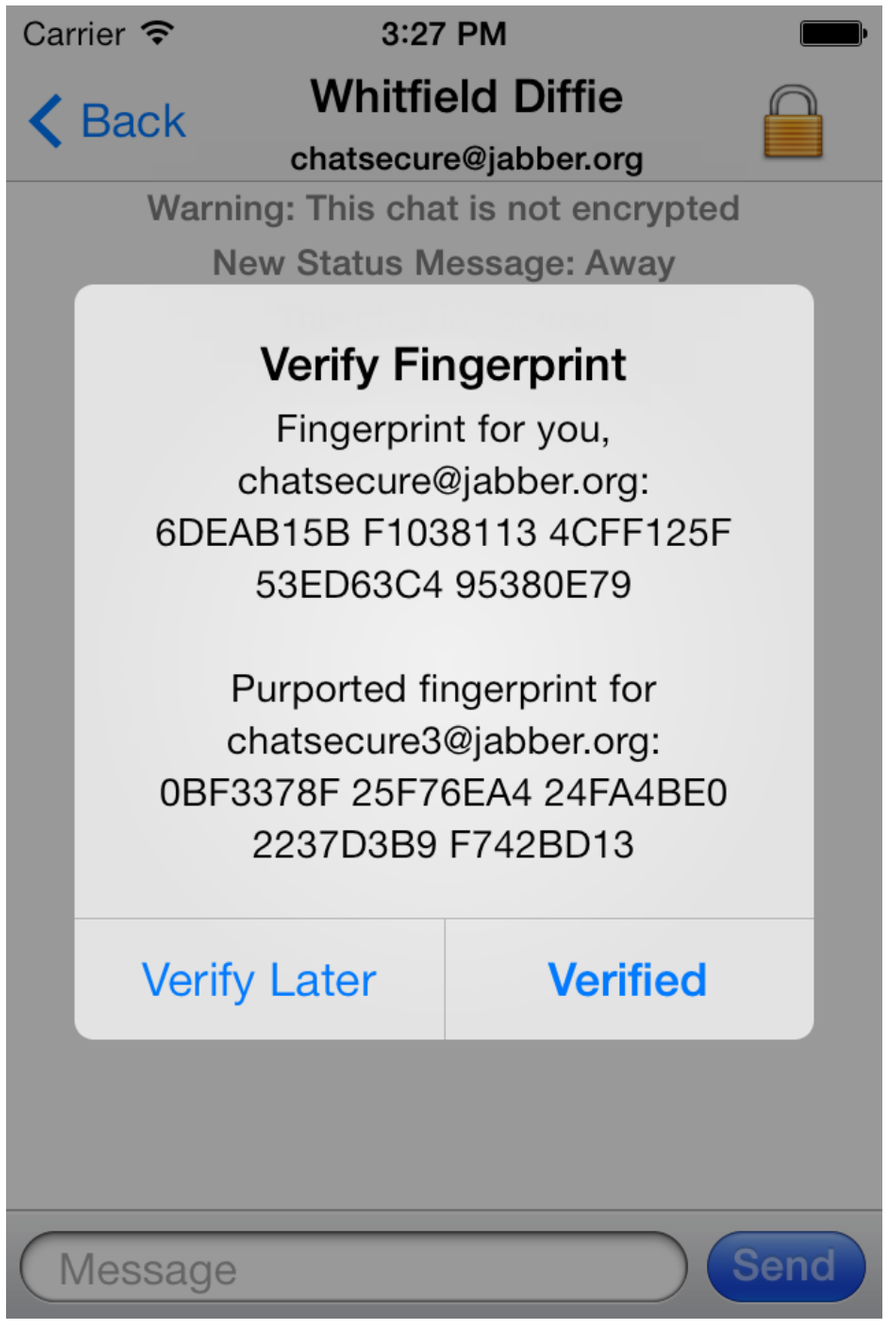


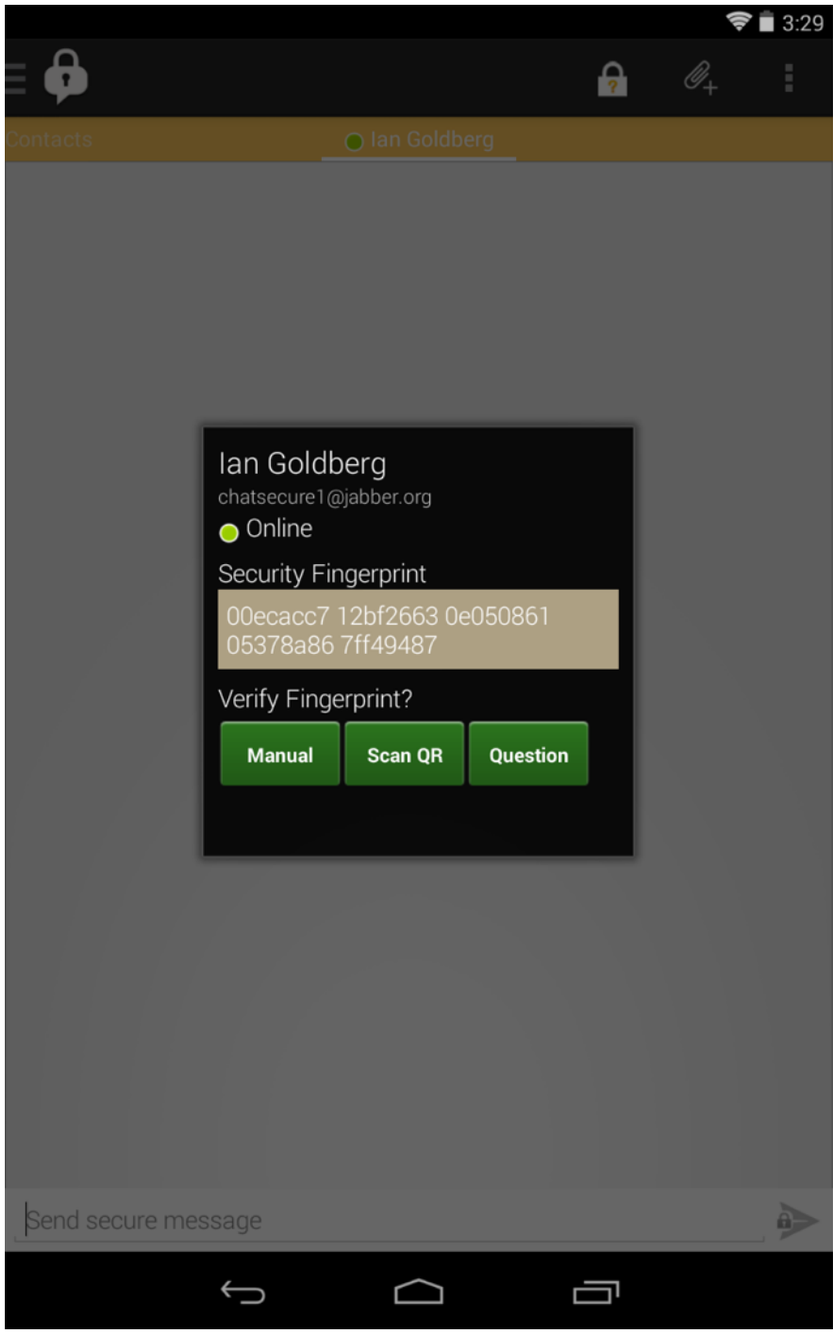
Telegram



Threema

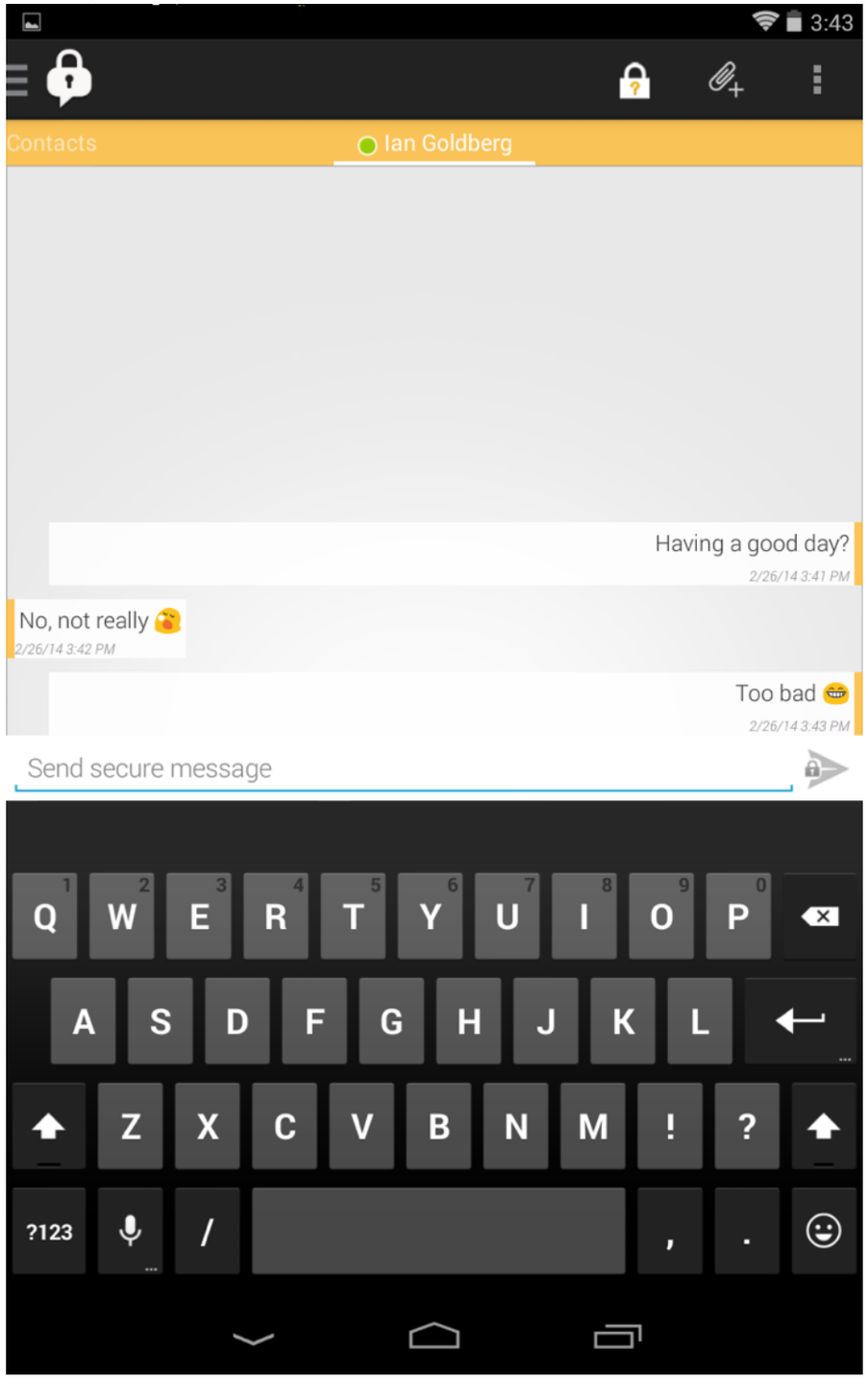
Fingerprint Verification





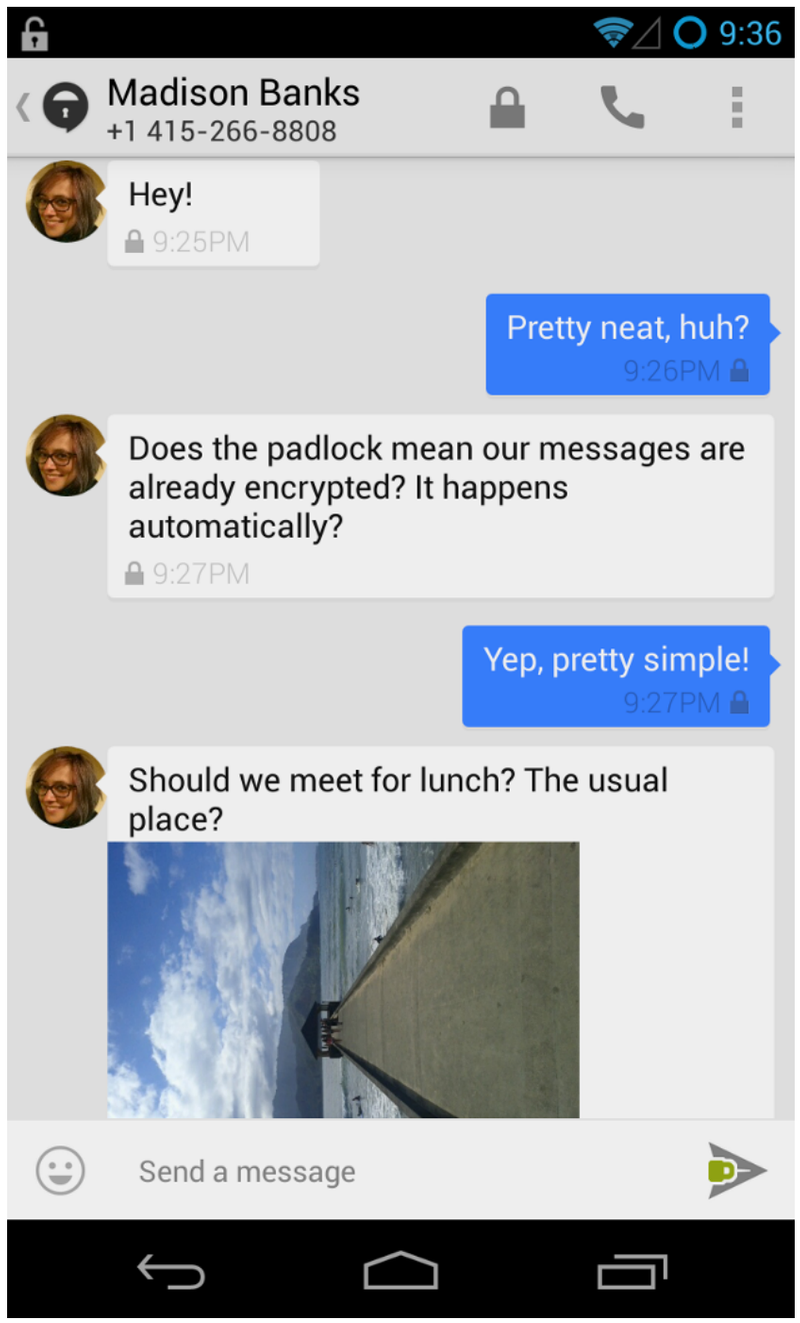
Chat View


Carrier
3:39 PM
Back
Martin Hellman
chatsecure@jabber.org
New Status Message: Available
Warning: This chat is not encrypted
This chat is secured
Feb 26, 2014 3:38 PM
Hello
Excuse me?
Goodbye
Message
Send


3:43
Contacts
Ian Goldberg
Having a good day?
2/26/14 3:41 PM
No, not really
2/26/14 3:42 PM
Too bad
2/26/14 3:43 PM
Send secure message

Other Apps

TextSecure



Telegram

Threema

Attribution

- Smartphone by George Agpoon from The Noun Project
- Server by Sergio Luna from The Noun Project
- Spy by Dan Hetteix from The Noun Project