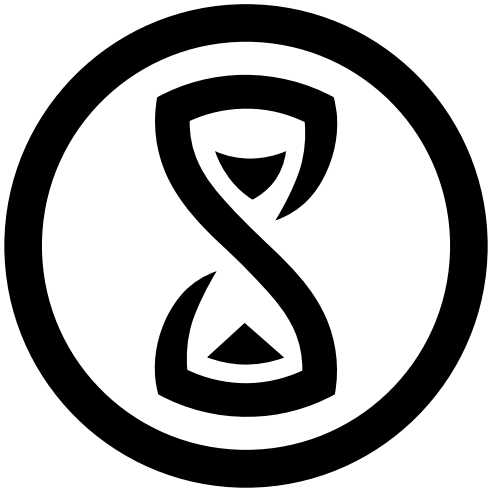
Sichere Kommunikation via Smartphone

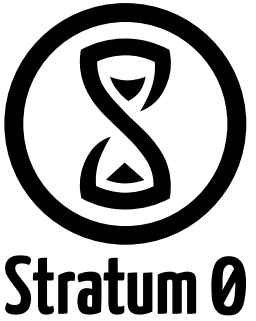
Eine Aufstellung verfügbarer Mobile Messenger für Android und iOS



Emantor

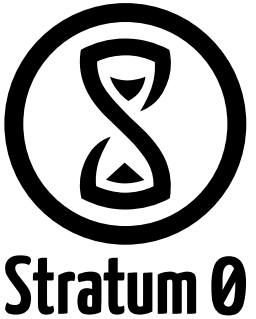
14.03.2014

Inhalte



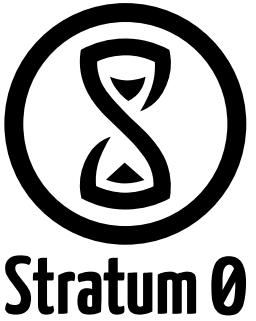
- Disclaimer
- XMPP + OTR
- Telegram
- Threema
- TextSecure
- Fragen? Diskussion?
- Random Stuff

Disclaimer



I ain't no cryptographer, don't judge me to hard and correct my mistakes!

XMPP – Komfortabilität



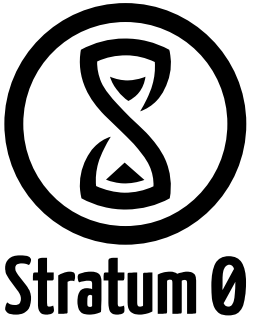
- Verschiedene XMPP Clients mit OTR sind sowohl für Android als auch iOS verfügbar
- XMPP Registrierung muss selbst durchgeführt werden
- Dazu wird ein Server mit annehmbarer Uptime benötigt
- OTR Key wird automatisch erstellt
- OTR Verbindung kann automatisch durch „magic whitespace“ initiiert werden
- OTR ist für synchrone Kommunikation ausgelegt, synchrone Auslieferung von Nachrichten bei Geräten im Ruhezustand entweder unmöglich oder kostet viel Batterieleistung

XMPP + OTR: Sicherheit

Stratum 0

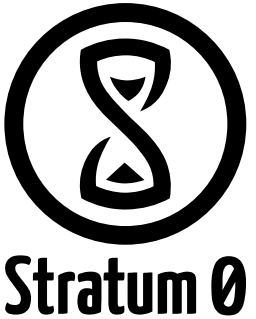
- XMPP unterstützt TLS
- OTR bietet Perfect Forward Secrecy
- Validierung der Kontakte über Fingerprint oder geheime Frage
- Kontinuierlicher DH-Schlüsselaustausch während der Nachrichten
- Key acknowledge, new key advertisment pro Nachricht

Telegram - Allgemein



- Für alle großen mobilen Betriebssysteme, die Linux Kommandozeile und als Browser-Plugin
- Registrierung über Telefonnummer
- Adressbuch wird automatisch hochgeladen (Keine Angaben in welchem Format)
- Standardmäßig kein „Geheimer Chat“ d.h. keine Ende-zu-Ende Verschlüsselung

Telegram – Sicherheit



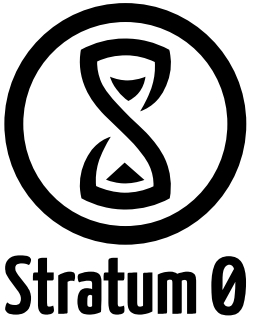
- Telegram nutzt TLS
- Eigens Entwickeltes Protokoll
- Gerät generiert einen Schlüssel der per DH mit dem Server ausgetauscht wird
- Nachrichtenschlüssel werden aus SHA1 der Nachricht und dem zuvor genannten Schlüssel generiert
- Für Secret Chats findest ein DH Austausch zwischen den betreffenden Clients statt
- For more information visit: https://core.telegram.org/mtproto

Threema – Allgemein

Stratum 0

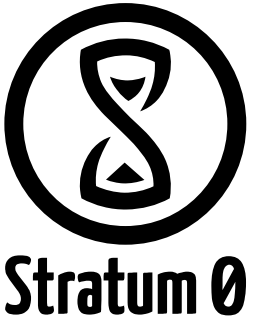
- Registrierung über Telefonnummer optional
- Für Android & iOS verfügbar
- Validierung von Fingerprints durch QR-Code Scan
- Kostet ~2€ im Play und Apple Store

Threema - Sicherheit



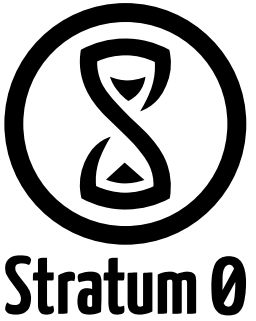
- NaCL cryptobox Implementierung
- Public/Private Keypair wird auf dem Gerät generiert
- Public Key wird auf den Server hochgeladen
- Individuelle nonce pro Nachricht, cipher ist XSalsa20
- For more information visit NaCL Website
- Keine Informationen darüber was neben der crypto-Kommunikation geschieht
- Bietet Validierungswebsite an

TextSecure - Allgemein



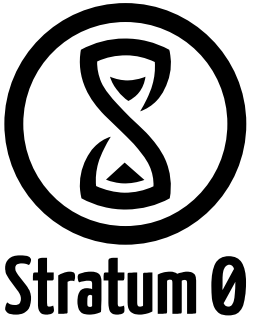
- Registrierung durch Telefonnummer
- Standard SMS App Replacement (unter Android, iOS unterstützt dieses Feature nicht)
- Upload der Kontakttelefonnummern als Hashes, Server liefert Treffer zurück
- Automatisches versenden von Push-Nachrichten sofern beide Kontakte TextSecure besitzen
- Fallback auf SMS falls keine Daten verfügbar sind
- Validierungsanzeige (noch) nicht verfügbar

TextSecure - Sicherheit



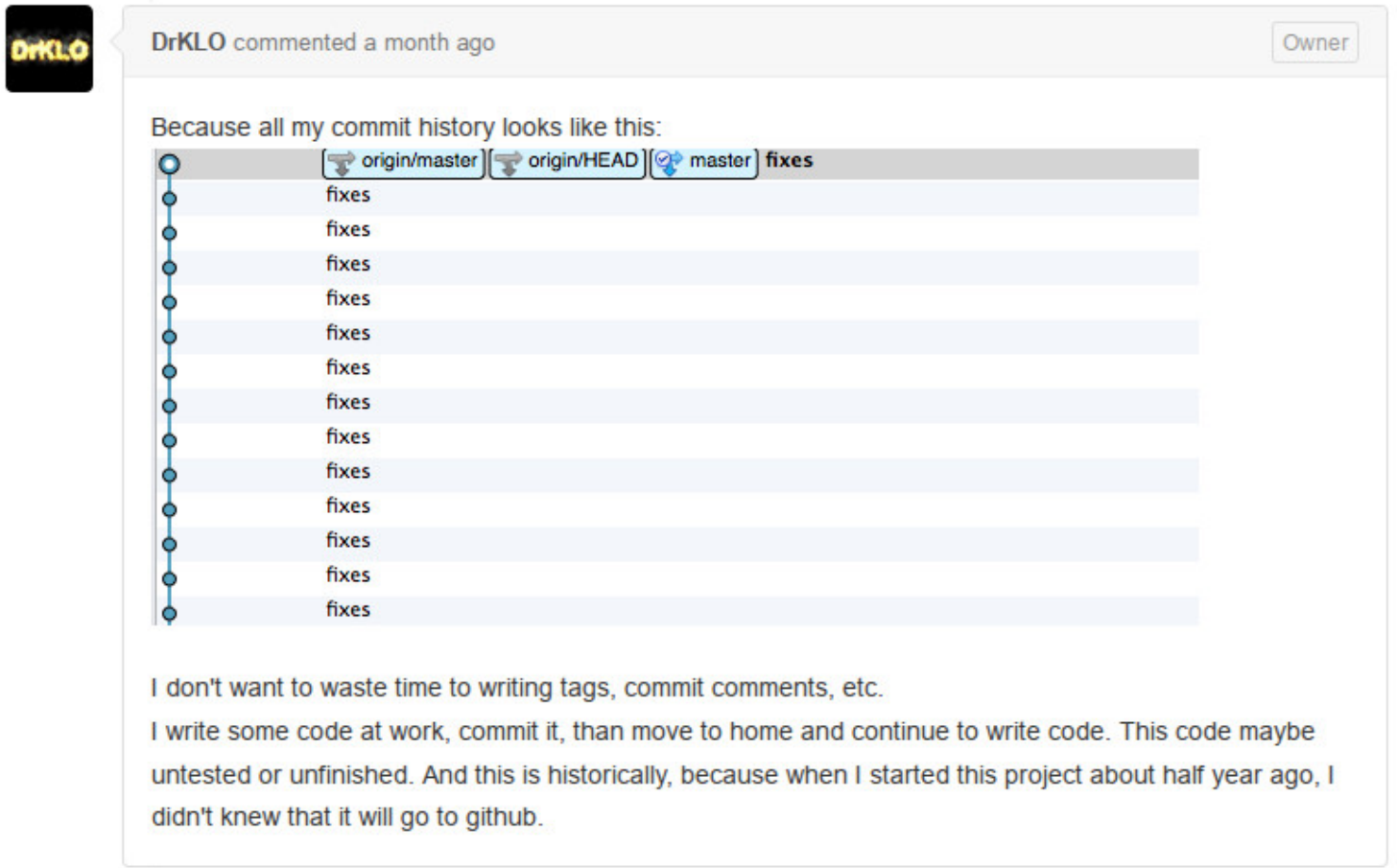
- TLS mit certificate pinning
- NaCL ECC25519 public/private Keypair
- Master key derived from ephemeral keys or pre key
- Initial root and chain key derived from master key using HKDF
- Chain Key is used for subsequent messages without messages from the other party
- For more information visit: https://whispersystems.org/blog/advanced-ratcheting/

Fragen? Diskussion?



Sonst gibt's noch Random Stuff

Random Stuff – Telegram



DrKLO commented a month ago — Owner

Because all my commit history looks like this:

origin/master | origin/HEAD | master | **fixes**

fixes
fixes
fixes
fixes
fixes
fixes
fixes
fixes
fixes
fixes
fixes
fixes
fixes

I don't want to waste time to writing tags, commit comments, etc.
I write some code at work, commit it, than move to home and continue to write code. This code maybe untested or unfinished. And this is historically, because when I started this project about half year ago, I didn't knew that it will go to github.

Random Stuff – TS Activity

Stratum 0

February 14 2014 - **March 14 2014**

Period: **1 month**

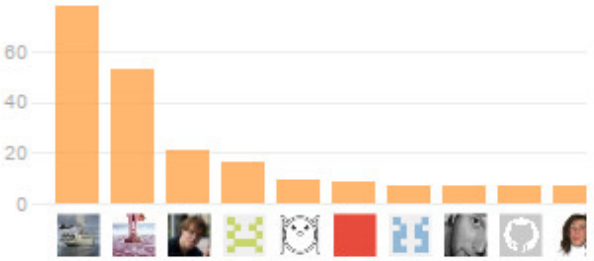
Overview

67 Active Pull Requests

466 Active Issues

29 Merged Pull Requests	**38** Proposed Pull Requests	**231** Closed Issues	**235** New Issues

60 authors have pushed **322 commits** to all branches, excluding merges. On master, **417 files** have changed and there have been **17,067 additions** and **3,032 deletions**.



29 Pull Requests merged by **18** people

Kthx, bai

Emantor
phoenix@emantor.de

Stratum 0 e.V. Braunschweig
https://stratum0.org