Threema GmbH
Staldenbachstrasse 11
CH-8808 Pfäffikon SZ

Rapperswil, November 2, 2015

Security Review Threema: Security Statement

To whom it may concern

Threema GmbH provides a secure messaging service (Threema). The service runs on mobile devices (smart phones and tablets) in collaboration with a centralized message routing system. Threema provides secure messaging with end-to-end encryption. In order to assure the expected security, a review of the App and of the centralized functions has been performed, including a review of the source code for critical and encryption-relevant functions. The goal of the investigation was to confirm that the quality of the system meets the security claimed in the public Threema specification. Furthermore, the investigation was to compare the solution with the state of the art, to identify any weaknesses, and to come up with recommendations for improving the situation where this seems necessary. cnlab security AG (cnlab) has performed this review in August 2015.

Based on our work we can testify that Threema allows secure end-to-end communication. We do not see immediate need for improvements in the investigated areas. In particular, we have not detected any weakness in the implementation of the used encryption mechanisms. We further confirm the quality of the system as claimed by Threema in their public specification.

Based on this review, we can summarize that Threema provides a security level which compares favorably with the state of the art in similar messaging services.

In the sequel we provide further information regarding compliance with the security statements which are published on the Threema web site.

Sincerely, cnlab security AG

Threema Public Security Statements

Threema makes a number of statements about the security of the Threema system (on the Threema web site). We provide here a short assessment on the correctness of these security statements.

Encryption

Threema Statement: “Threema encrypts all your communications end-to-end including messages, group chats, files and even status messages. You can rest assured that only the intended recipient can read your chats, and nobody else – not even us.”

cnlab has verified on Android and iOS Apps that all communication is encrypted end-to-end. The implemented encryption algorithms are appropriately selected and appropriately used.

Guaranteed Privacy

Threema Statement: “Threema is designed to generate as little data on servers as possible: Group memberships and contact lists are managed on your device only. Messages are immediately deleted after they have been delivered. This effectively prevents the collection of meta data.”

cnlab has verified this statement: No divergences have been observed in this area.

Trusted Contacts

Threema Statement: “Verify your contacts simply by scanning their QR code or comparing key fingerprints. This makes sure you're really talking to the intended person and not a man-in-the middle.”

cnlab has verified this statement: Partners can be reliably identified if the Threema ID is used as the identifying element.

Full Anonymity

Threema Statement: “Each Threema user receives a random Threema ID for identification. A phone number or email address is not required to use Threema. This unique feature allows you to use Threema completely anonymously.”

cnlab has verified this statement: No divergences have been observed.

Independent Company

Threema Statement: “We are a 100% independent and self-financed company in the heart of Switzerland with its own servers and in-house software development. Switzerland is a country with some of the most user friendly privacy laws in the world.”

cnlab has verified this statement: No divergences have been observed.

Note: Ownership and financing related statements have been compared with publicly available official information about Swiss companies. No in-depth analysis has been implemented in this area.

No-nonsense Privacy Policy

Threema Statement: “Threema's transparent privacy policy is concise and fits on a sheet of paper.”

cnlab has verified this statement: No divergences have been observed.