Reference Sheet

Privacy and Security

This document summarizes how privacy and security form the very core of Threema Work and how they are applied during use.

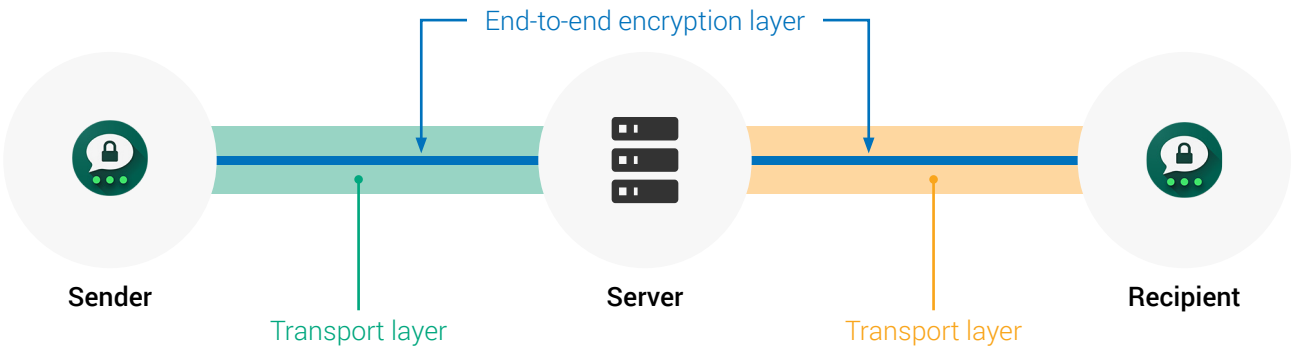
1. Introduction

Threema Work and Threema are based on the same blueprint and share the same principle of avoiding metadata through decentralization to the largest possible extent. In contrast to conventional cloud services, messages and media files are transmitted **categorically without any storage**. The aim is to provide a maximum of security with a minimum of metadata. **Messages are transient and are immediately deleted from the server after successful delivery**. The app doesn't require an email address or phone number and is therefore suitable for tablet use.

The Threema app is used by millions of private and business users worldwide and has been consistently proving its reliability, scalability, and security ever since its launch in 2012. **Our award-winning data protection and security measures, as well as the general concept, have been successfully audited and verified multiple times.**

2. Encryption and key-pair management

Threema's state-of-the-art asymmetric cryptography protects messages between sender and recipient and additionally the communication between app and server. The open-source library NaCl, the encryption protocol Threema uses, can be verified independently at any time.



Threema uses **two encryption layers**: an end-to-end encryption layer between the chat partners, and an additional transport layer, which protects against the interception of the connection between app and server. This prevents an attacker who is recording network packages (e.g. in a public wireless network) to reveal a user identity.

Users are identified with the so-called **Threema ID**: a randomly generated eight-digit string that is irrevocably associated with the encryption key pair. The key pair consists of a private and public key. The former remains on the device, while the latter is sent to the server.

Any encryption or decryption of a message occurs exclusively and directly on a user device. Only the user has control over key exchanges. No third party – not even the provider – can decrypt the content of a message.

Our extensive Cryptography Whitepaper explains in full detail all concepts and algorithms relating to the encryption and transmission of data.

3. Physical Security

Threema GmbH runs its own servers in an a high-security data center of an ISO 27001-certified colocation partner in Zurich. This state-of-the-art data center includes biometric access control, full-height turnstiles, video surveillance, emergency power systems, fire protection, fail-safe air-conditioning, and a fully redundant Internet connection.

In addition, Threema GmbH disposes of a second hosting site at a separate location used for the defense of DDoS attacks and the bridging of network failures. It corresponds to the security features of the main location to the largest possible extent.

4. Legal Compliance

Using Threema ought to generate as little data on the servers as possible. At the root of Threema's basic concept, **data protection is our undisputed core** competency. Threema Work is **fully compliant with the European General Data Protection Regulation (GDPR)**. As a Swiss company, Threema is also subject to Switzerland's strict Federal Act on Data Protection (DSG) and the accompanying Ordinance to the Federal Act on Data Protection (VDSG).

Transmitting data from the EU to Switzerland is permitted by law without any additional evaluation. Based on Article 25 (6) of the European Data Protection Directive, Swiss law guarantees a level of data protection equivalent to European legislation.

Details on data handling practices at Threema are included in the annex.

5. Decentralized Architecture

Data such as contact lists or group chats is managed solely on user devices and not on Threema servers. The latter assume the role of a switch; messages and data get forwarded, but not permanently stored. This guarantees the highest possible data security:

- **Immediate deletion of messages upon successful delivery.** All messages and media files are transmitted end-

to-end encrypted in Threema. Even if someone could intercept your message, it would be completely useless. Only the intended recipient is able to decrypt and read a message.

- **No storage of contact lists:** Your address book's email addresses and phone numbers are anonymized (hashed) before they are sent to the server. Once the comparison is finished, they are immediately deleted from the server.
- **Local creation of the key pair used for encryption:** Your private key remains unknown to us. It is technically impossible for us to decrypt message contents.
- **No analytics related to individuals,** no logs about who is communicating with whom, no disclosure of data to third parties, no subcontracts.

Annex: Details on data handling practices

The following list contains detailed about when and why data is generated when using Threema Work and who has access to it to what extent.

Data generated when creating a Threema ID

- Key pair (locally generated). Public key is sent to server, private key remains on device.
- Threema ID (eight digits, generated by server).
- Creation date (without time) of the Threema ID.
- Push Token used to receive push notifications (Android: GCM; iOS: APNS; Windows Phone: MPNS).
- Optional
  - Depending on app settings: The link between a Threema ID and a phone number or email address is transmitted to the server. Email addresses are hashed.
  - If the optional contact synchronization is enabled, phone numbers and email addresses are transmitted hashed to the server, where they are matched with encrypted links. Once the process is completed, they are immediately removed from the memory.
  - Linking a Threema ID to an email address or phone number is optional, and so is contact synchronization. As an alternative or in addition, contacts can be added using the management cockpit in Enterprise subscriptions.

Data flows

- A detailed description of all data flows can be found in our Cryptography Whitepaper, pp. 6–7.
- Data flows occur on three servers:
  - **Chat server:** forwards messages
  - **Media server:** temporary storage of files (images, files, videos, audio recordings) until delivery of message
  - **Directory server:** Directory of Threema IDs and public keys
- Connections to all servers are transport-encrypted, any content (chats, media) is end-to-end encrypted and not readable by the provider. The respective protocols, algorithms, and parameters are described in the Cryptography Whitepaper.

Personal data accessible by an administrator

Using Enterprise subscriptions, the following information is readable in the management cockpit:

- User name (login credentials, license) as set by the administrator (individual credentials) as well as the associated password. Global credentials enable a generic username for all users, so no personal data is accessible.
- Nickname, chosen by the user or set by the employer.
- Threema ID, app version, timestamp of the latest license check.

- If using «custom contacts»: List of included contacts, consisting of first name, surname, and Threema ID.
- This information can be accessed using an API.

Analytics made by the provider

- Assessment whether the amount of licenses is sufficient.
- No other reports or appraisals whatsoever are made that could be linked to a specific customer or person.
- No usage data is compiled.

Location of and access to collected data

- As a matter of principle, Threema does not store any metadata or log files whatsoever.
- End-to-end encrypted data created during the transmission of messages is immediately deleted on the server upon successful message delivery.
- Threema operates its own servers (no hosting, no cloud). Access to these servers is restricted to internal, authorized maintenance personnel only.

List of References and Further Reading

Cryptography Whitepaper
https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf

Threema Encryption Validation
https://threema.ch/validation

Threema Work Website
https://work.threema.ch

Terms of Service
https://work.threema.ch/en/terms-of-service

Security Review: Security Statement, Cnlab
https://threema.ch/press-files/2_documentation/external_audit_security_statement.pdf

Further information about the app and its security
https://threema.ch/faq