Threema.Work

Reference Sheet
Privacy & Security

This document summarizes how privacy and security form the very core of Threema Work.

VERSION: JULY 27, 2020

Privacy & Security

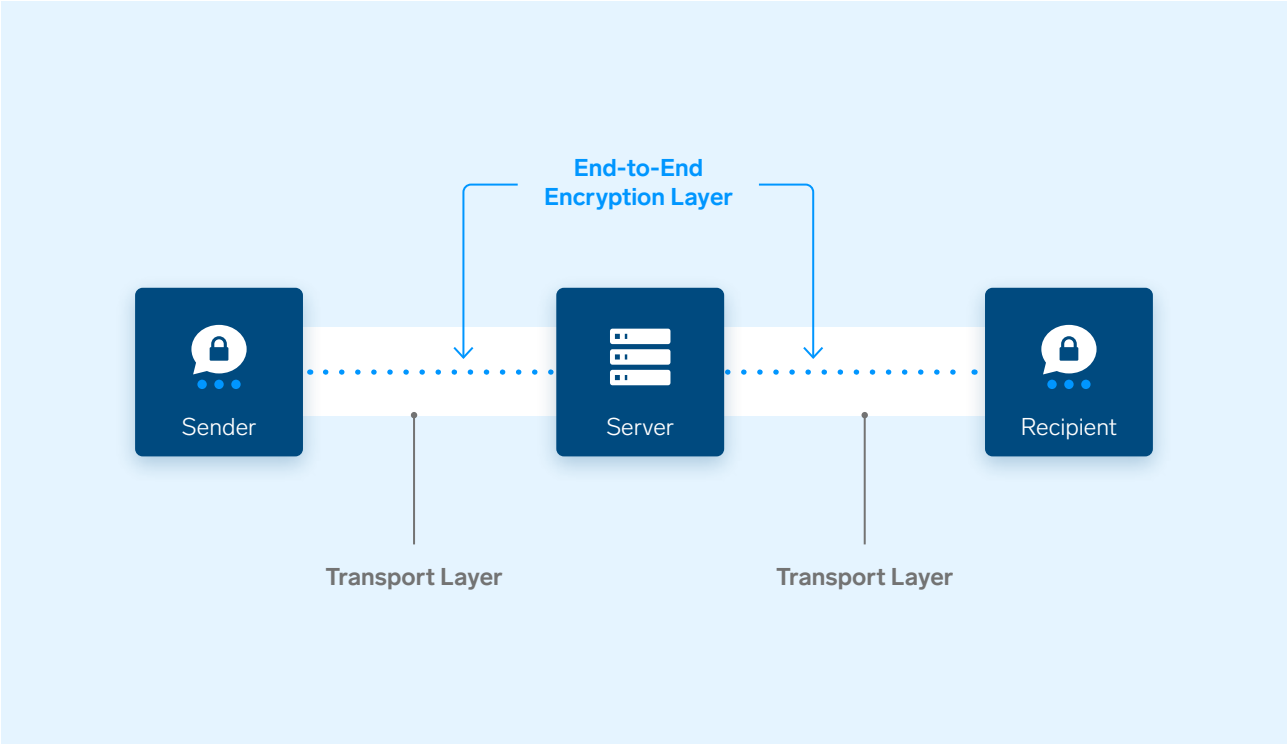
Threema Work and Threema are based on the same blueprint and share the same principle of avoiding metadata to the largest possible extent.

In contrast to conventional cloud services, messages and media files are transmitted without any storage. The aim is to provide the maximum of security with the 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.

Millions of private and business users worldwide use the Threema app, and it has been consistently proving its reliability, scalability, and security ever since its launch in 2012. The app's award-winning data protection and security measures as well as the general concept have been successfully audited multiple times.

Encryption & Key-Pair Management

Threema's state-of-the-art asymmetric cryptography protects both the messages between sender and recipient as well as the communication between app and server. Since the Threema apps are open source, they can be subjected to independent reviews 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's identity.

Users are identified by means of 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 the user device. Only the user has control over key exchanges. No third party – not even we as service provider – can decrypt the content of a message.

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

Physical Security

Threema GmbH runs its own servers in two physically separated, redundant data centers of an ISO 27001-certified colocation partner in the Zurich area.

These state-of-the-art data centers include biometric access control, full-height turnstiles, 24/7 security staff on site, video surveillance, emergency power systems, fire protection, fail-safe air-conditioning, and a fully redundant Internet connection. Encrypted offsite backups are maintained for disaster recovery purposes.

Data protection is our undisputed core competency.

Legal Compliance

Using Threema ought to generate as little data as possible on the server. That's Threema's basic concept and the reason why data protection is our undisputed core competency.

Threema Work is fully compliant with the European General Data Protection Regulation (GDPR), and transmitting data from the EU to Switzerland permitted by law without any additional evaluation (according to the adequacy decision of the European Commission 2000/518/EG, Swiss law guarantees a level of data protection equivalent to European legislation).

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).

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

Decentralized Architecture

Data such as contact lists or group chats is managed solely on user devices and not on Threema servers. The latter only 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. In Threema, all messages and media files are transmitted in end-to-end encrypted form. 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 completed, they are immediately and irrevocably deleted from the server.

Local creation of the key pair used for encryption: Your private key remains unknown to us. Therefore, it's impossible for us to decrypt messages.

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 information about when and why data is generated who has access to it, and 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: FCM; iOS: APNS).
- 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 in hashed form to the server, where they are matched against encrypted links. Once the process is completed, the hashes are immediately removed from memory.

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 us, the service provider. The respective protocols, algorithms, and parameters are described in the Cryptography Whitepaper.

Personal Data Accessible by an Administrator

When using an Enterprise subscription, the following information is contained in the management cockpit:

- User name (login credentials, license) as set by the administrator (individual credentials) as well as the associated password. Global credentials result in a single (generic)username for all users, which means that no personal data is involved.
- Nickname chosen by the user or set by the administrator.
- Threema ID, app version, time stamp of the latest license check.
- If using the option “custom contacts” in the management cockpit: List of included contacts, consisting of first name, surname, and Threema ID.
- This information can be accessed using an API.

Analytics Created by the Service Provider

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

Location of, and Access to, Collected Data

- As a matter of principle, Threema does not store any metadata or create any 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

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

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

Open Source Informationen
https://threema.ch/open-source

Security Audit Report 2020 (Cure53)
https://threema.ch/press-files/2_documentation/security_audit_report_threema_2020.pdf

Security Audit Report 2019 (Lab for IT Security of the Münster University of Applied Sciences)
https://threema.ch/press-files/2_documentation/security_audit_report_threema_2019.pdf

Privacy Policy
https://threema.ch/privacy_policy/index.php?lang=en&version=1k (app)
https://work.threema.ch/en/privacy-policy (Website)

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

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