THREEMA

MERKBLATT
SICHERHEIT UND DATENSCHUTZ

Dieses Dokument erklärt zusammenfassend, wie Sicherheit und Datenschutz das Fundament der Threema-Apps bilden.

VERSION: 24. APRIL 2025

SICHERHEIT UND DATENSCHUTZ

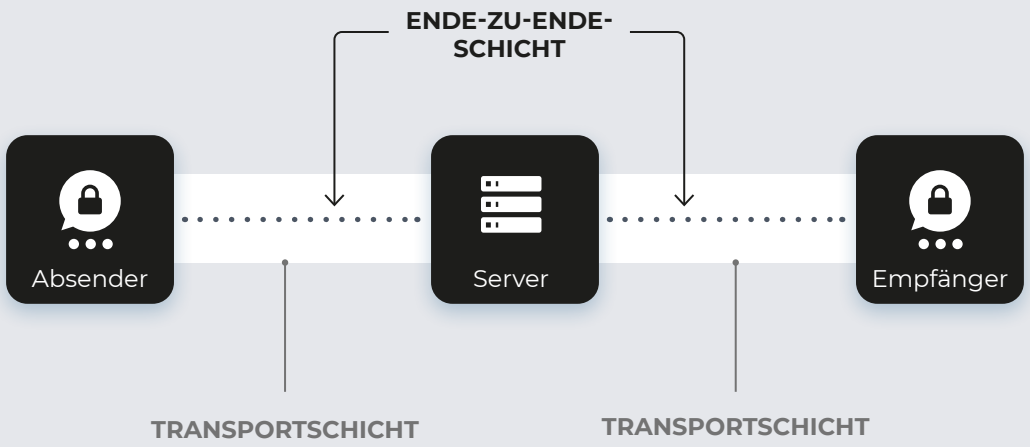
Threema Work und Threema Private basieren auf derselben Architektur und teilen dasselbe Prinzip der grösstmöglichen Vermeidung von Metadaten.

Im Gegensatz zu klassischen Cloud-Diensten findet bei der Übermittlung von Nachrichten und Medien grundsätzlich keine Speicherung statt, mit dem Ziel, ein Maximum an Sicherheit bei einem Minimum an Metadaten zu ermöglichen. Nachrichten sind transient und werden nach erfolgreicher Zustellung umgehend vom Server gelöscht. Die App kann vollständig ohne Handynummer oder E-Mail-Adresse verwendet werden und ist damit auch für den Einsatz auf Tablets geeignet.

Die Instant Messenger der Threema GmbH sind von Millionen privater und geschäftlicher Nutzer eingesetzte Mobilapplikationen, die seit 2012 weltweit im Einsatz sind und ihre Zuverlässigkeit, Skalierbarkeit und Sicherheit fortlaufend unter Beweis stellen. Datenschutz, Sicherheit und das Gesamtkonzept der App wurden mehrfach erfolgreich auditiert, verifiziert und prämiert.

VERSCHLÜSSELUNG UND SCHLÜSSELMANAGEMENT

Die Threema-Apps verwenden modernste asymmetrische Kryptografie, um Nachrichten zwischen Sender und Empfänger sowie zusätzlich die Kommunikation zwischen der App und dem Server zu verschlüsseln. Da Threemas Mobilapps quelloffen sind, lässt sich ihre Sicherheit jederzeit unabhängig überprüfen.



Es werden zwei Verschlüsselungsschichten verwendet: eine Ende-zu-Ende-Schicht zwischen Gesprächsteilnehmern und eine zusätzliche Schicht, die vor dem Abhören der Verbindung zwischen App und Server schützt. Damit wird verhindert, dass ein Angreifer, der Netzwerkpakete aufzeichnet (z.B. in einem öffentlichen drahtlosen Netzwerk), die Identität eines Nutzers herausfinden kann.

Nutzer werden mit der sog. Threema-ID identifiziert. Diese besteht aus einer zufällig erzeugten, achtstelligen Abfolge von Buchstaben und Ziffern und ist untrennbar mit dem Schlüsselpaar verbunden, welches zur Verschlüsselung verwendet wird. Das Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel, wobei der private Schlüssel auf dem Gerät verbleibt und der öffentliche Schlüssel an den Server gesendet wird.

Die gesamte Ver- und Entschlüsselung der Nachrichten erfolgt ausschliesslich direkt auf dem Endgerät. Die Kontrolle über den Schlüsselaustausch liegt beim Benutzer. Keine Drittpartei – nicht einmal der Serverbetreiber – kann den Inhalt der Nachrichten entschlüsseln.

Unser umfangreiches Cryptography Whitepaper erläutert sämtliche Konzepte und Algorithmen in Zusammenhang mit der Verschlüsselung und Datenübertragung.

PHYSISCHE SICHERHEIT

Die Threema GmbH betreibt ihre eigenen Server in zwei räumlich getrennten, redundanten Rechenzentren eines «ISO 27001»-zertifizierten Colocation-Partners im Grossraum Zürich.

Die Rechenzentren entsprechen dem neuesten Stand der Technik und sind mit biometrischer Zutrittskontrolle, Personenvereinzelungsanlage, 24/7-Sicherheitspersonal vor Ort, Videoüberwachung, Notstromsystemen, Brandschutzeinrichtungen, ausfallsicherer Klimatisierung und vollständig redundanter Internetanbindung ausgerüstet. Verschlüsselte Offsite-Backups werden zwecks Disaster-Recovery erstellt.

Datenschutz ist unsere unbestrittene Kernkompetenz.

RECHTSKONFORMITÄT IM DATEN- UND GEHEIMNISSCHUTZ

Bei der Nutzung der Threema-Apps sollen so wenige Daten wie möglich auf Servern anfallen. Das gehört zum Grundkonzept von Threema Private und Threema Work, weshalb Datenschutz unsere unbestrittene Kernkompetenz ist.

Die Threema-Apps sind sowohl mit der Europäischen Datenschutz-Grundverordnung (DSGVO) als auch mit dem Schweizerischen Bundesgesetz über den Datenschutz (DSG) konform. Als Fernmeldedienst im Sinne des Schweizerischen Fernmeldegesetzes (FMG) unterliegen die Daten der Nutzer der Threema-Apps dem strafbewehrten Fernmeldegeheimnis.

Datenübermittlungen zwischen der EU und der Schweiz sind ohne Überprüfung rechtlich zulässig, da gemäss Angemessenheitsbeschluss der Europäischen Kommission COM/2024/7 vom 15. Januar 2024 das Datenschutzniveau der Schweiz den strengen Standards des europäischen Datenschutzrechts genügt.

Details zur Bearbeitung von Personendaten im Rahmen der Nutzung von Threema Work können unserem Auftragsbearbeitungsvertrag (AVV) entnommen werden. Über einen optionalen zusätzlichen Anhang zum AVV können der Threema GmbH zusätzliche Pflichten zum Schutz von Daten in Zusammenhang mit Amts- oder Berufsgeheimnissen, z.B. von Ärzten oder Rechtsanwälten, auferlegt werden.

DEZENTRALE ARCHITEKTUR

Daten wie z.B. Kontaktlisten oder Gruppenchats werden auf den Geräten der Nutzer verwaltet und nicht auf den Threema-Servern. Letztere fungieren lediglich als Relaisstation; Nachrichten und Daten werden weitergeleitet, aber nicht dauerhaft gespeichert. Das garantiert grösstmögliche Datensicherheit.

Sofortige Löschung von Nachrichten nach erfolgreicher Übermittlung

Alle Nachrichten und Medien werden bei Threema Ende-zu-Ende-verschlüsselt übermittelt. Selbst wenn jemand eine Nachricht abfangen könnte, wäre sie völlig unbrauchbar, da sie nur der vorgesehene Empfänger entschlüsseln und lesen kann.

Keine Speicherung von Kontaktlisten

Die E-Mail-Adressen und Telefonnummern des lokalen Adressbuchs werden zum Abgleich anonymisiert (gehasht) an Threemas Server übermittelt. Nach dem Abgleich werden die Hashes umgehend vom Server gelöscht.

Lokale Generierung des zur Verschlüsselung verwendeten Schlüsselpaars

Die privaten Schlüssel bleiben uns als Betreiber unbekannt, die Entschlüsselung von Nachrichten ist ausgeschlossen.

Keine personenbezogenen Auswertungen

Es werden keine Logs erstellt, welche Threema-ID mit welcher Threema-ID kommuniziert.

QUELLENVERZEICHNIS UND WEITERFÜHRENDE VERWEISE

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

Cryptography Whitepaper
https://threema.com/assets/documents/cryptography_whitepaper.pdf

Informationen zu Open Source
https://threema.com/de/why-threema/open-source

Sicherheitsprüfungen
https://threema.com/de/faq/code_audit

Auftragsbearbeitungsvertrag (AVV)
https://threema.com/de/dpa

Nutzungsbedingungen (Softwarelizenzvertrag)
https://work.threema.ch/de/terms-of-service

Weitere Sicherheits- und App-spezifische Hinweise
https://threema.com/de/support