Merkblatt

Sicherheit und Datenschutz

Dieses Dokument fasst zusammen, auf welche Weise Sicherheit und Datenschutz das Fundament von Threema Work bilden und wie sie angewendet werden.

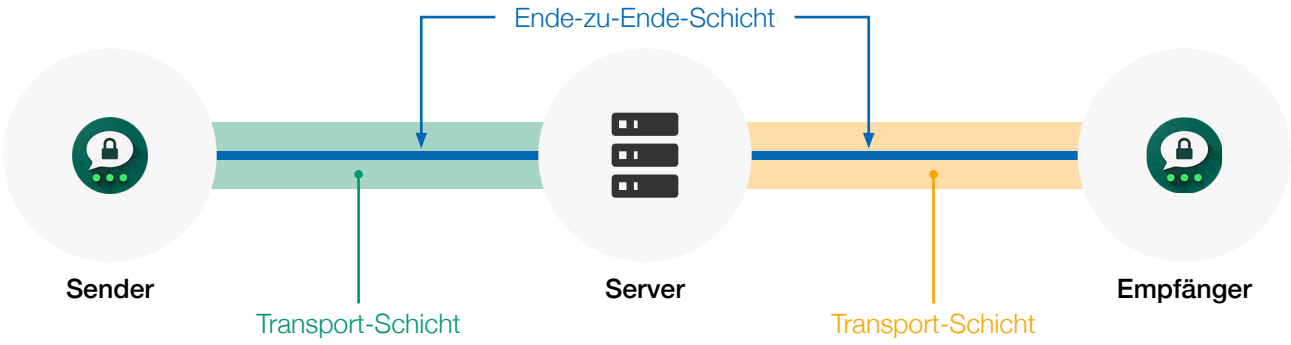
1. Allgemein

Threema Work und Threema basieren auf derselben Architektur und teilen das gleiche Prinzip der Vermeidung von Metadaten durch grösstmögliche Dezentralisierung. 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 Handy-Nummer oder E-Mail-Adresse verwendet werden und ist damit auch für den Einsatz auf Tablets geeignet.

Threema ist eine von Millionen privater und geschäftlicher Nutzer eingesetzte Mobilappliaktion, die seit 2012 weltweit im Einsatz ist und ihre Zuverlässigkeit, Skalierbarkeit und Sicherheit fortlaufend unter Beweis stellt. **Datenschutz, Sicherheit und das Gesamtkonzept wurden mehrfach erfolgreich auditiert, verifiziert und prämiert.**

2. Verschlüsselung und Schlüsselmanagement

Threema verwendet modernste asymmetrische Kryptografie, um Nachrichten zwischen Sender und Empfänger, sowie zusätzlich die Kommunikation zwischen der App und den Servern zu verschlüsseln. Das Verschlüsselungsprotokoll von Threema steht mit der Nutzung der Open Source Bibliothek NaCl unabhängigen Überprüfungen offen. Die korrekte Anwendung der Verschlüsselung kann jederzeit verifiziert werden.



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 Verschlüsselung und Entschlüsselung der Nachrichten geschieht 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.

3. Physische Sicherheit

Die Threema GmbH betreibt ihre eigenen Server in einem hochsicheren Rechenzentrum eines ISO 27001 zertifizierten Colocation-Partners in Zürich. Das Datacenter entspricht dem neuesten Stand der Technik und ist mit biometrischer Zutrittskontrolle, Personenvereinzelungsanlage, Videoüberwachung, Notstromsystemen, Brandschutzeinrichtungen, ausfallsicherer Klimatisierung und vollständig redundanter Internetanbindung ausgelegt.

Daneben verfügt die Threema GmbH über einen zweiten Hosting-Standort für die Abwehr von DDoS-Attacken und die Überbrückung von Netzwerk-Ausfällen. Dieser Standort ist örtlich getrennt und entspricht bezüglich Sicherheit weitestgehend den Merkmalen des Hauptstandorts.

4. Datenschutzgesetze

Bei der Nutzung von Threema sollen so wenig Daten wie möglich auf den Servern anfallen. Das gehört zum Grundkonzept von Threema, weshalb **Datenschutz unsere unbestrittene Kernkompetenz** ist. Threema ist vollständig konform mit der heutigen Schweizer- und EU-Datenschutzgesetzgebung, und strebt **volle Kompatibilität mit der im Mai 2018 in Kraft tretenden EU-DSGVO** an.

Details zur Datenhandhabung bei Threema sind im Anhang erläutert.

5. Dezentrale Architektur

Daten wie z.B. Kontaktlisten oder Gruppen-Chats werden auf den Geräten der Nutzer verwaltet und nicht auf den Threema-Servern. Diese funktionieren lediglich als Relaisstation; Nachrichten und Daten werden weitergeleitet, aber nicht dauerhaft gespeichert. Dies 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 nur der vorgesehene Empfänger diese entschlüsseln und lesen kann.
- **Keine Speicherung von Kontaktlisten:** Die E-Mail-Adressen und Telefonnummern des lokalen Adressbuchs werden zum Abgleich anonymisiert (gehasht) an unsere Server übermittelt. Nach dem Abgleich werden die Hashes umgehend wieder von den Servern gelöscht.
- **Lokale Generierung des zur Verschlüsselung verwendeten Schlüsselpaars** auf den Nutzergeräten: Die privaten Schlüssel bleiben uns als Betreiber unbekannt, die Entschlüsselung von Nachrichten ist ausgeschlossen.
- **Keine personenbezogenen Auswertungen**, keine Logs, welche Threema-ID mit welcher Threema-ID kommuniziert, keine Weitergabe von Daten, keine Untervertragsverhältnisse.

Anhang: Details zur Datenhandhabung

Der folgende Fragenkatalog enthält Angaben darüber, wann welche Daten bei der Nutzung von Threema Work generiert werden und wer in welchem Umfang darauf Zugriff haben kann.

Welche Daten werden bei der Anmeldung generiert?

- Schlüsselpaar (lokal generiert). Öffentlicher Schlüssel wird an den Server gesendet, privater Schlüssel verbleibt auf dem Gerät.
- achtstellige Threema-ID (durch den Server generiert).
- Datum (ohne Uhrzeit), an dem die Threema-ID generiert wurde.
- Push-Token, um Benachrichtigungen erhalten zu können (Android: GCM; iOS: APNS; Windows Phone: MPNS/WNS).
- Optional
    - Falls eine Verknüpfung von Rufnummer und/oder E-Mail gewünscht wird, werden diese Angaben an den Server übermittelt. Die E-Mail-Adresse wird in einwegverschlüsselter Form gespeichert.
    - Falls eine Synchronisation mit dem Adressbuch gewünscht wird, werden Rufnummern und E-Mail-Adressen in einwegverschlüsselter Form an den Server übermittelt, dort mit den verschlüsselten Angaben aus Verknüpfungen verglichen und umgehend aus dem Arbeitsspeicher entfernt. Es findet keine Speicherung statt.
    - Verknüpfung der Threema-ID mit einer E-Mail-Adresse und/oder Rufnummer und Adressbuch-Synchronisation sind optional. Alternativ oder als Ergänzung können mit dem Enterprise-Preisplan Kontaktlisten über das Management-Cockpit vorbelegt werden.

Wie fliessen die Daten?

- Eine ausführliche Beschreibung sämtlicher Datenflüsse finden Sie in unserem Cryptography Whitepaper auf Seite 6 und 7.
- Datenflüsse finden zu drei Servern statt:
    - **Chatserver:** Weiterleitung von Nachrichten
    - **Medienserver:** Zwischenspeichern von Medien (Bildern, Videos, Dateien, Sprachnachrichten) bis zur Ablieferung
    - **Verzeichnisserver:** Verzeichnis von Threema-IDs und öffentlichen Schlüsseln
- Die Verbindung zu allen Servern ist transportverschlüsselt, alle Inhalte (Chats, Medien) sind Ende-zu-Ende-verschlüsselt und für den Betreiber nicht lesbar. Die verwendeten Verfahren, Algorithmen und Parameter finden Sie im Cryptography Whitepaper erläutert.

Welche personenbezogenen Daten können durch die Administrationsebene ausgewertet werden?

Beim Enterprise-Preisplan sind folgende Angaben im Management Cockpit einsehbar:

- Durch den Administrator gewählter Benutzername (Zugangsdaten, Lizenz), falls individuelle Zugangsdaten gewählt, sowie dazugehörige Passwörter. Bei globalen Zugangsdaten handelt es sich um einen generischen Nutzernamen, der für alle Nutzer identisch ist, und damit nicht um personenbezogene Daten.
- Durch den Arbeitgeber vorgegebener oder (falls zugelassen) durch den Nutzer gewählter Nickname.
- Threema-ID, App-Version, Datum und Zeit des letzten Lizenz-Checks.
- Bei Nutzung der Option «Interne Kontakte kennzeichnen»: Liste der vorbelegten Kontakte, bestehend aus Vorname, Nachname und Threema-ID.
- Diese Informationen sind, falls gewünscht, auch über eine API verfügbar.

Welche Auswertungen werden vom Anbieter vorgenommen?

- Prüfung, ob Anzahl der Lizenzen ausreicht.
- Es werden keinerlei andere Auswertungen vorgenommen, die einem Kunden oder einer Person zugeordnet werden könnten.
- Es werden keine Nutzungsdaten/Analytics erfasst.

Wo liegen erhobene Daten und wer hat Zugriff?

- Threema bewahrt prinzipiell keine Metadaten oder Logdateien auf.
- Die Ende-zu-Ende-verschlüsselten temporären Daten, die bei der Übertragung von Nachrichten entstehen, werden nach Ablieferung der Nachricht umgehend gelöscht.
- Threema betreibt eigene Server (kein Hosting, keine Cloud). Der Zugriff auf diese Server beschränkt sich auf das dafür autorisierte firmeneigene Wartungspersonal.

Quellenverzeichnis und weiterführende Verweise

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

Nutzungsvereinbarungen
https://work.threema.ch/de/nutzungsbedingungen

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

Weitere Sicherheits- und App-spezifische Hinweise
https://threema.ch/faq