General information

What is GlobE Threema?
GlobE Threema is utilized to describe the interim solution for the secure exchange of information under the GlobE Network, i.e. the use of the Threema Work application. The GlobE Network offers this application to its members free-of-charge. Threema Work is an application for direct secure communication. It works like any other secure messaging application, but with an emphasis on end-to-end encrypted security and professional use.

Why did the GlobE Network implement a secure communication solution?
The GlobE Network aims to provide a platform for peer-to-peer information exchange and informal cooperation to better identify, investigate and prosecute cross-border corruption offences and recover stolen assets. It implemented GlobE Threema as an interim secure communication solution to facilitate timely and efficient communication between all GlobE practitioners, with a view to promoting informal cooperation in the investigation and prosecution of transnational corruption cases.

Who has access to GlobE Threema?
Access to GlobE Threema is granted to designated representatives of the GlobE Network members. Each potential user is verified by the GlobE secretariat before an account is set up.

Who can see the content of my messages on GlobE Threema?
You and the recipient of your message when they open it. Your message is end-to-end encrypted.

What types of information can be shared over GlobE Threema?
In the first contact, practitioners are encouraged to indicate any specific parameters for information they can share via Threema. Consistent with the objectives of the Network and subject to domestic legal systems, practitioners could decide to share the following information over GlobE Threema:
• Information obtained via informal cooperation, e.g. information gathered via non-coercive measures or information that is publicly available.

• Information supporting formal mutual legal assistance (MLA), e.g. to identify and establish direct contact with the central authorities of the requested States, to identify legal basis for MLA or the procedural rules including evidential requirements of MLA, to prepare the requested State in advance and expedite the execution of MLA requests, to request for emergency provisional measures, with the promise of a formal MLA request soon.

• Information to facilitate parallel and/or joint investigations.

What are the benefits of using GlobE Threema for direct communication?

GlobE Threema provides practitioners with a secure messaging application with an array of benefits:

• GlobE Threema provides a free and common platform for direct communication, which envisages zero-knowledge security, efficient employee communication, powerful user management, and comprehensive security parameters.

• GlobE Threema enables users to initiate individual secure chat, and voice or video calls, and to share documents, images, and videos securely. The end-to-end encryption of the application provides the highest level of security for practitioners to exchange information, including case-specific intelligence. Users can decide whether, how and when to use it.

• GlobE Threema is the tailored version of Threema Work exclusively for GlobE practitioners. The GlobE Network secretariat maintains a directory of contacts and verifies the identity of users before issuing credentials, ensuring additional security.

What data can be accessed by the GlobE Network secretariat?

The GlobE Network secretariat only has access to consolidated and anonymized generic statistics e.g., the number of active GlobE Threema users across Android and iOS devices between a certain time period. No personal usage data or messages, nor your lists of groups or contacts, can be seen by the secretariat.
Safety and security

Why is the Threema Work application secure?

- Threema Work uses state-of-the-art asymmetrical cryptography to encrypt both the communication between users as well as the data transfer between the Threema application and Threema servers. Threema Work not only end-to-end encrypts text and voice messages but also voice and video calls, media files, and status messages.
- There is no central storage of personal data on the Threema servers. Where there is no data saved, there is nothing to be accessed or misused.
- Threema Work runs its own servers (i.e. company-owned hardware) in data centres of an ISO 27001-certified collocation partner in Switzerland.
- There is no requirement for a user to share any personal data, not even a phone number or an email address, to use Threema Work.
- The application has centralized access management functionality available to the GlobE Network secretariat, therefore, users can be verified before getting credentials.

Security and Privacy by Design

Threema Work was designed from scratch with focus on security and data protection. In contrast to many other business messengers, all types of communication are end-to-end encrypted in Threema Work. It’s not required to provide personal information, such as a phone number or email address, to use this application.

What does end-to-end encryption mean?

End-to-end encryption (E2EE) is a method of secure communication that prevents third parties from accessing data while it is transferred from one end system or device to another. In E2EE, the data is encrypted on the sender’s device, and only the intended recipient can decrypt it. As the message travels to its destination, it cannot be read or altered by the internet service provider, application service provider (Threema in this case), hackers or any other entity or service. Only the sender and the intended recipient can read a given message.
Can the application service provider (Threema) see the data of the GlobE Threema users kept on its servers?

Using Threema Work generates as little data on its servers as possible. The Threema servers assume the role of a “switch”; messages and data are forwarded, but not permanently stored. The following clarifies what data is kept on the Threema servers and for how long.

- Messages and group chats: As soon as a message has been successfully delivered to the recipient, it is immediately deleted from the Threema server. For the brief period a message in transit resides on Threema server, it continues to be encrypted and cannot be decrypted even by Threema.
- Key pairs for encryption and decryption of messages are generated on your device. Threema will never know your private key, and thus cannot decrypt any message contents.
- No contact lists are stored when synchronizing contacts: Contact synchronisation is completely optional, and the user needs to explicitly enable it. The email addresses and phone numbers from your address book are anonymized (hashed) before they reach the server. Once the comparison is finished, they are immediately deleted from the server.
- Threema does not log who is communicating with whom.

All encryption and decryption happen directly on the user devices. No third party – not even the application service provider (Threema) – can decrypt the content of the messages, calls and media files. Threema is also GDPR compliant.

---

**European Union General Data Protection Regulation (GDPR)**

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It is considered as one of the toughest privacy and security laws in the world.

---

**Security threats are constantly evolving. How does Threema Work stay secure?**

Threema Work provides rock-solid encryption, and unparalleled privacy protection. All its source code is publicly available for IT specialists across the globe to review. External experts are commissioned to conduct comprehensive security audits on a regular basis. The most recent audit was carried out by Cure53, a leading cyber security firm, in October 2020.
Access and functionality

How do I register to use GlobE Threema?

Please use the GlobE Threema step-by-step-guide to register. Kindly contact the GlobE Network secretariat through globenetworkscp@un.org for further technical support.

What types of permissions might Threema Work require?

The following are some of the permissions that may be required by the Threema Work application depending on what your personal usage will be:

- Camera - Required for Threema video calls; also used for contact verification via QR code;
- Microphone - Required for Threema calls and voice messages;
- Location - Required only if the user wishes to share their location with other users;
- Device storage - Required for reading and storing media files (images, videos, documents);
- Manage phone calls - Required to reject incoming phone calls while a Threema call is ongoing.

What additional security features does Threema Work contain?

You can set access control on the Threema Work application based on PIN, biometric or system screen lock to prevent any unauthorised access. Additionally, you can mark certain chats as “private chats” and protect them with a PIN and temporarily hide them from your message list. This way, confidential chats are protected from prying eyes. Push notifications for new messages in a private chat contain neither a message preview nor the name of the sender.