

# MobiVisor-Messenger

## INTRODUCTION

MobiVisor-Messenger is a secure and encrypted messenger application that eliminates the need for WhatsApp in the workspace. The app provides all the basic features of a messenger and beyond, with all network communications in the Messenger running over a secure infrastructure encrypted with SSL/TLS. In addition, all application data is stored in encrypted local storage areas.

## FEATURES

Naturally, users can send each other messages in a secure and encrypted way. This can be done 1:1, but groups can also be created within the application and thus mass messages can be sent.

Through the messaging application, users can send files (images, documents, audio files, etc.) in encrypted form. Messages are encrypted in the application using the 256-bit AES/CBC algorithm using 256-bit (elliptic curve) public-private keys.

## ADMINISTRATION

*Admin portal* – All users of the Messenger can be managed centrally via an online portal. The administrator can lock, unlock and invite users and view user activity. Via the device network, the administrator can send notifications (e.g. in the form of push messages) to all devices registered in the system.

*Activity protocols* - MobiVisor-Messenger offers professional revision protocols. These logs record a chronological log of all activities relevant to security, privacy, compliance and administration.

*Whitelisting of users* - Selected users, teams and business areas can be activated for MobiVisor Messenger. This allows the company-wide use of the Messenger to be controlled and ensures that only authorized employees have access to the app.

*Pooling of users* - Employees can be assigned to certain closed areas via the administration portal (e.g. marketing, accounting, sales, etc.). This allows IOTIQ to restrict the exchange of confidential content and prevent data leakage.

*Filter and bulk operations* - As the number of users rises, the effort required by administrators increases, because activities often have to be performed several times. MobiVisor-Messenger has filters and bulk operations to simplify user management.

## **MOBILE APPLICATION MANAGEMENT**

*EMM-Integration* - MobiVisor-Messenger is available as a stand-alone application that can also be fully integrated into our Enterprise Mobility Management solution. The Messenger app can be easily configured company-wide and ensures the implementation of internal security policies for mobile devices.

*Automated installation*- The entire registration and rollout process is fully automated without the need for user actions or support efforts.

*User management* - If a new employee is hired or an old employee leaves the company, access can easily be granted or blocked by the administrator.

*Data archives* - The data of the users of a company can be archived via the admin portal. The user chats are stored in the device database. Archiving can be done for specific periods and user groups. The archive is only accessible to authorized persons.

*Limitations* - Certain rules can be set for all users to prevent the distribution of messages via copy & paste or the sending of other content (such as pictures, videos, files, etc.). The restrictions can be set individually for users and groups via the admin portal. MobiVisor-Messenger was developed exclusively for internal company communication.

*Data loss prevention* - If an employee loses his or her terminal device or it is stolen, sensitive data can become public. In such scenarios, all data and content on MobiVisor Messenger can therefore be deleted remotely.

## **INFRASTRUCTURE**

*Private Cloud or On-Premise* - MobiVisor Messenger is the right solution regardless of the IT infrastructure. MobiVisor Messenger can be hosted in our German cloud, on-premise

or in a private cloud. The range of functions is not affected by the type of hosting. On-premise installations use the storage space provided on the servers.

*Security guidelines* – MobiVisor Messenger applies our strict corporate security policies to prevent unauthorized access to infrastructure, systems and data centers.

*Scale* – MobiVisor Messenger ensures the highest scalability and reliability for companies of all sizes. This makes the Messenger suitable for both small businesses and large companies.

## **DATA PROTECTION**

*Data protection rights* – MobiVisor Messenger is a product of IOTIQ GmbH with headquarters in Leipzig. All data and contents are stored exclusively on German servers. Thus, the German and European data protection law (incl. GDPR) is fulfilled.

*Data minimisation* – As little data as possible is used to operate the Messenger. Personal data is only accessed if absolutely necessary for security or administration reasons.

*Integration* – All interfaces and APIs to third-party providers have been developed in the MobiVisor Messenger itself. This prevents uncontrolled data outflows.

## **COMPLIANCE**

MobiVisor-Messenger is a data protection-compliant messenger for companies and authorities. The data traffic is anonymous without telephone numbers and without telephone book data. The data processing is carried out in accordance with GDPR, whereby the protection of personal data is of particular importance. Transparency is important for requests for information. We therefore provide all information on the use of personal data as quickly as possible. In addition, companies have the possibility to configure organization-wide guidelines for the access and exchange of data with the Messenger. In contrast to conventional messengers, you can therefore be sure that you comply with data protection regulations when using MobiVisor Messenger.

The following regulations and laws are fulfilled by MobiVisor-Messenger:

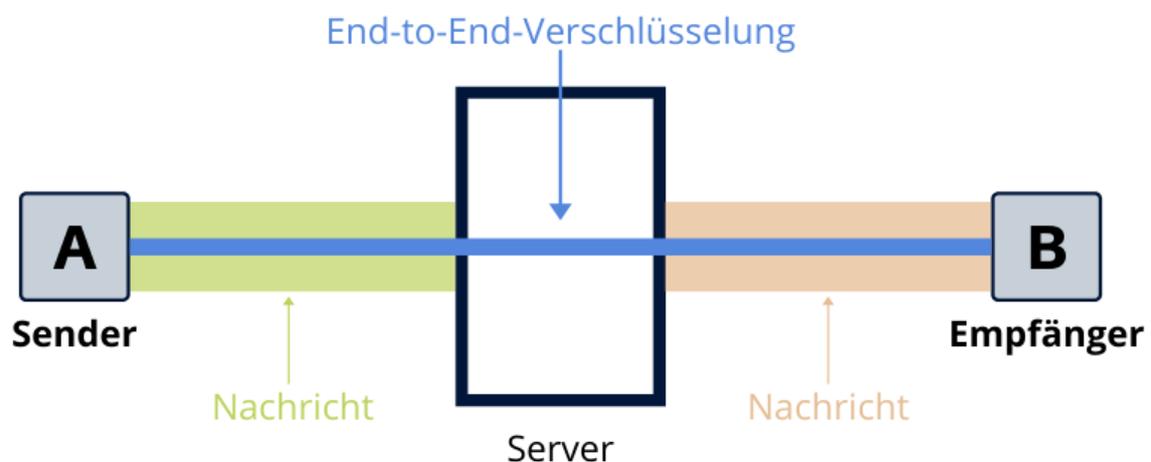
- Europäische Datenschutz-Grundverordnung (EU-DSGVO/GDPR)
  - Protection of personal data
- Bundesdatenschutzgesetz (BDSG)
  - Handling of personal data
- Telekommunikationsgesetz (TKG):
  - Preventing the interception of messages
- Telemediengesetz (TMG):
  - Data protection during operation and the release of data

More information on data protection is provided in our transparent data protection declaration. It provides detailed information about the type, purpose and scope of processing of personal data.

## TECHNICAL DATA

All connections are established in the MobiVisor Messenger via TLS. TLS certificates and settings have the latest security options. MobiVisor-Messenger receives the highest rating of A+ in Qualys SSL Labs test (SSL Server Test). The messages use end-to-end encryption. When using push messaging services (Firebase Cloud Messaging, Apple Push Services), no content is sent, only a notification notice. This prevents data loss (even if encrypted) to third parties.

*end-to-end encryption*



**256-bit** public-private Keys are generated (equals **3072 bit RSA**).

$$AB_{shared} = createSharedSecret_{Curve25519}(A_{private}, B_{public}) // 256 bit$$

$$AB_{shared\_expandet} = HBKDF(AB_{shared}) // 512 \text{ bit}$$

$$KEY_{encrypt} = AB_{shared\_expandet}[0 - 255] // \text{Encryption Key}$$

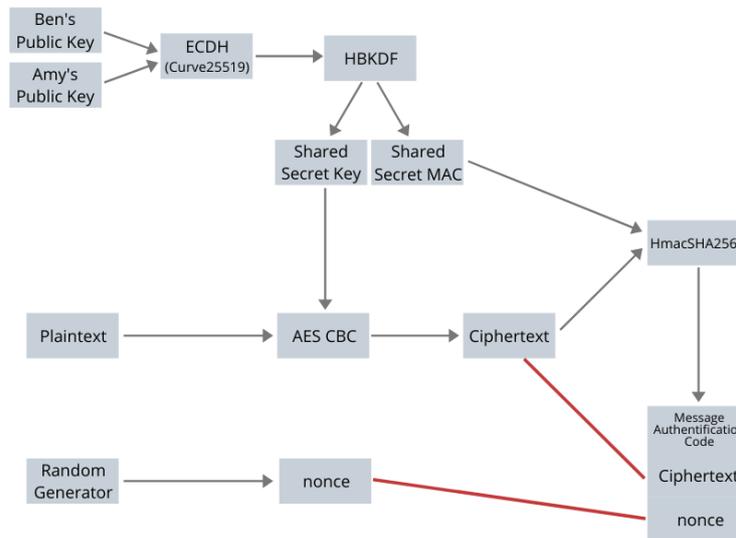
$$KEY_{mac} = AB_{shared\_expandet}[256 - 511] // \text{Integrity Check}$$

Encryption:

$$encryptedContent = AES_{CBC_{key}}(Plaintext) // \text{AES256 Block Encryption}$$

$$Mac = HmacSHA256(encryptedContent) // \text{Integrity Check}$$

$$Message = \{ \dots encrypted \text{ Content} \mid mac \dots \}$$



### Local hard drive encryption

The messages are not stored in full text. They are encrypted and can be retrieved with a PIN created by the user.

key: randomly generated (256-bit)

PIN: user defined

pin\_key= Scrypt(PIN)

encrypted\_key=encrypt<sub>pin\_key</sub>(key)

Messages are encrypted with key, encrypted\_key is stored on the hard disk. A PIN is required to open the messages with key.

Encrypt function: 256-bit AES/CBC

## **WHY WHATSAPP JUST ISN'T ENOUGH**

WhatsApp messages are backed up in the user's cloud (if the user accepts). What are the server locations? WhatsApp is owned by Facebook. Therefore the servers are also owned by Facebook. WhatsApp is designed for end users. Future features may violate company policies. The same applies to WhatsApp Business.