MobiVisor Messaging

Introduction

MobiVisor Messaging is a secure and encrypted messenger application that makes WhatsApp superfluous in the workplace. The app offers all the basic functions of a messenger and beyond, with all network communication in the messenger being handled via a secure infrastructure that is encrypted with SSL/TLS. In addition, all application data is stored in encrypted local storage areas.

Features

It goes without saying that users can send messages to each other in a secure and encrypted manner. This can be done 1:1, but groups can also be created within the application and thus mass messages can be sent.

Users can send files (images, documents, audio files, etc.) in encrypted form via the messaging application. The messages are encrypted in the application with the 256-bit AES/CBC algorithm using 256-bit (elliptic curve) public-private keys.

Administration

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

MOBIVISOR

MobiVisor Messaging

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

Filters and bulk operations - As the number of users increases, so does the workload for administrators, as activities often have to be carried out multiple times. MobiVisor Messenger has filters and bulk operations to simplify user management.

Features

EMM integration - MobiVisor Messaging 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 setup - The entire registration and rollout process is fully automated, with no user action or support required.

User management - If new employees are hired or existing employees leave the company, access can easily be granted or blocked by the administrator.

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

MobiVisor Messaging

Restrictions - Certain rules can be set for all users that prevent the distribution of messages via copy & paste or the sending of other content (such as images, 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 employees lose their devices or they are stolen, sensitive data can be leaked. Therefore, in such scenarios, all data and content of MobiVisor Messaging can be deleted remotely.

Infrastructure

Private cloud or on-premise - MobiVisor Messaging is the right solution regardless of which IT infrastructure is in place. 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.

Security policies - MobiVisor Messaging applies our strict company-wide security policies to prevent unauthorized access to infrastructure, systems and data centers.

Scalability - MobiVisor Messaging ensures maximum scalability and reliability for companies of all sizes. The messenger is therefore suitable for both small and very large companies.

MobiVisor Messaging

Data security

Data protection law - MobiVisor Messaging is the product of IOTIQ GmbH, headquartered in Leipzig. All data and content is stored exclusively on German servers. This complies with German and European data protection law (incl. GDPR).

Data avoidance - As little data as possible is used to operate the messenger. Personal data is only accessed if absolutely necessary for security or administrative reasons.

Integration and connection - All interfaces and APIs to third-party providers have been developed in MobiVisor Messaging itself. This prevents uncontrolled data outflows.

Compliance

MobiVisor Messaging is a data protection-compliant messenger for companies and public authorities. Data traffic is anonymous without telephone numbers and without telephone book data. Data processing is carried out in accordance with the GDPR, whereby the protection of personal data is of particular importance. Transparency is important when requesting information. We therefore provide all information about the use of personal data as quickly as possible. In addition, companies have the option of configuring organization-wide policies for accessing and sharing data with Messenger. In contrast to conventional messengers, you can therefore be sure that you are complying with data protection regulations when using MobiVisor Messaging.

MOBIVISOR

MobiVisor Messaging

MobiVisor Messaging complies with the following regulations and laws:

- European General Data Protection Regulation (EU GDPR)
  - Protection of personal data
- Federal Data Protection Act (BDSG)
  - Handling of personal data
- Telecommunications Act (TKG)
  - Prevention of interception of messages
- Telemedia Act (TMG)
  - Data protection during operation and the release of data

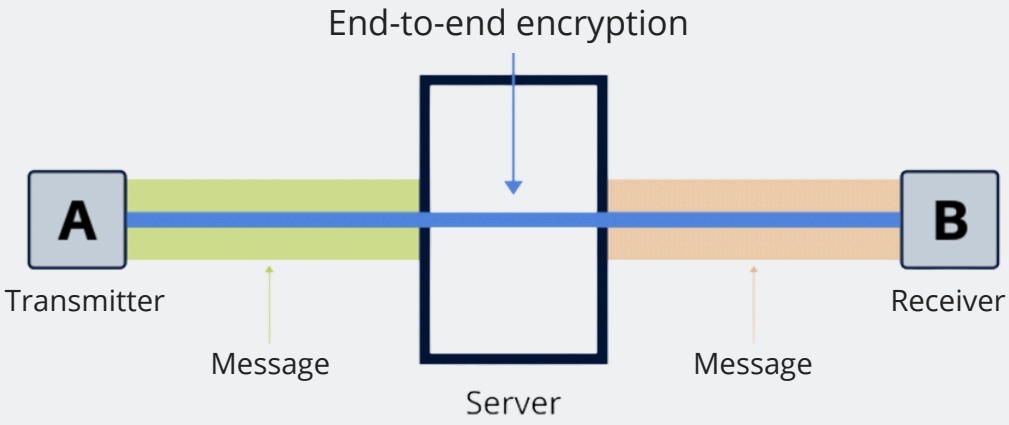
Our transparent privacy policy provides more information on data protection. It provides detailed information about the type, purpose and scope of the processing of personal data.

Technical Data

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

MobiVisor Messaging

End-to-end encryption:



256-bit public-private Keys werden generiert (entspricht **3072 bit RSA**).

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

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

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

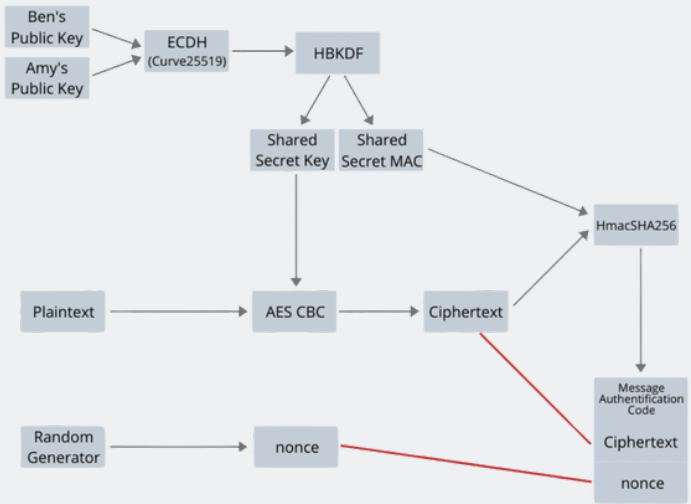
$$KEY_{mac} = AB_{shared\_expandet}[256-511]\ //\ Integrity\ Check$$

Encryption:

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

$$Mac = HmacSHA256(encryptedContent)\ //\ Integrity\ Check$$

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



MOBIVISOR

MobiVisor Messaging

Local hard disk encryption:

The messages are not saved 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=$encrypt_{pin\_key}$(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 isn’t sufficient

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