

In cooperation with



**FREE
TESTING
6 WEEKS**

SIMPLE AND SECURE COMMUNICATION

Enterprise Messaging with NetSfere

NO DAY WITHOUT

Every day, people all over the world send 65 billion messages via WhatsApp. Also thanks to this leading consumer app, messaging has become part of peoples' everyday lives. Rapid, mobile exchange of information has also arrived in companies. Of these, 70 percent already use chat apps for simple communication among employees. 61 percent use them for group discussions. On the other hand, 41 percent of all companies do not know whether their employees also use consumer messaging for business purposes. There are great risks associated with this, such as the violation of regulations and data protection legislation, lost and theft of company data or even infiltration of malware. WhatsApp, for example, does not assume liability for this type of damage if it used for business purposes. The secure messaging solution NetSfere, which was specially developed for companies, can solve this problem. Thanks to its valuable features, security and IT integration possibilities, NetSfere is gaining importance on the market. According to the Ovum study, NetSfere is in 3rd place globally, and 2nd place in Germany. For efficient and secure collaboration, T-Systems will provide NetSfere in your company, either in the Cloud, on site or as a hybrid solution.

NETSFERE HIGHLIGHTS

- Mobile communication for closed user groups
- With HD telephony and video broadcasts
- For all current mobile operating systems and PC
- End-to-end encrypted conversations
- IT administrators control user accounts and security guidelines
- Control of communication relationships and attachments
- Rapid (de)activation of user and guest accounts
- Remote deletion of content on lost or stolen devices
- Statistics, reports and secure archiving
- Bot with artificial intelligence for automated response to open questions to relieve employees
- Available as a Cloud-based, on-premise and hybrid solutions
- Compliant with General Data Protection Regulation

**Winner in the digitization category
in the German health care industry 2018**
Entscheiderfabrik, February 2018

T · · Systems ·

TAILORED TO THE NEEDS OF COMPANIES WITH MANY FUNCTIONS



Most current end-to-end encryption



Central control and administration



Synchronization in real time



HD audio calls and broadcast communication channels



Inclusion of external participants



MOST CURRENT END-TO-END ENCRYPTION

NetSfere ensures security through first class protection for conversations and internal company data. The central function for maintaining confidentiality of corporate communication is the encryption using one of the most modern methods currently available. The Secure Real-Time Transport Protocol (SRTP) uses the 256-Bit-AES algorithm with elliptical curve key exchange. The encryption is done device to device and secures every message and attachment continually along the entire transfer path with a unique key.

CENTRAL CONTROL AND ADMINISTRATION

The IT administrator retains complete control of the implementation of the end user guidelines and the administrative, physical and technical security measures. They can deactivate user accounts, remotely delete mobile devices, lock attachments by file type and platform and view file access, file saving and use statistics via a web-based control field.

SYNCHRONIZATION IN REAL TIME

NetSfere enable immediate communication and collaboration among team members. The information is synchronized on various devices in real time and message and provision status is immediately visible. If an employee is using a different mobile device, they only have to install the app, log in with their existing account and all of their personal messages are available. Even entire calls can be synchronized on multiple devices.

HD AUDIO CALLS AND BROADCAST COMMUNICATION CHANNELS

Telephoning and publishing videos on the app requires the highest quality in the business sphere. Thus NetSfere enables encrypted audio calls in HD quality and high performance video broadcast.

INCLUSION OF EXTERNAL PARTICIPANTS

Using the guest function and personalized invitations, external users can join a conversation via URL access. Permanent or temporary, secure chat rooms simplify cooperation with external participants.

ARCHIVING AND REGULATORY COMPLIANCE

All sent messages can be archived to comply with regulations. These remain available long-term, even if the user deletes his messages. The administrator retains control of all archives and access, which will also be reported. Such a report can be called up at any time and relevant reports can be generated for audits.

10× DATA PROTECTION

1. No access to the user's local address book
2. Protection of message meta-data through end-to-end encryption
3. No data saving or data transfer outside of the European Union
4. Full control of all integrations, bots and APIs
5. Option for complete data and user deletion
6. The data protection manager has the option of checking security breaches
7. Completely searchable messaging archive
8. Pseudonymization and encryption of all personal information
9. Protection from undesired, damaging outflow of data (Data Loss Prevention)
10. Audit logs and reporting of all significant processes

CONTACT

Andreas Uhrich
Phone: +49 175 2917627
E-Mail: mobile-enterprise@telekom.de

PUBLISHED BY

T-Systems International GmbH
Hahnstrasse 43d
60528 Frankfurt am Main, Germany