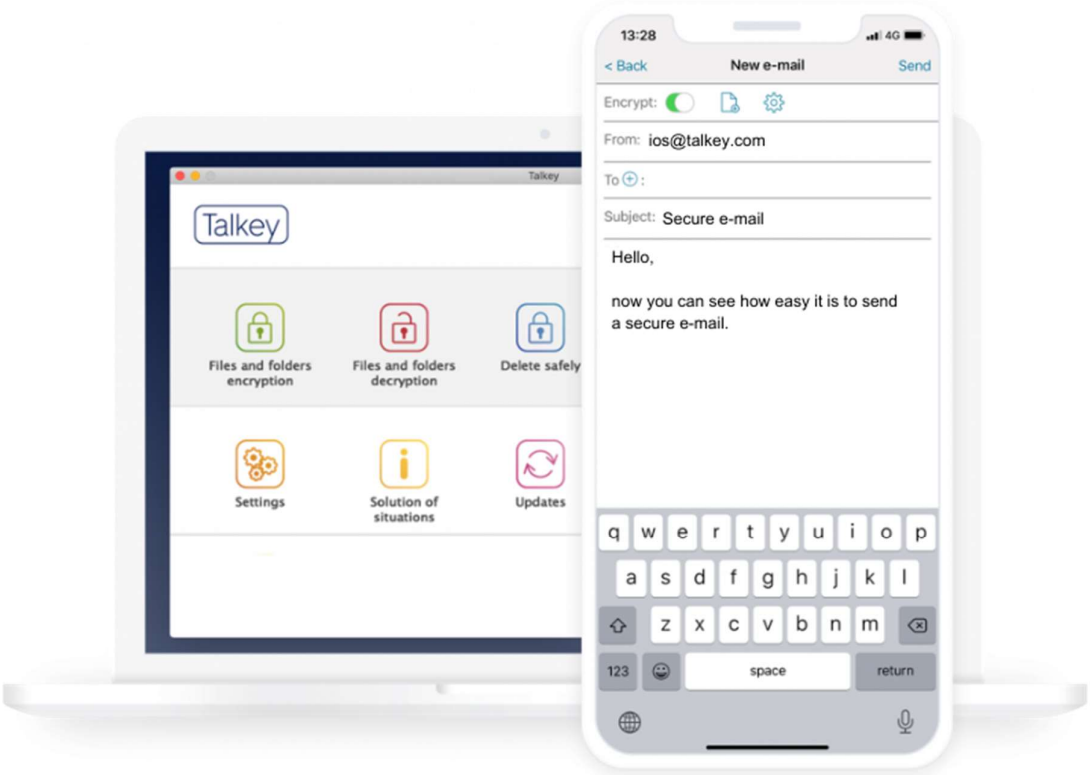
Talkey

Datasheet



member of ette

Talkey

Talkey is an encryption tool that offers a solution for secure electronic communication. Encrypts emails, folders and files. It has advanced functions, thanks to which the user defines how their data is handled also in the environment of third-party devices. Talkey is available for both mobile devices (Android, iOS) and desktop platforms (Windows, macOS).

Principles of used technology

The implemented algorithms meet the recommendations of the National office for Cyber and Information Security in the field of cryptographic means.

✓ **End-to-end encryption**
Communication does not run through the service provider‘s servers.

✓ **Double encryption**
Talkey uses double encryption, symmetric and asymmetric:

- symmetric algorithms: AES-256 CBC
- asymmetric algorithms: RSA-2048 OAEP
- hash algorithms: SHA-384

E-mails, files and folders are symmetrically encrypted with a randomly generated symmetric key. Together with the key they are then encrypted asymmetrically with the public key of the counterparty-recipient. This creates an encrypted .mtm e-mail, an encrypted .mtk file, and an encrypted.mtd folder. E-mails, files and folders encrypted in this way, can only be decrypted on their device by user who has the appropriate private key.

✓ **Resilience to attacks on infrastructure**
The system dos not have any "Master Key“, which, if obtained, would mean a loss of credibility of the entire system. There is no way to obtain users' private decryption keys from the service provider‘s servers.

✓ **Multi-factor protection of decryption keys**
The user has the option to save the key to a computer and mobile phone, or for better security on a password protected token with a limited number of attempts to enter the password.

Functionality

E-mail encryption

- ✓ setting the time, for which the message is accessible
- ✓ setting the number of e-mail openings
- ✓ deleting an already sent message in the recipient‘s mailbox
- ✓ option to disable the display of an e-mail on the mobile device
- ✓ option to disable e-mail forwarding
- ✓ deniable encryption by embedding a confidential message in a fictitious message
- ✓ encrypted e-mails search
- ✓ encryption of content, including attachments
- ✓ automatic detection of a Talkey user on the recipient‘s side
- ✓ confirmation of the sender‘s identity

Files/Folders encryption

- ✓ setting the time for which files/folders are accessible
- ✓ setting the number of times files/folders can be opened
- ✓ secure deletion of files/folders without the possibility of recovery
- ✓ management of user groups for access to files/folders

Talkey

The process of e-mail communication between users

Automatic recipient detection

If the sender fills in the recipient entry in the e-mail, the Talkey client contacts the operator's server service and determines whether the recipient is a Talkey user or not.

1/ If the recipient is a Talkey user, the application automatically chooses encryption, and the e-mail is encrypted before sending.

2/ If the recipient is not a Talkey user, the sender is asked to enter recipient's phone number to which a password for reading encrypted messages will be sent. After entering the phone number, the e-mail is encrypted and sent.

Content transfer

A sent e-mail, encrypted thanks to Talkey, looks like a pile of illogical characters on its way from sender to recipient and can only be read by a person who has a unique key to decrypt it.

Sender confirmation

Talkey automatically inserts confirmed sender identity information into encrypted e-mails. The recipient has a guarantee that the message actually comes from the sender and that is has not been read or altered during its transmisson.

Decryption

The recipient receives an encrypted e-mail.

1/ If the recipient is a Talkey user, he decrypts the content by clicking on the .mtm file attachment.

2/ If the recipient is not a Talkey user, he decrypts the e-mail by clicking on the link in the e-mail. The e-mail content is decrypted in a secure web interface after entering the password from the text message.

Sending an encrypted reply to an encrypted e-mail

1/ If the recipient is a Talkey user, he can reply by clicking the send button. Then he proceeds as when initialising the encrypted communication.

2/ If the recipient is not a Talkey user, he still has the option of answering incoming encrypted e-mail by an encrypted reply for free. After clicking reply he will be asked to download the Talkey reader version. As a Talkey reader user, he can answer incoming encrypted e-mail by an encrypted reply but cannot initiate a new communication.

Talkey Enterprise Server

The server part of the solution in a corporate environment allows:

- ✓ user management and setting of their permissions
- ✓ settings the permission hierarchy for opening messages from selected recipients
- ✓ automatic connection of users
- ✓ global/local communication
- ✓ enabling/disabling the use of mobile platforms
- ✓ enabling/disabling the use of advanced features
- ✓ solution of borderline situations – destruction of keys in case of their loss, shutdown of the user
- ✓ release management support – dissemination, enforcement of new version, security upgrades and central installations

Technical requirements for installation

Minimal requirements

Servers running in a virtualised enviroment (Talkey Enterprise Server)

- 4 vCPU
- 4 GB RAM
- 100 GB HDD
- OS: CentOS 7
- DB server MySQL
- MariaDB database server
- Web server Apache

End PC stations

Windows operating system

- Windows 10 and newer
- MS Outlook 2010 and newer
- 1 GHz processor and faster
- RAM 512 MB
- Hard disk space: 500 MB
- 1 x USB port 2.0 or 3.0 (when using token)
- Internet connection

macOS operating system

- Mac OS X 10.10 Yosemite and newer
- Encryption and decryption is done in the Talkey app
- 1 GHz processor and faster
- RAM 512 MB
- Hard disk space: 500 MB
- 1 x USB port 2.0 or 3.0 (when using token)
- Internet connection

Mobile devices

- Android 6 and newer
- iOS 8 and newer
- iPadOS 13 and newer

Basic product support

Service-level agreement (SLA)

Helpdesk support	24/7
Response Time	NBD*)
Repair Time	within 30 days of reporting the issue

*) NBD – Next Business Day

Warning: The user can back up their key to external media. If the key and its backup are lost, the data cannot be restored.