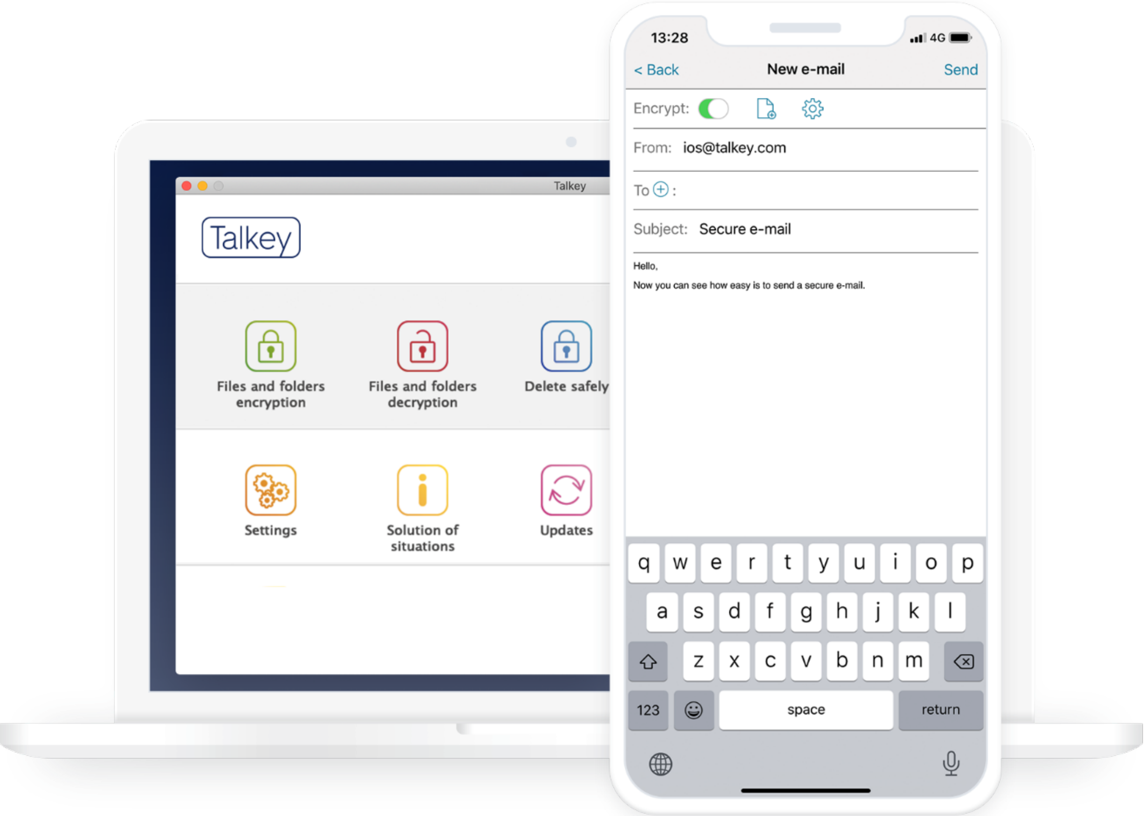
Talkey

Datasheet



From: ios@talkey.com

Subject: Secure e-mail

Hello,

Now you can see how easy is to send a secure e-mail.

member of ette

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 his 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 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 key 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 passwordprotected token with a limited number of attempts to enter the password

Functionality

E-mail encryption

- ✓ settings the time, for which the message is accessible
- ✓ setting the number of e-mail openings
- ✓ delete an already sent message in the recipient´s mailbox
- ✓ option to disable the display of e-mail on the mobile device
- ✓ option to disable e-mail forwarding
- ✓ denyable encryption by embedding a confidential message in a fictitious message
- ✓ encrypted e-mails search
- ✓ encrypt content, including attachments
- ✓ automatic detection of the 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 group for access to files/folders

Invite contacts to encrypted communication

The user can invite an unlimited number of people to create their own community with which to communicate securely. He simply invites his contacts to use Talkey Reader, which allows them to decrypt for free and also reply to the user in encrypted form. The invitee will become a free user without access to advanced features.

The whole process is simple and takes place in two steps:

1) sending an initialization e-mail for installation and sms message with a password,
2) activation of encryption on the invited party - key generation, password authentication and inclusion in the infrastructure of the public key exchange service provider.

The process of e-mail communication between users

Automatic recipient detection

If the sender fills in the recipient's entry in the e-mail, the Talkey client contacts the operator's server service and finds out whether the recipient is a Talkey user or not. If it is, it automatically chooses encryption and the email is encrypted before sending. This feature can be turned off by the user.

Sender confirmation

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

Content transfer

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.

Decryption

The recipient receives an encrypted e-mail. After clicking on the .mtm file, the contents of the encrypted message will be displayed.

Talkey Enterprise Server

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

- ✓ user management and settings their permissions
- ✓ settings the permission hierarchy for opening messages from selected recipients
- ✓ automatic connection of users
- ✓ global/local communication
- ✓ allowing/prohibiting the use of mobile platforms
- ✓ enable/disable 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 vesrion, security upgrades and central installations

Technical requirements for installation

Minimal requirements

Servers running in a virtualized 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

operating system Windows

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

operating system macOS

- 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 (while 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 his key to external media. If the key is lost and its backup, the data cannot be restored.