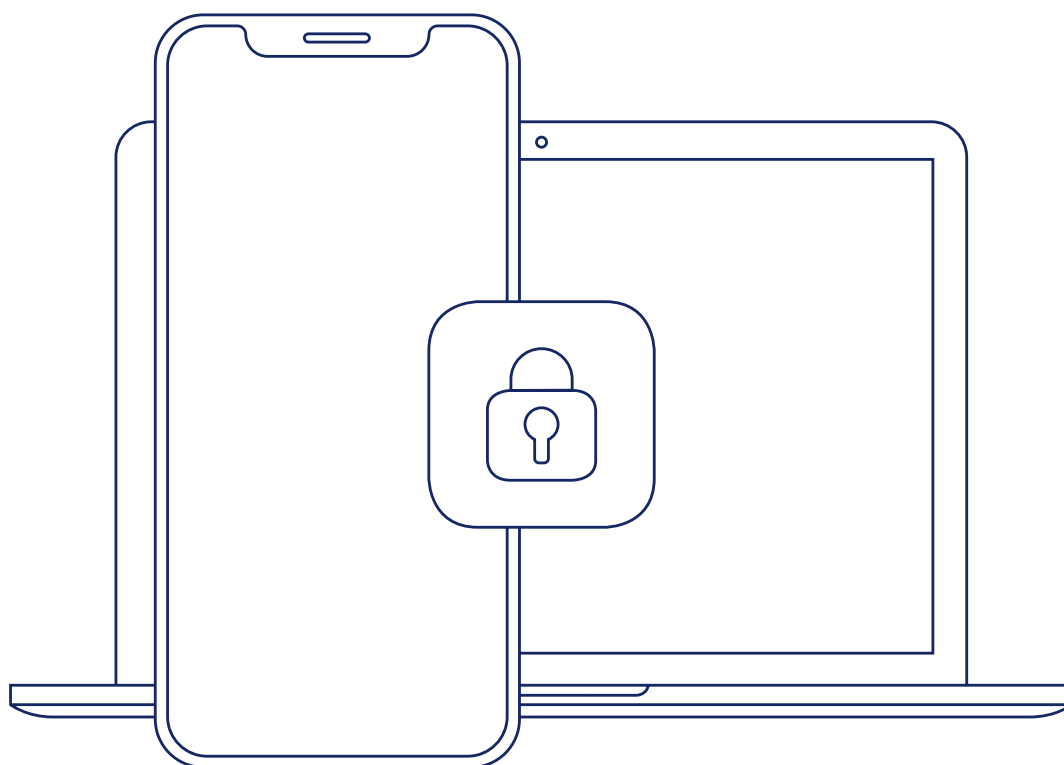




E-MAIL A DATA V BEZPEČÍ

Datasheet





E-MAIL A DATA V BEZPEČÍ

Talkey je šifrovací nástroj, který nabízí řešení pro bezpečnou elektronickou komunikaci. Šifruje e-maily, složky a soubory. Disponuje pokročilými funkcemi, díky kterým uživatel definuje, jakým způsobem se s jeho daty nakládá také v prostředí cizích zařízení. Talkey je k dispozici jak pro mobilní zařízení (Android, iOS), tak pro desktopové platformy (Windows, macOS).

Odesílání šifrovaného e-mailu

Odeslání šifrovaného e-mailu je stejně jednoduché jako u e-mailu běžného, pouze u příjemců, kteří dosud Talkey nepoužili, přidá odesílatel jejich mobilní číslo, na které bude zasláno heslo pro dešifrování odeslaného e-mailu. Příjemce získá rovněž možnost instalovat si aplikaci Talkey do svého zařízení, která mu umožní zdarma přijímat i odesílat šifrované e-maily a stane se tak plnohodnotným uživatelem.

Proces šifrované komunikace

Automatická detekce příjemce

Pokud odesílatel vyplní položku příjemce v e-mailu, Talkey klient kontaktuje serverovou službu provozovatele a zjišťuje, zda daný příjemce je, nebo není uživatelem Talkey. Pokud je, automaticky zvolí šifrování a e-mail se před odesláním zašifruje. Tuto funkci si může uživatel vypnout.

Přenos obsahu

Odeslaný e-mail, zašifrovaný díky Talkey, na své cestě od odesílatele k příjemci vypadá jako hromada nelogických znaků a přečíst ji dokáže pouze osoba, která vlastní jedinečný klíč k jejímu dešifrování.

Potvrzení identity odesílatele

Talkey automaticky vkládá do šifrovaných e-mailů informaci potvrzující identitu odesílatele. Příjemce má záruku, že zpráva skutečně pochází od uvedeného odesílatele a že během svého přenosu nebyla přečtena ani pozměněna.

Dešifrování

Příjemce obdrží zašifrovaný e-mail. Po kliknutí na soubor s příponou .mtm se mu zobrazí obsah zašifrované zprávy. Pokud příjemce ještě není uživatelem Talkey, dešifruje kliknutím na odkaz v e-mailu. Obsah se dešifruje v zabezpečeném webovém rozhraní po zadání hesla z sms zprávy.

Odeslání šifrované odpovědi na šifrovaný e-mail

Pokud příjemce chce odpovědět šifrovaně, je třeba mít aplikaci Talkey nainstalovanu.

Principy použité technologie

Implementované algoritmy splňují doporučení Národního úřadu pro kybernetickou a informační bezpečnost v oblasti kryptografických prostředků.



End-to-end šifrování

Komunikace neběží přes servery poskytovatele služby.



Dvojitě šifrování

Talkey využívá dvojitě šifrování, symetrické a asymetrické:

symetrické algoritmy: AES-256 CBC

asymetrické algoritmy: RSA-2048 OAEP

hash algoritmy: SHA-384

E-maily, soubory a složky jsou symetricky zašifrovány náhodně vygenerovaným symetrickým klíčem. Spolu s klíčem jsou následně zašifrovány asymetricky veřejným klíčem protistrany–příjemce. Tímto postupem vznikne šifrovaný e-mail s příponou .mtm, šifrovaný soubor s příponou .mtk a šifrovaná složka s příponou .mtd. Takto zašifrované e-maily, soubory a složky může na svém zařízení dešifrovat pouze uživatel, který má k dispozici příslušný privátní klíč. Upozornění: Svůj klíč může uživatel zálohovat na externím médiu. Při ztrátě klíče a jeho zálohy data nelze obnovit.



Odolnost proti útokům na infrastrukturu

System nedisponuje žádným „Master Key“, který by v případě jeho získání znamenal ztrátu důvěryhodnosti celého systému. Neexistuje možnost, jak získat privátní dešifrovací klíče uživatelů ze serverů poskytovatele služby.



Více faktorová ochrana dešifrovacích klíčů

Uživatel má možnost si klíč uložit do počítače a mobilu, nebo pro větší bezpečnost na token chráněný heslem s omezeným počtem pokusů o jeho zadání.

Funkcionality



Šifrování e-mailů

- nastavení doby, po kterou je zpráva přístupná
- nastavení, kolikrát lze zprávu otevřít
- smazání již odeslané zprávy ve schránce příjemce
- možnost zakázat zobrazení e-mailu na mobilním zařízení
- možnost zakázat přeposílání e-mailů
- popíratelné šifrování vnořením důvěrné zprávy do zprávy fiktivní
- vyhledávání v šifrovaných e-mailech
- šifrování obsahu, včetně příloh
- automatická detekce uživatele Talkey na straně příjemce
- potvrzení identity odesílatele



Šifrování souborů/složek

- nastavení doby, po kterou jsou soubory/složky přístupné
- nastavení, kolikrát lze soubory/složky otevřít
- bezpečné smazání souborů/složek bez možnosti obnovení
- správa skupin uživatelů pro přístup do souborů/složek

Talkey Enterprise Server

Serverová část řešení v korporátním prostředí umožňuje:

- správu uživatelů a nastavení jejich oprávnění
- správu klíčů a jejich zálohování
- nastavení hierarchie oprávnění pro otevření zpráv od vybraných příjemců
- automatické propojení uživatelů
- globální/lokální komunikaci
- povolení/zákaz používání mobilních platforem
- povolení/zákaz používání pokročilých funkcí
- řešení mezních situací – zničení klíčů při jejich ztrátě, vypnutí uživatele
- podpora release managementu – šíření, vynucení nových verzí, bezpečnostních upgradů a centrálních instalací
- napojení na Active Directory



E-MAIL A DATA V BEZPEČÍ

Technické požadavky pro instalaci

Minimální požadavky

Servery provozované ve virtualizovaném prostředí (Talkey Enterprise Server)

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

Koncové PC stanice

operační systém Windows

- Windows 10 a novější
- MS Outlook 2010 a novější
- Procesor s frekvencí 1 GHz a vyšší
- RAM 512 MB
- Prostor na disku: 500 MB
- 1 x USB port 2.0 nebo 3.0 (při využití tokenu)
- internetové připojení

operační systém macOS

- Mac OS X 10.10 Yosemite a novější
- Šifrování a dešifrování probíhá přes aplikaci Talkey
- Procesor s frekvencí 1 GHz a vyšší
- RAM 512 MB
- Prostor na disku: 500 MB
- 1 x USB port 2.0 nebo 3.0 (při využití tokenu)
- internetové připojení

Mobilní zařízení

- Android 6 a novější, iOS 8 a novější, iPadOS 13 a novější

Základní podpora produktu

Service-level agreement (SLA)

Přístup na Helpdesk	24/7
Response Time	NBD*)
Repair Time	do 30 dní od nahlášení vady

*) NBD - Next Business Day - následující pracovní den



E-MAIL A DATA V BEZPEČÍ

talkey.com/datasheet



© TALKEY a.s.

Vydáno: únor 2022

Kontaktní údaje: info@talkey.com

www.talkey.com

 member of ette

 služby
udržitelnost
technologie
životní styl