AVENET
DISTRIBUTION

Talkey

Šifrovací technologie Talkey
pro vysoce bezpečnou ochranu e-mailové komunikace, souborů a dat uživatelů

Výhradní distributor pro Českou republiku
AVENET Distribution s.r.o.
Košinova 655/59, Královo Pole, 612 00 Brno

Tel: **+420 778 759 138**
Email: **distribution@avenet.cz**

Talkey je technologie pro šifrování dat. V současnosti podporuje šifrování emailové komunikace a souborů, ve vývoji je mnoho dalších funkcí. Design technologie Talkey stojí na těchto základních myšlenkách:

- Otevřená skupina uživatelů, která není limitována perimetrem korporace.
- End-To-End šifrování na úrovni uživatel – uživatel, bez jakéhokoli zásahu provozovatele služby.
- Vysoká bezpečnost daná vícefaktorovou ochranou dešifrovacích klíčů s využitím hardwarového tokenu.
- Minimum informací pro poskytovatele služby tak, aby uživatelé byli na něm v maximální míře nezávislí.
- Uživatelská přívětivost a maximální jednoduchost. Uživatel nesmí zásadně měnit své návyky.
- Politika záruky důvěryhodnosti založená na přístupu typu Crystal Box. Hodnota myšlenky a nápadu je jinde, než v samotných zdrojových kódech řešení Talkey.
- Unikátní a jedinečné funkce.
- Talkey nabízí čtyři základní produktové línie, které jsou popsány dále v samostatné kapitole.

TOKEN

- Speciální hardwarové USB zařízení, které obsahuje šifrovací technologii – vysoce bezpečné uložení dešifrovacího klíče a provádí se na něm veškeré kryptografické operace.
- Token nese dešifrovací klíče konkrétního uživatele, není jej možné sdílet více uživateli najednou. Token je přenositelný konkrétním uživatelem mezi více počítači.
- Přístup na token je chráněn heslem. Uživatel si může nastavit speciální heslo, po jehož zadání se nenávratně zničí všechny dešifrovací klíče, které jsou na tokenu uloženy. Obdobně je omezen počet pokusů chybně zadaného hesla. Po jejich vyčerpání se dešifrovací klíče opět ničí.
- Uživatelská práce s tokenem je jednoduchá a pro uživatele pochopitelná – při vsunutí tokenu do počítače a zadání hesla je uživatel schopen dešifrovat a šifrovat data. Po jeho vysunutí není možné data dešifrovat – vícefaktorová bezpečnost.
- Ke každému tokenu uživatel obdrží tzv. záložní flash, na který se při vygenerování uloží kopie dešifrovacích klíčů. Záložní flash slouží pro obnovu například ztraceného tokenu. Při zničení nebo ztrátě tokenu a ztrátě flash neexistuje cesta, jak lze dešifrovací klíče obnovit.
- V současnosti je k dispozici token pro desktop platformy s USB rozhraním. Ve vývoji je nový druh tokenu, který bude kompatibilní s většinou v současnosti používaných mobilních platforem.

ZÁKLADNÍ VLASTNOSTI

- **End-To-End komunikace**
  Komunikace neprochází žádným serverem poskytovatele. Obsah zpráv ani záznamy o komunikaci neprochází žádným způsobem přes infrastrukturu Talkey a poskytovatel nedisponuje žádnými záznamy o aktivitách uživatelů nebo jiných dat. Společnost se tak stává nevydíratelná.

- **Kde se šifruje?**
  Šifrování probíhá na tokenu pomocí šifrovacích klíčů uživatelů, kteří budou mít možnost e-mail nebo soubor dešifrovat. Šifrovací klíče jsou umístěny pro automatickou distribuci na serveru provozovatele. Tyto klíče jsou veřejné a slouží pouze k šifrování. Jejich znalost umožňuje pouze zašifrování, nepředstavuje tedy žádné riziko.
  K dešifrování je nutné mít na tokenu soukromý dešifrovací klíč. Tento dešifrovací klíč je uložen pouze na tokenu a jeho kopie na záložní flash. Provozovatel služby nemá k dispozici dešifrovací klíče, ani žádnou možnost, jak tyto klíče získat nebo dešifrovat data uživatelů.

- **Žádný Man In The Middle (MITM)**
  Řešení je plně odděleno od poskytovatele. Talkey je otevřená a globální služba – komunikovat může každý s každým, i ve skupinách. Služba nemá žádná zadní vrátka. Poskytovatel nemá žádnou kontrolu nad činností uživatelů. Cílem je poskytnout bezpečný uživatelský nástroj.

- **Uživatel není omezen počtem počítačů**
  Talkey může uživatel používat na neomezeném počtu zařízení. Pokud používá Windows ve firmě a osobní data na Apple zařízení – nijak jej Talkey nelimituje. Uživatel registruje pouze e-mail do komunitní služby Talkey.

JEDINEČNÉ VLASTNOSTI TALKEY

Jedinečnost Talkey je nejen v oddělení dešifrovacího klíče od samotných dat, ale také ve vlastnostech, a to pro:

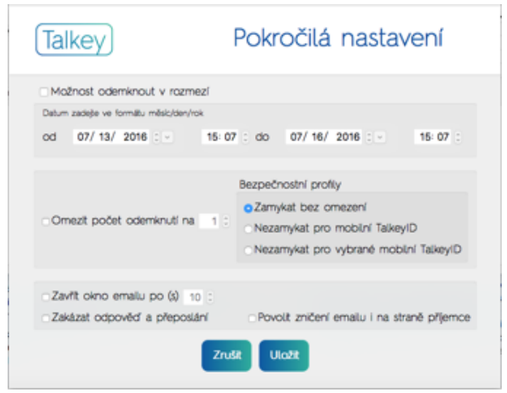
Šifrování e-mailové komunikace

- **Šifrování obsahu e-mailu včetně jeho příloh**
  Šifrovaný e-mail si přečte pouze odesílatel a vybraní příjemci. Uživatel si vybírá ze seznamu uživatelů, kteří již službu Talkey používají – e-mail se pro ně automaticky zašifruje.

- **Uživatel, který Talkey nepoužívá**
  Pokud uživatel Talkey pošle zašifrovaný e-mail uživateli, který Talkey službu nevyužívá, může si zabezpečený e-mail přečíst a odpovědet v Talkey prohlížeči /tzv. reader/. Nemá povoleny placené funkce. Odesílatel není nijak omezen v komunikaci – může poslat libovolný počet šifrovaných zpráv neomezenému počtu uživatelů. Je pouze na odesílateli, komu pošle šifrovanou zprávu. Příjemce, který Talkey nemá, má vždy možnost doručenou poštu přečíst a odpovědět.

- **Ničení odeslaných e-mailů odesílatelem na počítači příjemce**
  Odesílatel může ničit již odeslané e-maily i ve schránce příjemce. Jednoduše kliknutím na tlačítko u konkrétního e-mailu v odeslané poště.

- **Časové omezení existence e-mailové zprávy**
  Odesílatel nastavuje v parametrech zprávy /viz obrázek/ možnosti, kdy termínově zprávu příjemce může číst. Po uplynutí časového rozmezí se e-mail nenávratně zničí ve schránce příjemce.



- **Časové 10 sekundové okno pro přečtení zprávy**
  Lze zaslat e-mail, který se po 10 sekundách zničí a už jej nikdo ve schránce neotevře. Časový limit je možné měnit.

- **Zákaz přeposlání e-mailové zprávy příjemcem**
  Příjemce nemůže z e-mailů zkopírovat text, ani jej přeposlat dále.

- **Omezení počtu otevření e-mailů**
  Odesílatel nastavuje parametr počtu otevření. Po vyčerpání otevření se e-mail zničí.

- **Popiratelné šifrování**
  Uživatel je schopen do jedné zprávy umístit zprávy dvě, a to včetně příloh. Jedna je důvěrná, druhá klamavá. Podle toho, jaké příjemce zadá heslo, si příjemce zobrazí důvěrnou nebo klamavou zprávu. Neexistuje žádná cesta, jak z velikosti zprávy dovodit, že tato zpráva obsahuje zpráv více.

- **Až 10 e-mailových adres**
  Každý uživatel služby si může nastavit až 10 e-mailových adres, ze kterých může šifrovat e-maily nebo soubory.

- **Pozvat známého do služby Talkey**
  Každý uživatel služby Talkey může zaslat e-mailem pozvání ke službě Talkey například svým obchodním partnerům.

ŠIFROVÁNÍ SOUBORŮ

- **Šifrování souborů pro sebe**
  Uživatel velmi jednoduše šifruje své dokumenty a jakékoliv další soubory či celé složky. Má možnost využít i parametru pro bezpečné smazání souboru nebo složky po zašifrování.

- **Šifrování souborů pro ostatní**
  Uživatel vybírá v Talkey aplikaci další příjemce (podle e-mailové adresy), kterým povolí dešifrování dokumentu nebo složky. Nebo si vytvoří skupinu uživatelů – stačí jen zadat jméno skupiny a šifruje pro všechny uživatele ve skupině

- **Časové omezení platnosti dokumentů**
  Tak jako e-mailovou zprávu, tak dokument může uživatel časově omezit. Po uplynutí intervalu není možné dokument otevřít.

- **Omezení počtu otevření dokumentu**
  Uživatel sám nastaví počet otevření souboru. Po vyčerpání hodnoty parametru není možné soubor znovu otevřít.

- **Bezpečné smazání souboru**
  Běžně smazaný soubor lze obnovit. Soubor smazaný pomocí Talkey již obnovit nelze. Uživatel tak dostává další bezpečnostní výhodu.

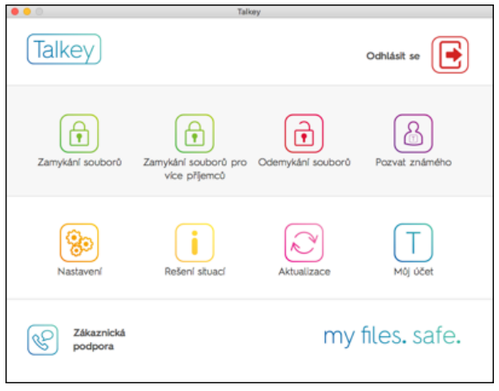
SPOLEČNÉ VLASTNOSTI

- **Aplikace Talkey /viz obrázek níže/**
  Aby služba mohla korektně fungovat, uživatel si instaluje na svůj počítač obslužný software - aplikaci Talkey, která slouží pro nastavení parametrů šifrování souborů, pro stahování aktualizací, přidávání dalších e-mailů do služby, pro nápovědu a řešení problémů, pro změnu hesla, a další.

- Po zašifrování e-mailu, souboru, nebo složky vznikne soubor se speciální příponou (.mtm, .mtk, .mtd). Přípony jsou naše vlastní formáty šifrovaného obsahu.

- **Záložní flash**
  Společnost Talkey nemá přístup ani k datům, ani dešifrovacímu klíči, ani k heslu k tokenu. Pokud jej uživatel ztratí, zničí nebo bude token zcizen, má možnost svůj dešifrovací klíč obnovit pouze ze záložního flash. Tato vlastnost je do jisté míry nevýhodou, ale z pohledu bezpečnosti je to jednoznačná výhoda. Je proto velmi důležité záložní flash bezpečně uschovat.

- **Správa záložní flash**
  Pro firemní prostředí je někdy důležité mít „určitou“ kontrolu nad komunikací ze strany zaměstnavatele. V tomto případě doporučujeme zaměstnavatelům ponechat si záložní flash s dešifrovacími klíči uživatelů ve správě a uživateli pouze poskytnou pouze token.



- **Mobilní platformy**
  Talkey podporuje práci na mobilních platformách v oblasti šifrování mailové komunikace a souborů. Protože token pro tyto platformy je ve vývoji a není tak možné dočasně nabídnout vícefaktorovou ochranu (dešifrovací klíč uživatele je uložen přímo na mobilním zařízení), umožňuje Talkey definovat bezpečnostní profily. Zde odesílatel – jako primární vlastník důvěrné informace – je schopen stanovit, zda je zpráva tak vysoce důvěrná, že ji příjemce je schopen dešifrovat pouze na tokenu, či takovou míru důvěrnosti nemá a uživatel ji může dešifrovat i na mobilním zařízení. Z kontextu toho vyplývá, že dešifrovací klíč uživatele na mobilním zařízení je jiný, než dešifrovací klíč uložený na tokenu.

POUŽÍVÁNÍ TALKEY A PODPOROVANÉ PLATFORMY

Talkey nijak neomezuje počet počítačů, kde se token používá. Svůj dešifrovací klíč si uživatel nese na HW zařízení - tokenu. Na daném počítači si pouze nainstaluje obslužný software Talkey.

- **Talkey aplikace**
  Instaluje se na zařízení s operačními systémy Microsoft Windows nebo Apple OSX. V aplikaci spravuje uživatel licenci, změnu hesla, stahuje aktualizace a nové funkce, přidává další e-maily pro šifrování, v případě potíží najde návody na řešení, nastavujete parametry šifrování, šifruje a dešifruje soubory, atp.

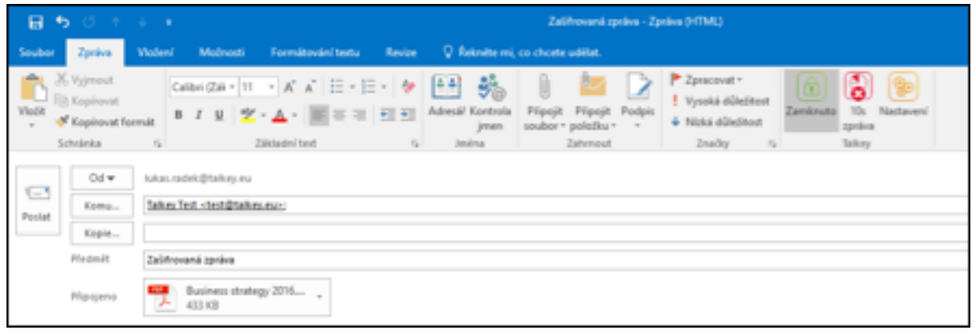
- **E-mailový klient**
  Uživatel není nijak omezen v používání svého e-mailového klienta, a to ani ve firemní infrastruktuře. Talkey podporuje dva typy klientů:

  Microsoft Outlook

  Mozilla Thunderbird

  Talkey E-mail for Android and iOS

- **Doplněk /AddOn/ pro e-mailového klienta**
  V procesu instalace aplikace se automaticky instaluje tzv. doplněk pro e-mailového klienta. Instalátor rozpozná typ klienta a přidá do menu nové tlačítka pro obsluhu Talkey.



TECHNOLOGIE A DŮVĚRYHODNOST

Případný útočník, který chce získat obsah šifrované komunikace, má teoreticky k dispozici tři cesty:

Útok na šifru hrubou silou – k tomuto útoku při použití šifer s dlouhými šifrovacími klíči, obvykle útočník nemá dostatek zdrojů.

Získání informace před jejím zašifrováním, případně po rozšifrování – zde je zachování důvěrnosti zpráv dáno zejména návyky uživatele (instalace nepotřebného či neověřeného software apod.)

Získání dešifrovacího klíče uživatele – v tomto případě musí jít o zcizení tokenu a útok na heslo uživatele s omezeným počtem pokusů.

Technologie Talkey je založena na dvojitém, symetrickém a asymetrickém šifrování. Talkey využívá standard RSA Encryption Standard 2048 bit v kombinaci s 3DES standardem.

Ochrana proti zkopírování dešifrovacího klíče je na nejvyšší úrovni. Certifikace FIPS 140-II level 3 zaručuje, že dešifrovací klíče nelze ze zařízení zkopírovat, ani mechanicky vyjmout čip. Při náznaku mechanického vniknutí se klíč samodestruktivně zničí.

Použité technologie a certifikace

- RSA 2048 https://en.wikipedia.org/wiki/RSA_numbers#RSA-2048
- 3DES https://en.wikipedia.org/wiki/Triple_DES
- FIPS 140-II level 3 https://en.wikipedia.org/wiki/FIPS_140-2#Level_3

Technologie je patentovaná a nabývá tak výhradního práva průmyslového užití.

Talkey navíc garantuje přístup typu Crystal Box je schopna přeložit zájemcům z řad klientů zdrojové kódy veškerého software k bezpečnostní analýze.

PATENTY A PRŮMYSLOVÁ OCHRANA

Český průmyslový vzor
- Zapojení pro ochranu dat, číslo 28 480

U.S. patenty v přípravě
- Šifrovaný telefon – před podáním
- HW token pro šifrování dat – v přípravě
- Pasivní scanner – v přípravě

PRODUKTY TALKEY

Poskytujeme 4 základní produktové linie s šifrovací technologií Talkey, které jsou určeny pro specifické komerční využití.

Talkey

Je základní službou pro uživatele. Uživatel má k dispozici veškeré funkce, kterou Talkey nabízí. Součástí licence je:

- Sada Talkey, obsahem je token a zálohovací flash, návod k instalaci
- Možnost generování 10 dešifrovacích klíčů pro 10 různých e-mailových adres uživatele
- Užití na neomezeném počtu počítačů a mobilních platforem
- Součástí je uživatelská podpora

Talkey Trial

Stejně jako u verze Talkey má uživatel má k dispozici veškeré funkce, kterou Talkey nabízí, ale pouze na omezenou časovou dobu (30 dní).

Talkey Reader

Uživatel je schopen číst a posílat šifrovanou poštu ale pouze s uživatelem který má aktivní placenou službu. Také je schopen dešifrovat své soubory. Scénář pro pochopení fungovaní Talkey reader: Právník posila via email Klientovi šifrovaný dokument/smlouvu. Právník je placeným uživatele Talkey, ale má potřebu komunikaci s osobou, která není placeným uživatelem Talkey. Proto jsme vyvinuli Talkey reader, aby Uživatel (Klient Právníka) byl schopen číst a posílat šifrovanou poštu, ale pouze s uživatelem který má aktivní placenou službu (v tomto případu Právník).

Klient Právníka v tomto případu je schopen dešifrovat emaile zaslané od Právníka zdarma (příklad: dešifruje email kde je word dokument, udělá v dokumentu změny, přiloží dokument jako přílohu do emailu, zašifruje email a odesle zpět Právníkovi). Musí si na žádost Právníka jenom stáhnout z webowe stránky talkey aplikace, která ma osekané funkce. To dává možnost právnické kanceláře bezpečně komunikovat se zákazníky, bez toho že pro ne musí koupit Talkey nebo „donutit" jeho zákazníka do toho aby Talkey koupil, protože nemá jinou možnost.

Takže jsme vyšli vstříc našim klientům a umožnili tento typ komunikace mezi jejich klienty. Možná říct, že kdo koupi jeden Talkey tak v ceně má

taky Talkey reader, ale v minimální funkcionalitě. Znamená to, že právník tak může komunikovat se všemi klienty. A pokud právník ukládá data v cloudu, odkud si je klient stahuje dokumenty, scénář je následující: Na Cloudu to muže fungovat tak, že tam je nějaká složka zákazníka kterou založil Právník, zákazník si muže šifrovaný dokument stáhnout k sobě, dešifruje si ho, uloží u sebe na disku a muže dělat změny. Bohužel už nemůže šifrovat zpět tento dokument ve kterém udělal změny. Co muže Klient udělat tak jenom zašifrovat email, takže muže dokument dat jako přílohu a odeslat šifrovaně na Právníka ne zpět na Cloud. To dává možnost právnické kanceláře bezpečně komunikovat se zákazníky.

Talkey Enterprise Solutions

Služba je navržena pro firemní prostředí a zákazníky veřejné správy, kteří mají požadavek na nasazení šifrování ve větším rozsahu mezi své zaměstnance a zároveň mají požadavek sami určovat a spravovat šifrovací klíče uživatelů. Kupujete si pouze určitý počet tokenů a jejich přidělování provádíte sami dle vlastních okamžitých potřeb. Technologii Talkey jako službu dokáže společnost provozovat a spravovat ve vlastní infrastruktuře. Jednoduše si sami volíte, kteří uživatele mohou komunikovat mimo interní firemní síť, a naopak stanovíte pravidla pro pohyb šifrovaných e-mailů a dokumentů pouze v rámci své interní sítě.

Chráníte si svá firemní data, identity zákazníků, důvěryhodné dokumenty obchodního nebo výrobního charakteru. Řídíte si sami distribuci a oběh dokumentů na veřejném internetu a eliminujete riziko zneužití a ztráty dat lidskou chybou.

Talkey Enterprise poskytuje obdobnou funkcionalitu, jako Talkey, s těmito rozdíly:

- Talkey Enterprise server je nainstalován a zprovozněn v síti (on premise) zákazníka, zákazník si sám provádí jeho správu a zajišťuje jeho provoz;
- Zákazník je oprávněn pro své zaměstnance generovat šifrovací klíče, znefunkčnit je;
- Talkey Enterprise server se synchronizuje se servery Talkey, proto uživatel Talkey Enterprise je schopen šifrovaně komunikovat s kterýmkoli jiným uživatelem Talkey kdekoli na světě;
- v rámci Talkey Enterprise je možné používat SW verzi Talkey bez HW klíče. Tato verze je však omezena pouze na jeden počítač a jedno mobilní zařízení.

Technická specifikace

- **Talkey Enterpise Server:**
  - o Generování šifrovacích klíčů uživatelů;
  - o Podpora SW i HW verze uložiště klíčů uživatelů;
  - o Reporty a přehledy generovaných klíčů a uživatelů
  - o Zneplatnění klíče
  - o Zničení šifrovacího klíče
  - o Bezpečnostní a funkční update
  - o HW serveru dodává kompletně Talkey, nebo si dodá klient sám dle požadavků Talkey

- **SW klient**
  - o Uživatel má jen jednu licenci pro SW klienta na jednom počítači a jednom mobilním zařízení
  - o V rámci této licence má po dobu placení služby přístup k plné funkcionalitě toho, co Talkey vydá, v současnosti jde o:
    - Šifrování mailů
    - Šifrování souborů
    - Chat
- **HW klient**
  - o Obdoba standardní služby Talkey omezená na jeden počítač a jedno mobilní zařízení
  - o Přístup k plné funkcionalitě, kterou Talkey vydá
- **Talkey Reader**

Nabízíme připravené virtuální prostředí, které pouze zprovozníte na vlastních serverech. Součástí řešení je poskytnutí licencí na bázi open-source.

2 modely architektury:

- **Encryption-as-a-Service (EaaS)**
  Šifrování jako službu provozuje společnost myTALKEY s.r.o. na svých serverech.
- **On Premise nasazení**
  Šifrování provozuje zájemce ve vlastní IT správě a na vlastních prostředcích.

SPOLEČNÉ VLASTNOSTI TALKEY

	Talkey Reader	Talkey Trial (for 30 days)	Talkey	Talkey Enterprise	
				Soft Key	Hardware Key
Email					
Dešifrování e-mailu	✓	✓	✓	✓	✓
Šifrování e-mailu	Pouze platícím uživatelům	✓	✓	✓	✓
10s zpráva	✗	✓	✓	✓	✓
Omezení podle datumu	✗	✓	✓	✓	✓
Popiratelné šifrování	✗	✓	✓	✗	✓
Omezení počtu otevření	✗	✓	✓	✗	✓
Zničení odeslaných e-mailů	✗	✓	✓	✗	✓
Zobrazení zprávy na určitý čas	✗	✓	✓	✗	✓
Zakázat kopírování textu nebo přeposílání	✗	✓	✓	✗	✓
Počet e-mailových adres	1	10	10	3	10
Úprava těla e-mailu	✗	✓	✓	✓	✓
Soubory a složky					
Dešifrování souborů a složek	✓	✓	✓	✓	✓
Šifrování souborů pro sebe	✗	✓	✓	✓	✓
Šifrování souborů pro ostatní	✗	✓	✓	✓	✓
Šifrování souborů pro skupiny	✗	✓	✓	✓	✓
Šifrování složek	✗	✓	✓	✓	✓
Limit velikosti souboru	do 100 MB	do 4 GB	do 4 GB	do 13 GB	do 4 GB
Podpora					
Technická podpora 24/7	✗	24/7	24/7	24/7	24/7
Použití na více počítačích	✗	✗	✓	✗	✓
Hardware Token	✗	✗	✓	✗	✓
Heslo ke zničení Tokenu	✗	✗	✓	✗	✓
Osobní instalace	✗	✓	✓	✓	✓
Další funkce					
Šifrovaný chat	✗	✓	✓	✓	✓
Bezpečnostné mazání souborů	✗	✓	✓	✓	✓
Mobilní client	✓	✓	✓	✓	✓
Lokální tzv. On Premise server	✗	✗	✗	✓	✓