



**Vaše bezpečná
firemní komunikace**

www.babelapp.com

I. Co je BabelApp?

BabelApp je **platforma pro bezpečnou a efektivní komunikaci**, navržená pro použití na mobilních zařízeních a počítačích ve firemním prostředí a na internetu.

- ✓ Umožňuje posílat a ukládat zašifrované zprávy a dokumenty,
- ✓ zajišťuje šifrované telefonní hovory,
- ✓ chrání firemní komunikaci,
- ✓ brání úniku obchodního tajemství, osobních údajů a dalších chráněných informačních aktiv

BabelApp je bezpečnou variantou k e-mailu nebo instant messaging systémům.

Není provozován jako sdílená centrální služba, ani nezískává informace o kontaktech uživatelů ze zařízení. Dává plnou kontrolu a bezpečnost do rukou uživatelů a správců. Každá firma/instituce provozuje a spravuje vlastní server, řídí jeho komunikaci s ostatními servery a je autoritou pro adresy (BabelApp jména) svých uživatelů.



II. Hlavní přednosti BabelApp

1. BabelApp zajišťuje bezpečnost ve všech fázích použití

✓ Šifrované telefonování

BabelApp zajišťuje šifrované telefonické hovory mezi mobilními zařízeními v datové síti prostřednictvím sady technologií VoIP - zejména signalizace pro řízení spojení a výměnu veřejných klíčů, kodeků a protokolů pro přímou komunikaci mezi zařízeními se zajištěním důvěrnosti a integrity.

✓ Pořízení nahrávek

Fotografie, videa a zvukové nahrávky se pořizují přímo v aplikaci. Ovládání fotoaparátu/kamery a mikrofonu je řízeno přímo kódem aplikace, ne zařízením.

✓ Bezpečné uložení

Veškeré zprávy, nahrávky a dokumenty jsou uloženy zašifrované v prostředí aplikace u odesílatele i příjemce.

✓ Šifrovaná komunikace

BabelApp zajišťuje aplikační úroveň šifrování mezi koncovými body přenosu, kdy šifruje zařízení odesílatele a dešifruje zařízení příjemce. Šifrovaný obsah je opatřen kontrolou integrity na základě HMAC kódu. Fyzický transport šifrované zprávy probíhá asynchronně prostřednictvím autentizovaného TLS spojení s BabelApp serverem. Pokud jsou účastníci připojenými k různým serverům, probíhá komunikace pouze prostřednictvím BabelApp serveru odesílatele, což dále zvyšuje bezpečnost.

✓ Doručení na zařízení příjemce

BabelApp doručuje zprávy a dokumenty až na koncová zařízení, neukládá je dlouhodobě na serveru. Server poskytuje služby pro odeslání a doručení zpráv, zasílá komunikujícím stranám upozornění a v případě nedoručitelnosti zprávy dokumenty maže. V žádném případě nemá žádné klíče, které by umožňovaly číst procházející šifrovanou komunikaci.

✓ Bezpečné prohlížení

BabelApp umožňuje bezpečné prohlížení zpráv a běžných typů dokumentů (fotografie, PDF apod.) přímo v aplikaci pomocí kódu aplikace. Dokumenty tak nemusí opustit bezpečné prostředí BabelApp a nejsou vystaveny hrozbám při otevření v aplikacích třetích stran.

2.

BabelApp lze instalovat a provozovat v prostředí organizace



On-premise instalace

Jednoduchá instalace pomocí web instalátoru, server ve vlastní síti a pod vlastní správou poskytuje plnou kontrolu nad provozem a bezpečností.



Serverová replikace

Řešení vysoké dostupnosti – v případě havárie serveru je BabelApp připraven na obnovení provozu (ve stavu před havárií) během několika málo minut.

3.

BabelApp je produkt přímo od výrobce, který je držitelem všech autorských práv

Vývoj BabelApp se řídí potřebami uživatelů. Přímá komunikace výrobce se zákazníky umožňuje poskytnout mimořádné podmínky:

- ✓ Schopnost implementovat požadavky zákazníků na doplnění nebo změnu funkcí,
- ✓ místní podporu přímo od týmů vývoje a podpory produktu,
- ✓ jednodušší integraci než v případě globálních aplikací,
- ✓ možnost přizpůsobení vzhledu klientských aplikací – logo instituce, barvy,
- ✓ pružnou licenční politiku.

4.

Integrace se stávajícími aplikacemi a synchronizace s adresářovými službami

BabelApp umožňuje komunikovat nejen mezi uživateli, ale také rozesílat šifrované zprávy z aplikací uživatelům.

- ✓ Jednoduchá integrace s aplikacemi třetích stran – např. DMS systémy, tiskárny, MS Outlook, apod. prostřednictvím serverového REST API,
- ✓ možnost nastavit automatickou nebo asistovanou synchronizaci s Active Directory / LDAP adresářem a zjednodušit tak správu uživatelských účtů.

Způsob šifrování a obrany proti útokům:

Každá zpráva je šifrována standardním symetrickým algoritmem AES s jedinečným klíčem Message Key, který náhodně generuje aplikace BabelApp na zařízení odesílatele. Stejný klíč potřebuje i příjemce pro rozšifrování zprávy, proto je Message Key také zašifrován (tentokrát klíčem Contact Key) a připojen ke zprávě. Contact Key je spočítán příjemcem i odesílatelem s použitím standardního algoritmu Diffie-Hellman. Pro tento výpočet musí mít obě strany k dispozici ověřenou hodnotu veřejného klíče protistrany. Tyto veřejné klíče bezpečně distribuujeme na všechna registrovaná zařízení firemní BabelApp server.

Bezpečná komunikace je založena nejen na šifrování přenášených zpráv, ale i na jejich autentizaci a kontrole integrity, aby příjemce získal jistotu, že data pocházejí od legitimního odesílatele a nebyla změněna útočníkem. K tomuto účelu je zpráva nejprve zašifrována a poté je výsledný šifrový text „podepsán“ pomocí algoritmu HMAC s vlastním autentizačním klíčem (Encrypt-then-Authenticate).

III. Základy, na kterých BabelApp stojí

BabelApp je od základu vyvíjen s myšlenkou a s ohledem na zajištění maximální bezpečnosti komunikace a využití v existujících firemních/institucionálních informačních a komunikačních systémech (propojení s adresářovými službami, možnost připojení aplikací třetích stran, web rozhraní pro centrální správu atd.).

Kryptografie

Z bezpečnostního hlediska je systém založen na použití moderního know-how z oblasti kryptografie a na správné aplikaci silných kryptografických technik. Kryptografický návrh BabelApp byl vytvořen ve spolupráci s předním českým kryptologem RNDr. Vlastimilem Klímou (<http://cryptography.hyperlink.cz/>).

„Systém BabelApp používá moderní know-how z oblasti kryptografie a aplikuje správně silné kryptografické techniky. Při kontrole kryptografického designu jsem nenašel žádné slabiny ani pochybení z kryptografického hlediska. U vývojářů systému BabelApp jsem se setkal se snahou aplikovat to nejlepší z existujících prostředků a know-how. Nebál bych se přenášet svá tajemství tímto systémem.“

BabelApp využívá kombinace nejlepších kryptografických algoritmů a protokolů, které chrání komunikaci před aktivním i pasivním útokem:

- ✓ end-to-end šifrování pomocí symetrické šifry AES pro bezpečné zasílání zpráv v reálném čase (IM),
- ✓ bezpečná distribuce veřejných klíčů z firemního serveru, není třeba pořizovat žádné PKI certifikáty,
- ✓ další použité algoritmy: PBKDF2, SHA-2, Diffie-Hellman, RSA, HMAC-SHA256.

Blockchain

Naše aplikace využívá pro ověřování klíčů unikátní mechanismus, který pracuje s moderním bezpečným úložištěm, kde není možné, aby již jednou vložená data kdokoli jakkoli modifikoval. Toto úložiště se nazývá blockchainová databáze.

Veřejné blockchainové DB jsou v současné době využívány výhradně pro kryptoměny. Největší a nejbezpečnější z nich je DB, kterou používá Bitcoin. Kromě toho, že je tato DB využívána k zápisu jednotlivých Bitcoinových transakcí, je možné do ní zapisovat i jiné údaje.

V našem případě koncové zařízení s aplikací BabelApp zapíše do této databáze informace potřebné pro ověření veřejného klíče, které si mohou kdykoli přečíst ostatní účastníci komunikace. Pokud má tedy BabelApp server aktivovanou ochranu pomocí Bitcoinové sítě, kdokoli s vámi může komunikovat bez obav z útoku MITM, aniž byste si před komunikací museli volat a ověřovat veřejné klíče.

Server

Srdcem systému je BabelApp server. Tento server udržuje databázi účtů uživatelů a registrovaných zařízení, ověřuje a bezpečně uchovává veřejné klíče uživatelů a synchronizuje je na registrovaná zařízení. Server je vybaven serverovým SSL certifikátem a poskytuje klientské licence pro zařízení uživatelů.

Server zprostředkovává datovou komunikaci mezi zařízeními uživatelů, neuchovává ovšem žádné privátní ani tajné klíče a neúčastní se šifrování zpráv. V případě, že odesílatel nebo příjemce nejsou připojeni on-line, zajišťuje server zasílání notifikací a asynchronní doručení šifrovaných zpráv.

K serveru se všechna zařízení musí registrovat s využitím jednorázového hesla nebo prostřednictvím volitelné autentizace do adresářových služeb. Při registraci server získá a ověří veřejný klíč uživatele a uloží jej do centrálního adresáře. Po dokončené registraci se zařízení autentizují k serveru automaticky, bez zásahu uživatele.

Neomezená komunikace je založena na serverech, které bezpečně komunikují s klienty i mezi sebou prostřednictvím internetu. Správci mají možnost dovolit nebo zakázat komunikaci s cizími servery a uživateli.

Komunikační služby serveru:

- centrální adresář kontaktů
- distribuce a synchronizace veřejných klíčů uživatelů
- komunikace mezi servery pro získání veřejných klíčů příjemce z cílového serveru a doručení zprávy uživateli z jiné domény
- asynchronní doručení zpráv a příloh na více zařízení příjemce
- synchronizace zpráv odeslaných z jednoho zařízení na ostatní zařízení odesílatele
- dočasné uložení zašifrovaných příloh pro stažení příjemcem zprávy
- brána pro zasílání požadavků na rozeslání Push notifikací o zprávách čekajících na doručení
- zasílání informací o doručení a přečtení zpráv nebo o nedoručitelnosti
- komunikační brána s REST API pro snadnou integraci s aplikacemi a programovatelnými zařízeními k rozesílání šifrovaných zpráv a automatizaci firemních procesů

Funkce serveru pro správce:

- plná kontrola nad správou a celou infrastrukturou v rukou firemního správce
- web konzole pro správu systému
- import uživatelů z LDAP/AD
- synchronizace změn účtů z LDAP/AD
- možnost vytváření a správy uživatelských účtů a skupin pro regulérní členy a externisty
- registrace zařízení uživatelů pomocí OTP nebo LDAP autentizace
- vynucování minimální délky hesla v klientských aplikacích
- odebrání registrovaného zařízení
- zneplatnění klíčů
- zablokování uživatele
- reset účtu serveru na vzdáleném serveru
- smazání vzdáleného serveru z databáze účtů lokálního serveru
- systémové logování událostí serveru a uživatelů
- statistiky provozu
- možnost zasílání tzv. automatických zpráv uživatelům (typicky upozornění na nové verze, apod.) přímo ze serveru podle plánu

Klientské aplikace

Klienti BabelApp umožňují z koncových zařízení bezpečně telefonovat, šifrovat, dešifrovat, odesílat a přijímat zprávy a přiložené dokumenty prostřednictvím serveru, pořizovat a přehrávat vybrané formáty dokumentů přímo v aplikaci (fotografie, videa, hlasové nahrávky), ukládat zprávy a dokumenty v zašifrovaném tvaru, pracovat s konverzacemi více účastníků nebo vyhledávat kontakty v aplikaci i v centrálním adresáři.

Klienti BabelApp jsou k dispozici pro všechny významné platformy mobilních i stolních zařízení. Klientské aplikace jsou k dispozici zdarma prostřednictvím příslušných služeb (App Store, Google Play), nebo ve formě instalačního balíčku.

Mobilní klienti BabelApp:

a) iOS b) Android c) BlackBerry

iOS



BlackBerry

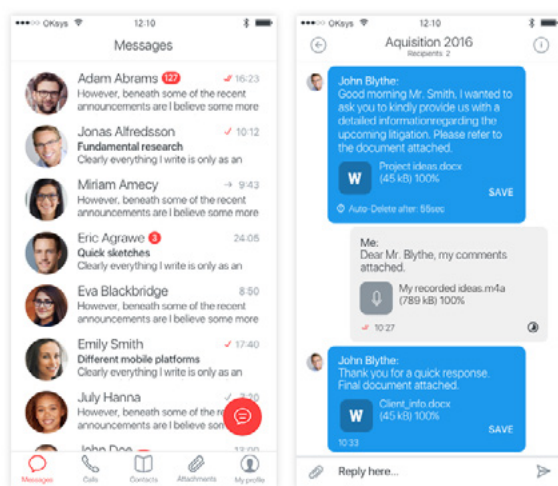
Klienti BabelApp pro počítače:

a) PC s Windows b) macOS (OS X)

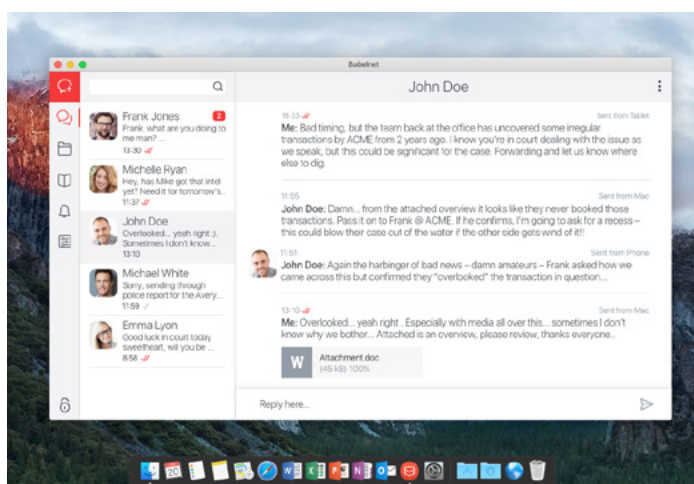
Windows



Každý uživatel může mít pod svým účtem registrováno více zařízení s libovolnou kombinací klientů. Každé zařízení může být připojeno k více serverům.



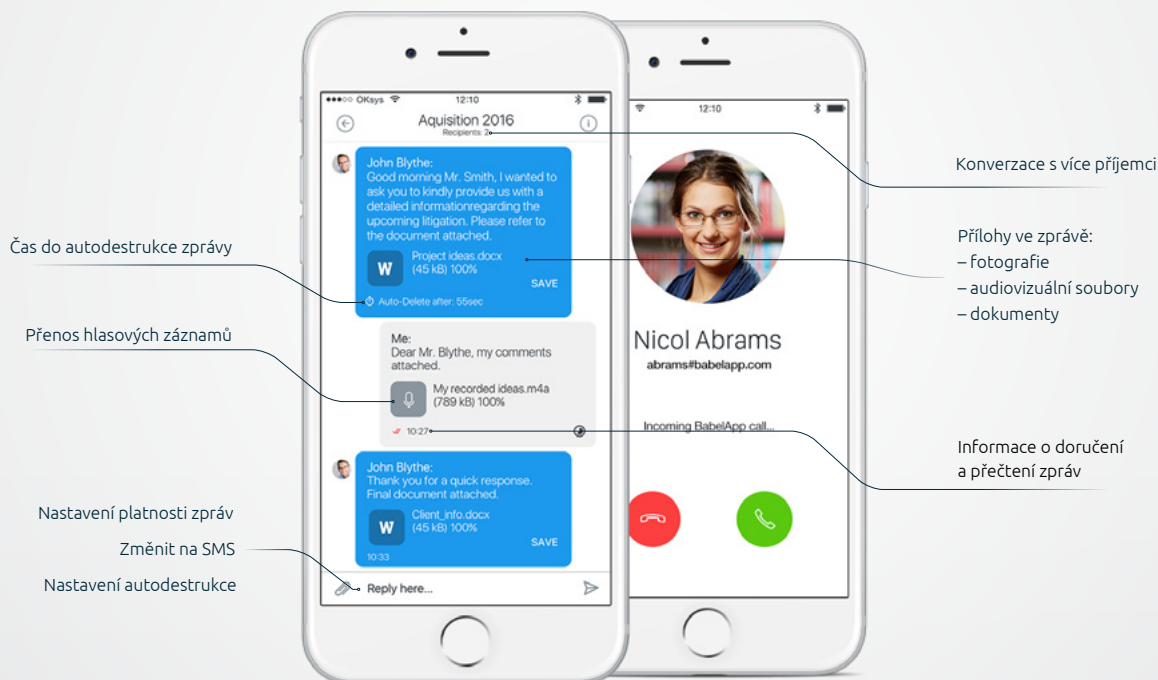
klient pro iOS



klient pro macOS

Funkce klientských aplikací

Hlavní funkce klientských aplikací jsou k dispozici na všech platformách, některé funkce (například šifrování SMS) jsou přístupné jen na mobilních zařízeních.



Telefonování:

- ✓ šifrované telefonování v datové síti prostřednictvím sady technologií VoIP
- ✓ Kvalitní zvuk a nepostřehnutelné zpoždění při nízké přenosové rychlosti
- ✓ Spotřeba dat pouze 0,5 MB/minutu hovoru

Základní funkce pro komunikaci:

- ✓ zasílání šifrovaných textových zpráv pomocí datového přenosu v internetu
- ✓ schopnost asynchronní komunikace (odesílatel nebo příjemce nemusí být on-line)
- ✓ zasílání šifrovaných textových zpráv pomocí SMS (v případě, kdy není roaming, nejsou data, nebo není server)
- ✓ zasílání zašifrovaných příloh (fotografie, videa, hlasové zprávy, libovolné další dokumenty...)
- ✓ možnost připojení zařízení k více serverům
- ✓ komunikace s více příjemci současně
- ✓ komunikace v konverzacích nebo samostatných zásilkách
- ✓ přeposlání zprávy jinému příjemci
- ✓ příjem a zobrazení informací o doručení zprávy, přečtení zprávy nebo upozornění o nedoručení odeslané zprávy
- ✓ příjem upozornění na zprávy čekající na doručení

Nastavení a mazání zpráv:

- ✓ nastavení platnosti zprávy
- ✓ autodestrukce zprávy
- ✓ mazání zpráv i celých konverzací
- ✓ kopírování zprávy

- ✓ uchování konceptů rozepsaných zpráv
- ✓ vzdálené smazání již odeslané zprávy na zařízení příjemce

Práce s dokumenty a přílohami:

- ✓ vytvoření základních příloh přímo v aplikaci – fotografie, video, zvuková nahrávka
- ✓ bezpečné uložení zašifrovaných přijatých i odeslaných zpráv a dokumentů přímo v aplikaci
- ✓ zobrazení náhledů příloh bez nutnosti stažení příloh
- ✓ zobrazení běžných typů dokumentů přímo v aplikaci, bez uložení rozšifrovaného dokumentu
- ✓ seznam všech odeslaných a přijatých dokumentů, s možností řazení podle různých kritérií

Práce s kontakty:

- ✓ editace kontaktů
- ✓ vizitky – možnost zobrazení a zaslání virtuální vizitky za účelem přidání kontaktu do BabelApp
- ✓ můj profil – editace vlastních informací (jméno, fotografie, generování autorizačních kódů za účelem spárování dalšího zařízení)
- ✓ zobrazení kódů klíčů pro jejich autentizaci s protistranou alternativním způsobem

Ostatní funkce:

- ✓ autentizace a rozšifrování klíče zařízení komplexním heslem při startu aplikace
- ✓ na mobilním zařízení, pokud již BabelApp běží, stačí k odemčení obrazovky zadat PIN, nebo otisk prstu
- ✓ lokalizace – angličtina, čeština, ruština