Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

BRNO • 22. ČERVNA 2026

KOMUNIKAČNÍ APLIKACE S END-TO-END ŠIFROVÁNÍM (E2EE) V ROCE 2026: TRH NABÍZÍ ŠIROKOU ŠKÁLU MOŽNOSTÍ, LIŠÍ SE KOMFORTEM, BEZPEČNOSTÍ A DŮVĚRYHODNOSTÍ PROVOZOVATELE

Komunikátor	Provozovatel	Státní jurisdikce	End-to-end šifrování*	End-to-end šifrování pro skupinové konverzace	Podpora češtiny	Nevyžaduje osobní údaje, email a/nebo telefonní číslo	Zdarma	Lze nastavit aby se zprávy po čase smazaly	Aplikace a/nebo provozovatel nespojen s bezpečnostními incidenty (3)	Multiplatformní (iOS, Mac, PC, Android)
Threema	Threema GmbH	Švýcarsko	✓	✓	✓	✓	✗	– (2)	✓	✓
Signal	Signal Technology Foundation	USA	✓	✓	✓	✗	✓	✓	✓ (4)	✓
Telegram	Telegram Messenger Inc.	Velká Británie/ UAE	– (1)	✗	✓	✗	✓	✓	✗	✓
WhatsApp	Meta (dříve Facebook)	USA	✓	✓	✓	✗	✓	✓	✗	✓
Messenger	Meta (dříve Facebook)	USA	✓	✓	✓	✗	✓	✓	✗	✓
Google messages	Google	USA	✓	✓	✓	✗	✓	✗	✗	✗ (6)
Apple iMessages	Apple	USA	✓	✓	✓	✗	✓	✓	– (5)	✗ (6)

(1) U aplikace Telegram se šifrování musí manuálně aktivovat a je dostupné jen ve speciálních režimech konverzace. K ostatním má provozovatel přístup.
(2) Lze nastavit automatické mazání zpráv po určité době na straně odesílatele.
(3) Viz text níže.
(4) Aplikace Signal je terčem častých útoků a snah o zneužití externími aktéry, dodnes ale neexistují dostupné informace o prolomení zabezpečení samotné komunikace nebo aplikace.
(5) Společnost Apple klade větší důraz na soukromí uživatelů než konkurence, ale její mobilní aplikace byla prolomena např. spywarem Pegasus (viz níže).[1]
(6) Režim E2EE je k datu vydání možný jen v rámci ekosystémů Android a Apple, ale pracuje se na vzájemně kompatibilním standardu.[2]

THREEMA: MAXIMÁLNÍ BEZPEČNOST A SOUKROMÍ ZA CENU PLACENÉ APLIKACE

Šifrovaný messenger Threema staví své renomé na maximálním důrazu na bezpečnost, anonymitě a soukromí. **V současnosti představuje jednu z nejlépe zabezpečených komunikačních aplikací.** Kromě využití end-to-end šifrování (E2EE) na veškeré formy komunikace (tedy i skupinové chaty, soubory, obrázky atd.) **disponuje i možností nastavit si unikátní hesla pro přístup k jednotlivým konverzacím.** [3] Všechna uživatelská data jsou ukládána lokálně v zařízení uživatele a šifrována na úrovni aplikace. [4] Výhodu představuje rovněž i současná švýcarská jurisdikce. [5] **Nejvýznamnější výhodou oproti jiným aplikacím je anonymita. Threema nevyžaduje žádné osobní identifikátory, jako například telefonní číslo nebo e-mailovou adresu.**[6] Uživateli je náhodně vygenerován jeho osobní ID kód, a provozovatel aplikace tak nemá žádné informace o tom, kdo se za daným profilem nachází. **Slabé stránky Threemy spočívají v místy méně intuitivním prostředí, a také faktu, že se jedná o placenou aplikaci.** Threema má tak menší uživatelskou základnu (což ovšem nemusí představovat problém v případě plošného využití v rámci organizace). **Threemu lze pořídit za jednorázový poplatek ve výši 159 Kč.**[7] Ačkoliv to pro některé uživatele může představovat nevýhodu, je třeba brát v potaz, že provozovatel aplikace má díky tomu transparentní zdroje financování. **V současnosti není evidován žádný bezpečnostní incident (zejména prolomení šifrování) jak u aplikace, tak u jejího provozovatele.**

SIGNAL: NEJPOPULÁRNĚJŠÍ BEZPLATNÝ ŠIFROVANÝ KOMUNIKÁTOR NABÍZÍ BEZPEČNOST, ALE MÉNĚ ANONYMITY

Signal je populární chatovací aplikací vyvinutou s důrazem na bezpečnost a end-to-end šifrování. [8] Pomocí E2EE jsou tak zašifrovány všechny formy komunikace. Signal omezuje i množství metadat, ke kterým má provozovatel přístup, a umožňuje nastavení automatického mazání zpráv po určitém časovém úseku. [9] Rovněž klade důraz na open-source přístup a nezávislé prověření, a jeho šifrování je považováno za velmi bezpečné. [10] Všechna uživatelská data jsou ukládána lokálně v zařízení uživatele a šifrována na úrovni aplikace.[11] **Významným nedostatkem je ovšem navázání uživatelského profilu na telefonní číslo.** [12] **Signal proto nelze užívat zcela anonymně a provozovatel má přístup k osobnímu údaji uživatele**. **Přesto je ovšem úroveň bezpečnosti a soukromí této aplikace velmi vysoká.** Signal je provozován neziskovou nadací Signal Foundation, sídlící v USA, jejíž provoz je financován dary jak jednotlivých uživatelů, tak větších investorů.[13] **V současnosti není evidován žádný incident spojený s prolomením aplikace či jejím provozovatelem**. [14] **Renomé aplikace je však často zneužíváno v sociálním inženýrství.**[15] Uživatelé by měli být opatrní především s ověřováním identity účastníků konverzace a zda si člověk stáhl ověřenou aplikaci z oficiálního zdroje. NÚKIB vydal doporučení pro co nejbezpečnější a nejefektivnější používání aplikace Signal.

TELEGRAM: BEZPEČNOSTNÍ PRVKY NIŽŠÍ NEŽ U KONKURENCE A VAZBA NA RUSKO

Telegram je populární zejména v ruskojazyčném prostředí. Jedním z důvodů zájmu o tuto aplikaci je její renomé „bezpečnější alternativy" k WhatsAppu poté, co WhatsApp začal navyšovat sdílení dat se svou mateřskou společností Meta. Vyšší bezpečnost Telegramu je ale sporná, jelikož v otázkách zabezpečení má významné nedostatky**. Jedním z klíčových problémů je absence plošného end-to-end šifrování. Běžné a skupinové konverzace jsou šifrovány až na serveru provozovatele, kde jsou také ukládány.**[16] **Koncově šifrované jsou pouze speciální konverzace mezi dvěma uživateli (funkce Secret Chat).**[17] Jejich data jsou ukládána lokálně, avšak bez zašifrování na úrovni aplikace.[18] **Dalším problémem je užívání vlastního šifrování. Šifrovací protokol MTProto není natolik důvěryhodný jako široce prověřené šifry formátu AES a byly v něm nalezeny zranitelnosti.** [19] Vytvoření profilu Telegram rovněž vyžaduje telefonní číslo uživatele. [20] Problematické je taktéž riziko vazeb na ruskou vládu skrze dodavatelské společnosti s potenciálními vazbami na ruskou rozvědku FSB. [21] Ačkoliv se nemusí jednat o selhání bezpečnosti jako takové, Telegram a jeho uživatelská základna taktéž trpí množstvím falešných účtů a botů s napojením na kyberkriminální aktéry nebo ruské zpravodajské služby.[22] **V případě užívání Telegramu lze proto doporučit zvýšenou ostražitost a nepřipojovat se ke skupinovým konverzacím s neznámými uživateli.**

WHATSAPP A MESSENGER: INTEGRUJÍ E2EE, MAJÍ OVŠEM PŘÍSTUP K VELKÉMU MNOŽSTVÍ OSOBNÍCH DAT

Portfolio komunikačních aplikací společnosti Meta zahrnuje masově rozšířené služby WhatsApp, Messenger a Instagram. **WhatsApp využívá end-to-end šifrování jako výchozí způsob ochrany komunikace.** Uživatelská data jsou ukládána lokálně na zařízení uživatele. V případě platformy Android jsou šifrováním na úrovni aplikace chráněna data textových zpráv, média jsou ukládána otevřeně pro přístup ostatních částí systému.[23] Na platformě iOS jsou šifrována na úrovni systému, který zároveň umožňuje přístup k datům ze strany dalších aplikací společnosti Meta.[24] Zároveň přetrvávají rizika spojená s ochranou soukromí, zejména vazba účtu na telefonní číslo a riziko shromažďování a sdílení metadat o hovorech, zprávách či seznamu kontaktů uložených v zařízení. Tato data nejsou E2EE šifrováním chráněna.[25] **Messenger (včetně zpráv z Facebooku) v minulosti nabízel E2EE pouze v omezeném režimu, nicméně v současnosti je end-to-end šifrování standardně aktivní pro osobní zprávy a hovory.[26]** Tím došlo ke sblížení bezpečnostního modelu s WhatsAppem, avšak i zde platí, že E2EE chrání pouze obsah komunikace, nikoliv metadata a informace vyplývající z provázanosti účtů v rámci ekosystému Meta. Na rozdíl od WhatsAppu jsou uživatelská data uložena na serverech společnosti Meta. **Instagram má vlastní komunikační kanály, ale integrace E2EE v této službě byla v květnu 2026 ukončena.[27] Společnost Meta (dříve Facebook) má problematickou minulost v oblasti ochrany dat a bezpečnosti uživatelů a i přes využití E2EE disponuje velkým množstvím dat o uživatelích, které komerčně využívá pro reklamu a trénink AI.[28]**

GOOGLE MESSAGES A APPLE IMESSAGE: VESTAVĚNÉ APLIKACE CHYTRÝCH TELEFONŮ PŘECHÁZEJÍ NA ŠIFROVANOU KOMUNIKACI

Chytré telefony obsahují základní aplikaci pro posílání zpráv. Ačkoliv tyto aplikace byly dříve primárně určeny pro komunikaci skrze formát SMS, v současné době přecházejí na použití protokolu RCS (Rich Communication Services).[29] **Při komunikaci přes RCS nabízejí telefony jak s iOS, tak s Androidem možnost end-to-end šifrování (RCS musí být povolen v aplikaci a podporován operátorem).[30] Obě výchozí aplikace proto mohou sloužit jako forma bezpečné komunikace, ačkoliv dedikované aplikace s důrazem na soukromí nabízejí lepší služby a komfort.** Obě aplikace umožnují i šifrované skupinové chaty.[31] **E2EE zatím nefunguje napříč mezi uživateli Androidu a iOS, ale kompatibilní protokol je již ve fázi testování.[32]** V obou případech jsou uživatelská data ukládána lokálně v zařízení uživatele a šifrována na úrovni operačního systému. U obou aplikací je pak třeba dbát na to, zda se skutečně jedná o komunikaci skrze protokol RCS či nikoliv, a to mezi všemi členy konverzace, jelikož zprávy formátu SMS pomocí E2EE zabezpečeny nejsou. Ačkoliv je samotný obsah konverzace šifrován, je třeba brát v potaz, že společnosti provozující aplikaci mají přístup k telefonnímu číslu a dalším informacím (např. seznam kontaktů) a mohou shromažďovat metadata. V tomto kontextu je třeba zmínit, že zatímco Apple klade poměrně výrazný důraz na soukromí uživatelů, společnost Google je známá svým obchodním modelem zaměřeným na prodej osobních dat pro reklamní účely (využití konverzací a e-mailů pro trénování AI se ovšem nepotvrdilo).[33]

SOCIÁLNÍ SÍTĚ S INTEGROVANÝMI CHATOVACÍMI SLUŽBAMI: ÚROVEŇ SE LIŠÍ, ZPRAVIDLA VŠAK NEINTEGRUJÍ E2EE A NEJSOU VHODNOU ALTERNATIVOU

Mnoho sociálních sítí a podobných služeb nabízí integrované chatovací služby, přičemž jen některé z nich disponují určitými formami E2EE. Společnost Meta integrovala E2EE do komunikátoru Messenger v rámci své sociální sítě Facebook (viz předchozí kapitola). Sociální sítě Instagram a Threads od stejné společnosti ale žádnou formu E2EE nemají.[34] Chat nyní umožňuje i konkurenční síť X, kde jsou E2EE funkce postupně integrovány.[35] Integrovanou chatovací službou disponuje i největší síť pro sdílení krátkých videí TikTok. **Ta ovšem nemá žádnou formu E2EE a zároveň představuje bezpečnostní hrozbu vyplývající především z množství shromažďovaných dat o uživatelích a způsobu, jakým jsou sbírána a jak je s nimi nakládáno, před čímž NÚKIB i zahraniční partneři dlouhodobě varují.[36]**

Obecně lze říct, že ačkoliv integrované chatovací služby sociálních sítí v posledních době zaznamenaly určitou míru integrace E2EE, není vhodné je používat na citlivou komunikaci. Sociální sítě z principu disponují velkým množstvím informací o uživatelích a jsou obecně problematické z hlediska soukromí. Případná integrace E2EE není v centru jejich zájmu a priorit. Data jsou zároveň ukládána na serverech poskytovatele aplikace, nikoli na zařízení uživatele, což dále snižuje kontrolu uživatele nad svými daty.

PŘÍLOHA 1: IMPLEMENTACE E2EE NA SOCIÁLNÍCH PLATFORMÁCH

Sociální síť	Provozovatel	Státní jurisdikce	Podpora E2EE	E2EE pro skupinové konverzace	Nevyžaduje osobní údaje, email a/nebo telefonní číslo	Lze nastavit aby se zprávy po čase smazaly	Aplikace a/nebo provozovatel nespojen s bezpečnostními incidenty	Služba nemá právo nahlížet do zpráv
Facebook	Meta (dříve Facebook)	USA	✓	✓	✗	✓	✗ (2)	– (5)
Instagram	Meta (dříve Facebook)	USA	✗	✗	✗	✓	✗ (2)	✗ (6)
Threads	Meta (dříve Facebook)	USA	✗	✗	✗	✗	✗ (2)	✗ (6)
X	xAI	USA	– (1)	✗	✗	✓	✗ (3)	✗ (7)
TikTok	ByteDance	Čína	✗	✗	✗	✗	✗ (4)	✗ (8)

(1) Platformy v určité míře E2EE integrovaly, nebo se chystají integrovat, není však dostupné plošně ve všech typech komunikace, ve všech regionech, nebo plně zprovozněno.[37]

(2) Meta za dobu svého působení figurovala v řadě bezpečnostních incidentů a musela zaplatit vysoké pokuty.[38]

(3) Společnost X se stala v roce 2025 terčem útoku, který vedl k masivnímu úniku osobních dat uživatelů jako například e-mailových adres.[39]

(4) TikTok a jeho mateřská společnost ByteDance jsou vysoce rizikové skrze napojení na čínský státní aparát, množství shromažďovaných dat o uživatelích a způsobu, jakým jsou sbírána a jak je s nimi nakládáno, před čímž NÚKIB i zahraniční partneři dlouhodobě varují.[40]

(5) Meta spolupracuje s evropskými a americkými autoritami a na základě legálního požadavku může úřadům poskytnout nešifrovaná data. Facebook ale disponuje plošným E2EE, a Meta by tak ke konverzacím neměla mít přístup.[41]

(6) Meta spolupracuje s evropskými a americkými autoritami a na základě legálního požadavku může úřadům poskytnout nešifrovaná data.[42]

(7) X spolupracuje s autoritami, jak evropskými, tak americkými a na základě legálního požadavku může úřadům poskytnout nešifrovaná data.[43]

(8) TikTok si ve svých licenčních podmínkách vyhrazuje právo nahlížet do zpráv, a to nejen v reakci na požadavky soudního vyšetřování.[44]

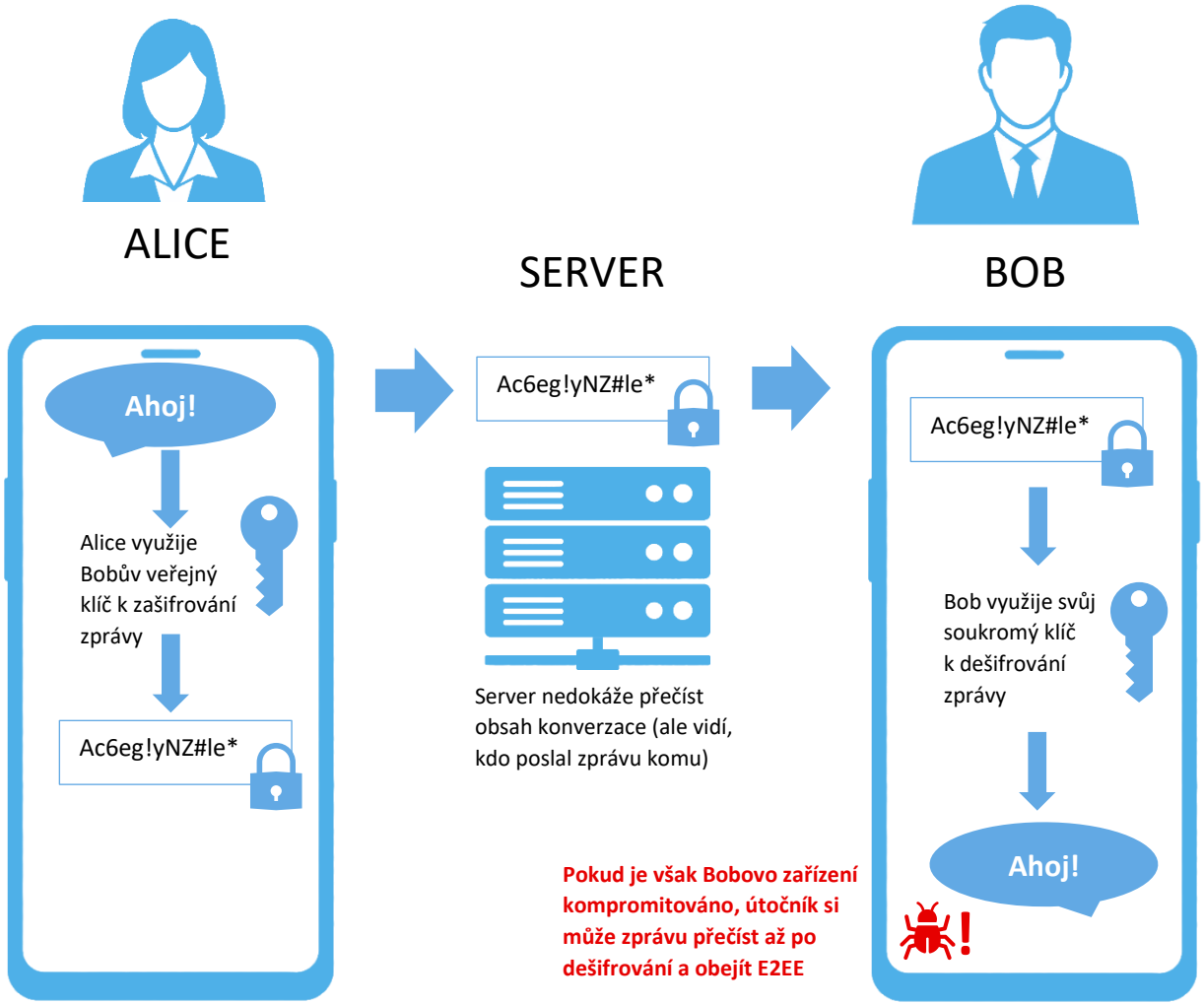
Žádná ze sociálních platforem podle dostupných informací nepoužívá obsah soukromých zpráv pro trénování AI, s výjimkou chatů s umělou inteligencí.

PŘÍLOHA 2: E2EE OCHRÁNÍ OBSAH ZPRÁVY BĚHEM PŘENOSU MEZI ODESÍLATELEM A PŘÍJEMCEM, NENÍ VŠAK ZÁRUKOU ZCELA BEZPEČNÉ KOMUNIKACE

End-to-end encryption (E2EE) je způsob zabezpečení komunikace, při kterém je obsah zprávy **šifrován už na zařízení odesílatele** a **dešifrován až na zařízení příjemce**. Po celou dobu přenosu (včetně průchodu servery poskytovatele služby) zůstává zpráva v nečitelné podobě.

Každý účastník komunikace má vlastní kryptografické klíče. Veřejná část klíče slouží k zašifrování zprávy, zatímco soukromá část, uložená pouze v zařízení příjemce, umožňuje její dešifrování. Poskytovatel služby k těmto soukromým klíčům nemá přístup, a technicky tedy není schopen obsah komunikace číst.

E2EE však nechrání tzv. metadata (např. kdo s kým a kdy komunikuje) a především nezajišťuje bezpečnost dat po jejich uložení na zařízení uživatele. V případě, že je koncové zařízení kompromitováno, je ochrana pomocí E2EE irelevantní. Jako příklad lze uvést spyware Pegasus. Ačkoliv je téměř jisté (90–100 %), že nedokáže prolomit E2EE komunikaci, dokáže kompromitovat zařízení jinými vektory a následně se dostat k výsledné dešifrované konverzaci. **Zásadní je proto také ochrana lokálních dat (viz níže).**



PŘÍLOHA 3: PŘEHLED PŘÍSTUPŮ KOMUNIKAČNÍCH PLATFOREM K UKLÁDÁNÍ A ŠIFROVÁNÍ DAT

Komunikátor	Provozovatel	End-to-end šifrování	Místo uložení uživatelských dat	Šifrování lokálních dat
Threema	Threema GmbH, Švýcarsko	ANO	Zařízení uživatele	ANO, na úrovni aplikace
Signal	Signal Technology Foundation, USA	ANO	Zařízení uživatele	ANO, na úrovni aplikace
Telegram	Telegram Messenger Inc., Velká Británie/SAE	jen u speciálních chatů, nutná manuální aktivace	Servery provozovatele služby pro běžné chaty, zařízení uživatele pro speciální chaty	ANO, na úrovni operačního systému
WhatsApp	Meta (dříve Facebook), USA	ANO	Zařízení uživatele	ANO, způsob se ale liší dle operačního systému (3)
Messenger	Meta (dříve Facebook), USA	ANO	Servery provozovatele služby	Data jsou uložena na serverech provozovatele služby
Google Messages	Google, USA	ANO, při využití RCS (1)	Zařízení uživatele	ANO, na úrovni operačního systému
Apple iMessages	Apple, USA	ANO (2)	Zařízení uživatele	ANO, na úrovni operačního systému
Komunikátory integrované v rámci sociálních sítí (Instagram, TikTok, X…)	Různí	zpravidla NE	Servery provozovatele služby	Data jsou uložena na serverech provozovatele služby

(1) Protokol RCS (Rich Communication Services) slouží pro zasílání zpráv přes internetový protokol. RCS musí být povolen v aplikaci a podporován operátorem. Pokud aplikace přijímají klasické SMS, komunikace probíhá nezašifrovaně přes telefonní síť.

(2) Pouze při dostupném internetovém připojení. Bez internetového připojení aplikace zasílá klasické SMS. Při komunikaci se zařízením s Androidem jsou zprávy koncově šifrovány pouze při využití RCS.

(3) Na platformě Android jsou na úrovni aplikace šifrovány textové zprávy. Média (fotografie, videa) jsou šifrována na úrovni operačního systému. V případě iOS jsou na úrovní operačního systému šifrována všechna uživatelská data.

NEZBYTNÁ JE I OCHRANA ULOŽENÝCH DAT. PŘÍSTUP JEDNOTLIVÝCH KOMUNIKAČNÍCH PLATFOREM K ZAJIŠTĚNÍ JEJICH DŮVĚRNOSTI SE PŘITOM VÝRAZNĚ LIŠÍ

Chránit data je nutné jak při jejich přenosu (data in transit), tak i na místě jejich uložení (data at rest). Zatímco ochranu dat během přenosu pomocí koncového šifrování provozovatelé komunikačních platforem velmi aktivně prezentují, způsob ochrany uložených dat je často opomíjen. Data mohou být uložena na serverech provozovatele služby, anebo lokálně v zařízení uživatele.

Lokálně v zařízení uživatele data ukládá Threema, Signal, WhatsApp, Google Messages, Apple iMessage a v případě využití Secret Chats také Telegram. Na serverech provozovatele služby jsou ukládána data aplikace Messenger, dalších komunikátorů integrovaných v sociálních sítích a také data běžných chatů platformy Telegram. S výjimkou Messengeru, který data šifruje koncově, jsou uložená data šifrována až na úrovni serveru a chráněna v případě jejich úniku. Provozovateli platformy je ale obsah dat dostupný.

LOKÁLNÍ DATA CHRÁNÍ ŠIFROVÁNÍ NA ÚROVNI OPERAČNÍHO SYSTÉMU ČI APLIKACE

Šifrování lokálních dat na zařízení uživatele může probíhat dvěma způsoby: na úrovni aplikace či na úrovni operačního systému. Jak iOS, tak Android defaultně šifrují veškerá data uložená na mobilním zařízení. Data komunikační aplikace jsou tak stejně bezpečná jako samotná mobilní platforma, respektive samotné zařízení. V případě šifrování na úrovni aplikace je přidána ještě jedna bezpečnostní vrstva, která má data aplikace zároveň chránit i před samotným operačním systémem.

Šifrování na úrovni aplikace využívá Threema, Signal a také WhatsApp na platformě Android, avšak pouze pro textové zprávy. Média (fotografie, videa) jsou ukládána separátně a spoléhají na šifrování na úrovni operačního systému**. Na platformách iOS a macOS WhatsApp spoléhá na šifrování na úrovni operačního systému pro všechny typy uživatelských dat.** Šifrování na úrovni operačního systému využívají i Google Messages, Apple iMessage a Secret Chats platformy Telegram.

TECHNICKY NEJROBUSTNĚJŠÍ ZPŮSOB OCHRANY DAT NABÍZÍ THREEMA A SIGNAL. ZÁSADNÍ JE ALE TAKÉ DŮVĚRYHODNOST PROVOZOVATELE

Technicky nejrobustnější řešení k zajištění důvěrnosti uživatelských dat představuje kombinace nasazení koncového šifrování, lokálního ukládání dat na zařízení uživatele a jejich šifrování na úrovni aplikace. Tyto přístupy využívají aplikace Threema a Signal.

Zajištění důvěrnosti uživatelských dat před samotným provozovatelem aplikace či operačního systému není však pouze technickou otázkou. Jelikož operační systém obsah konverzací uživateli zobrazuje, nelze zajistit, aby k nim žádný přístup neměl. Stejně tak existuje řada způsobů, jak může obsah uživatelských dat získat provozovatel aplikace, ať už před či po jejich koncovém zašifrování. Případné narušení důvěrnosti je zároveň velmi náročné prokázat. **Zásadní je proto i důvěryhodnost provozovatele aplikace a operačního systému.**

ARCHITEKTURA APLIKACE WHATSAPP NA PLATFORMĚ IOS A MACOS MŮŽE USNADNIT OBEJITÍ KONCOVÉHO ŠIFROVÁNÍ ZE STRANY SPOLEČNOSTI META

Přístup komunikační aplikace WhatsApp k ukládání a šifrování uživatelských dat se liší dle operačního systému. **Zatímco na platformě Android aplikace používá šifrování na úrovni aplikace, na iOS a macOS využívá šifrování na úrovni operačního systému.** WhatsApp se zároveň opírá o architekturu tzv. kontejnerů, ve kterých jednotlivé aplikace na operačních systémech od společnosti Apple fungují izolovaně. **V tomto případě aplikace WhatsApp sdílí kontejner s dalšími aplikacemi od společnosti Meta (zejména Facebook a Instagram), přičemž operační systém umožnuje aplikacím v rámci stejného kontejneru k datům vzájemně přistupovat.**

Společnost Meta by tímto způsobem mohla číst obsah uživatelských dat aplikace WhatsApp, ačkoli jsou data koncově šifrovaná, a tedy pro provozovatele služby během přenosu nečitelná. Přestože nejsou dostupné žádné důkazy, že by Meta tento přístup aktivně zneužívala, architektura vyvolává oprávněné obavy o izolaci uživatelských dat.

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP:RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP:AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Oranžová **TLP:AMBER**	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Zelená **TLP:GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP:CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

PRAVDĚPODOBNOSTNÍ VÝRAZY NÚKIB

Výraz	Pravděpodobnost
Téměř jistě	*90–100 %*
Velmi pravděpodobně	*75–85 %*
Pravděpodobně	*55–70 %*
Nelze vyloučit/Reálná možnost	*40–50 %*
Nepravděpodobně	*20–35 %*
Velmi nepravděpodobně	*0–15 %*

ZDROJE

[1] Marczak, B., J. Scott-Railton, B. Abdul Razzak, N. Al-Jizawi, S. Anstis, K. Berdan a R. Deibert. The Citizen Lab. 2021. FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild. FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild - The Citizen Lab

[2] Weatherbed, J. The Verge. 2025. Apple Will Soon Support Encrypted RCS Messaging with Android Users. https://www.theverge.com/news/629620/apple-iphone-e2ee-encryption-rcs-messaging-android

[3] Threema. 2026. What Are Private Chats and How Can I Use Them? What are private chats and how can I use them? - Threema

[4] Threema. 2026. Cryptography Whitepaper. Cryptography Whitepaper

[5] Všechna data jsou chráněna legislativou "ustanovení o ochraně dat švýcarskou vládou" (DPA) a "nařízení o ochraně dat švýcarskou vládou" (DPO), která nabízí jednu z nejsilnějších ochran soukromí na světě. DLA Piper. Data Protection Laws of the World. 2025. Data Protection Laws in Switzerland. Data protection laws in Switzerland - Data Protection Laws of the World

[6] Taylor, S. Restore Privacy. 2025. Threema Review 2026: Secure Messenger with Drawbacks. Threema Review 2026: Secure Messenger with Drawbacks (restoreprivacy.com)

[7] Threema. 2026. Google Play. Threema – Aplikace na Google Play

[8] Curry, D. Business of Apps. 2026. Signal Revenue & Usage Statistics (2026). Signal Revenue & Usage Statistics (2026) - Business of Apps

[9] Signal Support. 2026. Group Calling. Group Calling - Voice or Video with Screen Sharing – Signal Support

[10] Mann, D. 2025. Signal Review 2026: Secure Messenger (Pros and Cons). Signal Review 2026: Secure Messenger (Pros and Cons)

[11] Deepwiki. 2026. Signal (Android) Database System | signalapp/Signal-Android | DeepWiki
Deepwiki. 2026. Signal (iOS) Database & Storage | signalapp/Signal-iOS | DeepWiki
Deepwiki. 2026. Cryptography. Cryptography | carderne/signal-export | DeepWiki

[12] Signal. 2026. Why a Phone Number Is Necessary to Register at Signal. Why a phone number is necessary to register at Signal

[13] Viktor, V. Productmint. 2022. The Signal Business Model – How Does Signal Make Money? The Signal Business Model – How Does Signal Make Money? (productmint.com)

[14] Kauzy spojené s aplikací Signal doposud stály na podvržené aplikaci, která se za Signal vydávala, přidání špatného člověka do konverzace nebo jiné phishingové metody. Nejsou známy informace, že by došlo k prolomení E2EE nebo úniku citlivých dat ze Signal Foundation.

[15] Black, D. Google Blog. 2025. Signals of Trouble: Multiple Russia-Aligned Threat Actors Actively Targeting Signal Messenger. Signals of Trouble: Multiple Russia-Aligned Threat Actors Actively Targeting Signal Messenger | Google Cloud Blog

[16] Gozman, S. IEEE Spectrum. 2024. The Trouble With Telegram: The Platform May Not Be as Secure as It Claims to Be. Telegram May Not be as Secure as it Claims - IEEE Spectrum

[17] Gorman, B. Avast. 2024. Is Telegram a Safe and Secure Messaging App? Is Telegram a Safe and Secure Messaging App?

[18] Fortuna, A. 2026. Telegram Evidence Beyond the Cloud. Telegram evidence beyond the cloud | Andrea Fortuna

[19] Ibidem

[20] Gorman, B. Avast. 2024. Is Telegram a Safe and Secure Messaging App? Is Telegram a Safe and Secure Messaging App?

[21] Anin, R., Kondratyev, N. iStories. 2025. Telegram, the FSB, and the Man in the Middle. Telegram, the FSB, and the Man in the Middle

[22] Brešťan, R. HlídacíPes.org. 2025. Ruský nábor sabotérů probíhá i v Česku. „Selský rozum“ na Telegramu užívá ruská rozvědka. Ruský nábor sabotérů probíhá i v Česku. „Selský rozum“ na Telegramu užívá ruská rozvědka — HlídacíPes.org

[23] Digital Forensics Today. 2026. WhatsApp Forensics — Messages, Media, and the Encryption Challenge. WhatsApp Forensics — Messages, Media, and the Encryption Challenge — Digital Forensics Today

[24] Cyber Security News. 2026. WhatsApp Chat Histories Stored Unencrypted on macOS and iOS. WhatsApp Chat Histories Stored Unencrypted on macOS and iOS

[25] Doffman, Z. Forbes. 2026. Not Secure—Do You Suddenly Need To Stop Using WhatsApp On Your Phone? ‘Not Secure’—Do You Suddenly Need To Stop Using WhatsApp?

[26] How-To Geek. 2023. Facebook Messenger Now Uses End-to-End Encryption by Default. Facebook Messenger Now Uses End-to-End Encryption by Default

[27] Cyber Security News. 2026. Meta to Permanently Remove End-to-End Encryption Feature in Instagram DMs. Meta to Permanently Remove End-to-End Encryption Feature in Instagram DMs
[28] Fernando, J. Investopedia. 2026. Cambridge Analytica: Overview, History, and Example. Cambridge Analytica: Overview, History, and Example, Meta nepoužívá k tréningu dat osobní konverzace, ale veškerý veřejný obsah na jejich sociálních sítích a konverzace s Meta chatbotem. Viz Crissy, J. Norton. 2025. How to Opt Out of Meta AI: Options to Protect Your Data. How to opt out of Meta AI: Options to protect your data
[29] Dove, J. Digital Trends. 2021. What Is RCS Messaging? Everything You Need to Know About the SMS Successor. What Is RCS Messaging, and Exactly How Does It Work? | Digital Trends
[30] Privacy. 2025. Apple. Privacy - Features - Apple,
[31] Sorrentino, M. CNET. 2025. iPhone or Android, Here's How to Finally Escape That Endless Group Chat. iPhone or Android, Here's How to Finally Escape That Endless Group Chat - CNET
[32] Mehrotra, D., Greenberg, A. Wired. 2025. Security News This Week: End-to-End Encrypted Texts Between Android and iPhone Are Coming. End-to-End Encrypted Texts Between Android and iPhone Are Coming | WIRED
[33] Arntz, P. Malwarebytes. 2025. [Correction] Gmail Can Read Your Emails and Attachments to Power “Smart Features”. [Correction] Gmail can read your emails and attachments to power "smart features" | Malwarebytes
[34] Fernando, J. Investopedia. 2025. Cambridge Analytica: Overview, History, and Example. Meta's Threads Now Has DMs - Business Insider
[35] Karissa, L. Engadget. 2025. X Is Finally Rolling Out Chat, Its DM Replacement with Encryption and Video Calling. X is finally rolling out Chat, its DM replacement with encryption and video calling
[36] Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). 2023. Varování 2236/2023-NÚKIB-E/350.. 2023-03-08_Varovani-TikTok_final.pdf, Cabinet Office a Dowden, O. UK Government. 2023. TikTok Banned on UK Government Devices as Part of Wider App Review. https://www.gov.uk/government/news/tiktok-banned-on-uk-government-devices-as-part-of-wider-app-review
[37] Aplikace Instagram v současnosti v ČR E2EE nepodporuje. X postupně integruje E2EE, ale v rámci tohoto procesu ještě podle dostupných informací neintegrovala všechny potřebné bezpečnostní prvky. Viz: Lorenzo, F. TechCrunch. 2025. X Is Now Offering Me End-to-End Encrypted Chat — You Probably Shouldn’t Trust It Yet. X is now offering me end-to-end encrypted chat — you probably shouldn't trust it yet | TechCrunch
[38] BBC News. 2024. Facebook Parent Company Fined €91m over Password Storage. https://www.bbc.com/news/articles/cvgl8lerx85o
[39] Binder, M. Mashable. 2025. Massive Breach of Elon Musk’s X Allegedly Leaks over 200 Million Users’ Email Addresses. https://mashable.com/article/elon-musk-x-twitter-breach-data-leak-breachforums
[40] Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). 2023. Varování 2236/2023-NÚKIB-E/350. 2023-03-08_Varovani-TikTok_final.pdf
[41] Meta Platforms, Inc. Meta Safety Center. 2026. Information for Law Enforcement Authorities. https://www.meta.com/safety/communities/law/guidelines/
[42] Meta Platforms, Inc. Meta Safety Center. 2026. Information for Law Enforcement Authorities. https://www.meta.com/safety/communities/law/guidelines/
[43] X Corp. X Help Center. 2026. Guidelines for Law Enforcement. https://help.x.com/en/rules-and-policies/x-law-enforcement-support
[44] TikTok. 2026. Privacy Policy. Privacy Policy | TikTok, McGowan, E. Norton. 2025. Is TikTok Safe? Risks You Should Be Aware Of. Is TikTok safe? Risks you should be aware of