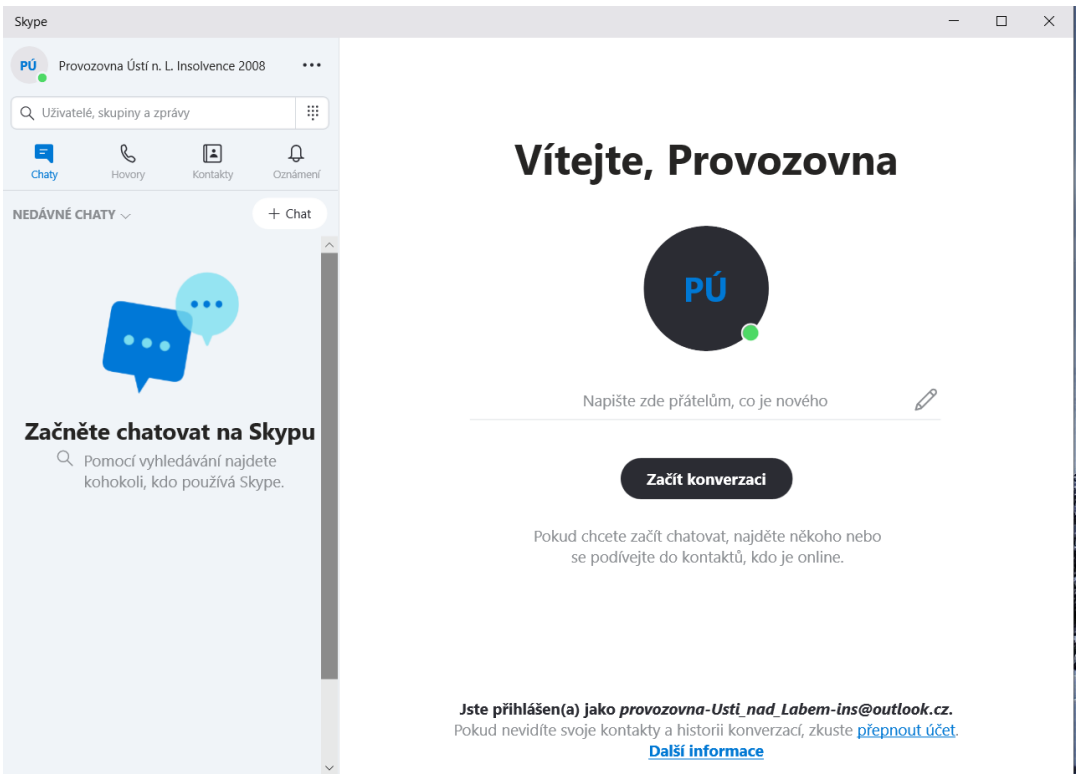
ZABEZPEČENÁ KOMUNIKACE MEZI PROVOZOVNOU A SPRÁVCEM

Microsoft Skype umožnuje použít komunikaci šifrovanou tzv. end-to-end. Ta zajistí, že si Vaše zprávy nepřečte ani poskytovatel služby.

Šifrování se vztahuje na **textové zprávy, audiohovory, videohovory** a také **odeslané soubory**. Microsoft využil všeobecně uznávaný protokol **Signal,** který můžeme považovat za standard v oblasti šifrování komunikace.

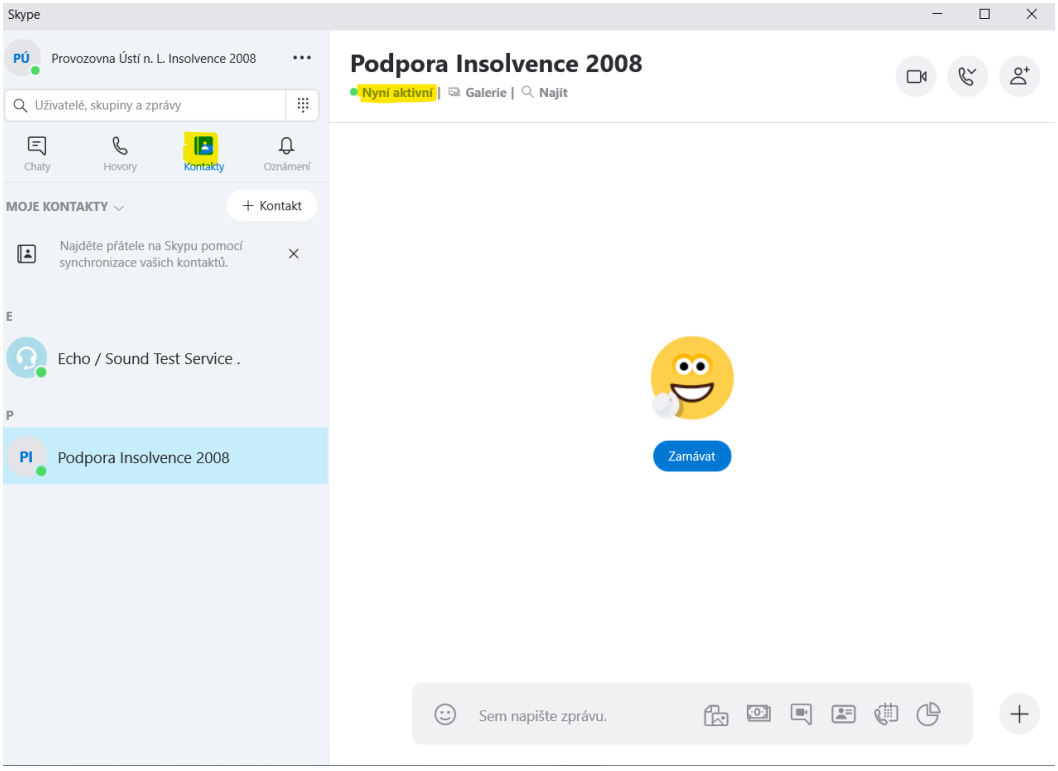
Tento režim provozu nazývá **Soukromá konverzace**

Úvodní obrazovka Skype

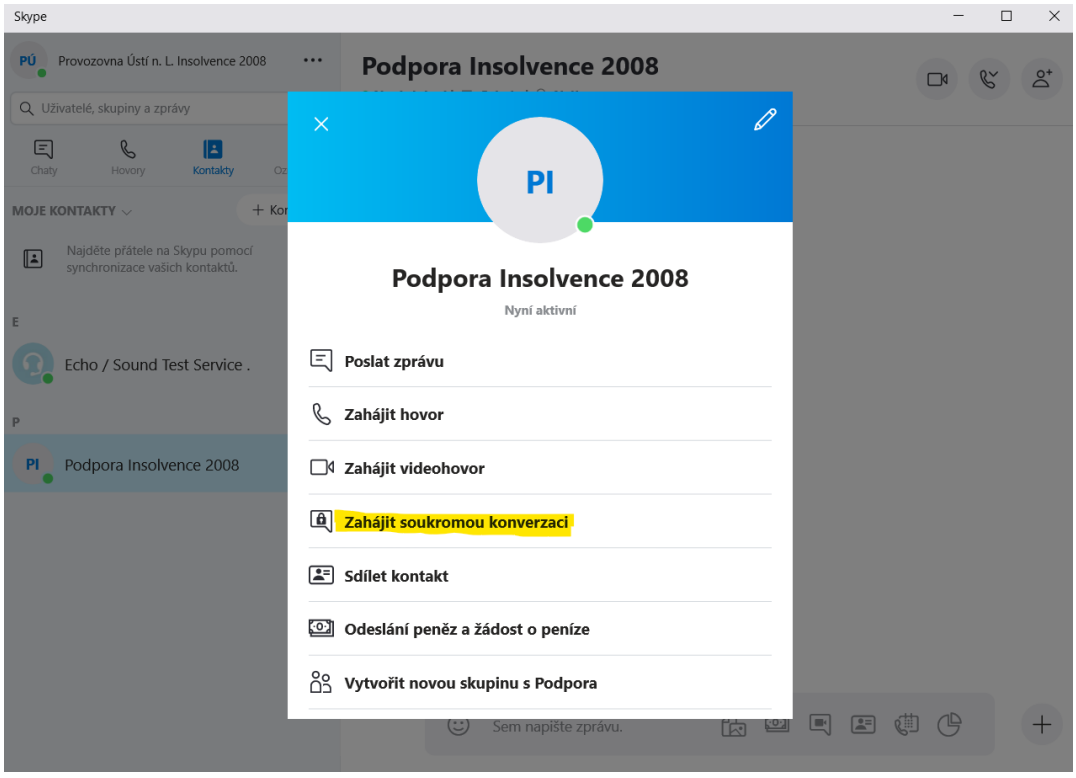


Postup vedení konverzace

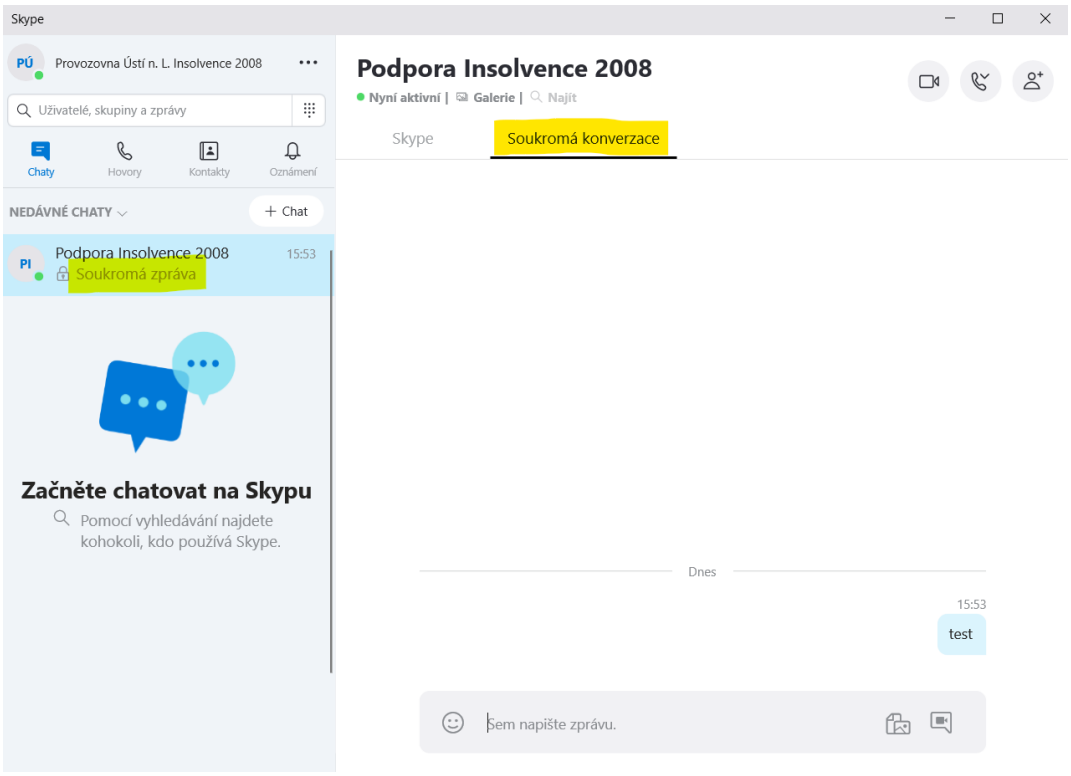
Kliknutím na Kontakty a status Nyní aktivní …



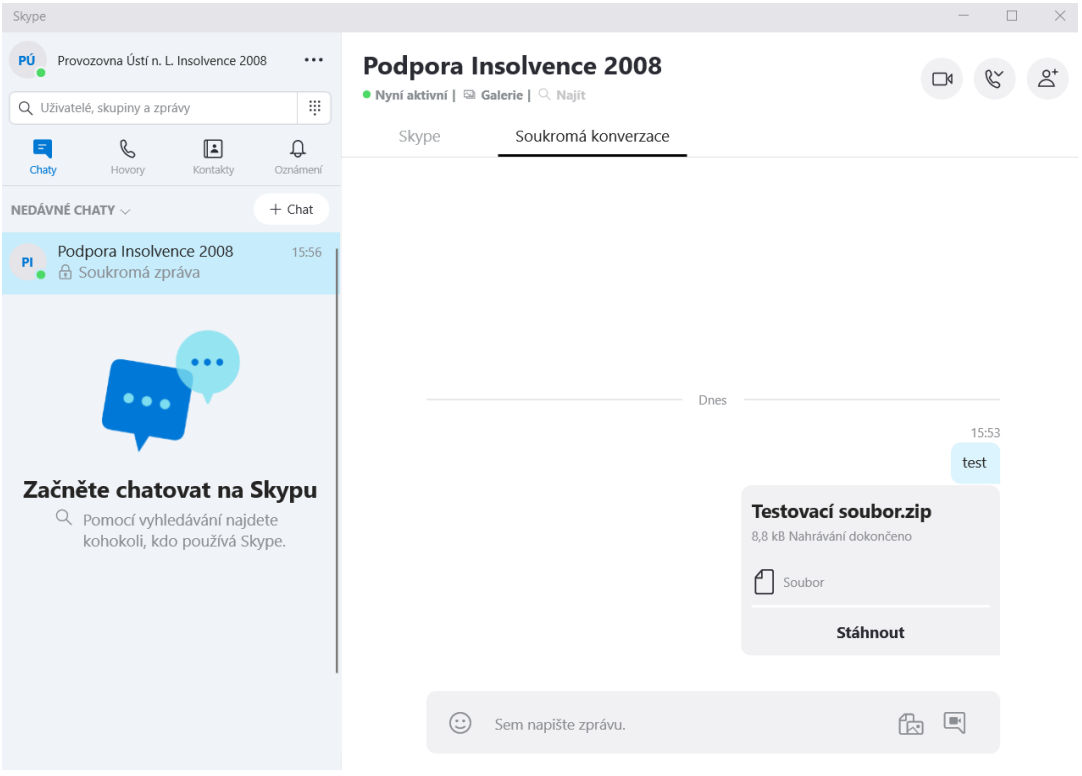
Vyvoláme možnost Soukromé konverzace



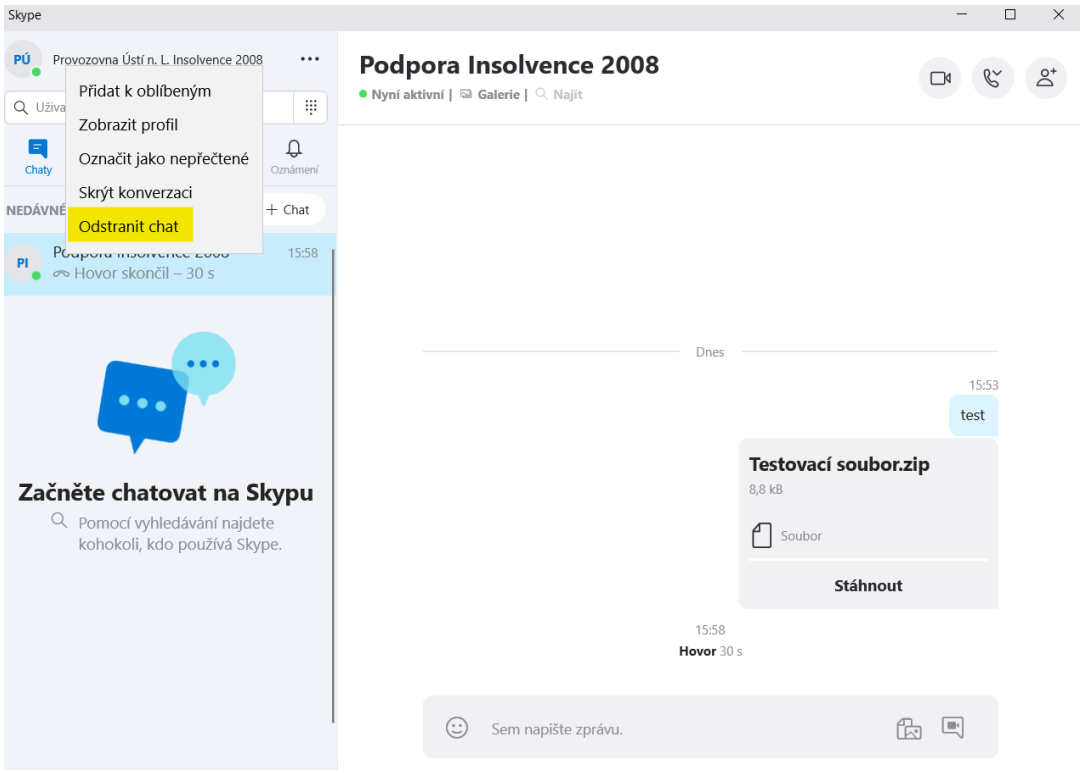
Soukromá konverzace je pevně spojena s daným zařízením. Oproti běžnému chatu si tak zprávy z této konverzaci neleze přečíst na dalších zařízeních.



Soukromá konverzace umožnuje mimo jiné posílat bezpečné soubory, prostým přetažením daného souboru do okna.



Po skončení konverzace smažeme bezpečně obsah komunikace



Co je End-to-end šifrování (End-to-End encryption)?

End-to-end šifrování je způsob ochrany komunikace před třetí stranou, např. před odposlechem. Takto zašifrovaná komunikace probíhající mezi dvěma stranami (odesílatel a příjemce) je čitelná pouze pro tyto dvě strany.

Ke zprávám nemá přístup ani útočník (ten, kdo by chtěl odposlouchávat), ale ani poskytovatel služby (například chatovacího programu, messengerového systému a podobně). End-to-end šifrování přináší bezpečnost, ale zároveň klade větší nároky na koncová zařízení, jelikož šifrování a dešifrování vyžaduje určitou výpočetní kapacitu těchto zařízení (mohou také například spotřebovávat více baterie). Zařízení, která obsahují end-to-end šifrování, jsou také zpravidla dražší.

Kde a jak se end-to-end šifrování používá?

Je důležité pro všechny firmy, které chtějí chránit své citlivé a důvěrné informace před konkurencí nebo chtějí chránit osobní údaje z důvodu, že jim to nařizuje legislativa (např. HIPAA, GDPR atp.). End-to-end šifrování také umožní zamezit odposlechu nebo útokům typu MITM (man in the middle).

End-to-end šifrování představuje nejbezpečnější způsob komunikace, ke které mají přístup pouze komunikující strany. Ani poskytovatel služby nemůže do komunikace zasahovat ani ji poskytovat například vyšetřovacím orgánům. Kryptografické klíče totiž drží pouze koncová zařízení a nikdo jiný. Můžou tak být zabezpečeny různé fromy komunikace:

Co je protokol Signal?

Signální protokol (dříve známý jako protokol TextSecure) je nefederovaný kryptografický protokol, který lze použít k poskytování šifrování mezi koncovými body pro hlasová volání, videohovory, hovory [3] a konverzace v režimu rychlých zpráv [2]. Protokol byl vyvinut Open Whisper Systems v roce 2013 [2] a byl poprvé představen v open-source aplikaci TextSecure, která se později stala Signal. Několik aplikací s uzavřeným zdrojem tvrdí, že implementovali protokol, jako je WhatsApp, který má podle něj šifrovat konverzace "více než miliardy lidí na celém světě".Facebook Messenger také říká, že nabízí protokol pro volitelné tajné konverzace, stejně jako Skype pro své soukromé konverzace.

Protokol kombinuje algoritmus Double Ratchet, prekeys a trojnásobnou eliptickou křivku Diffie – Hellman (3-DH) handshake a používá Curve25519, AES-256 a HMAC-SHA256 jako primitivy.

Použité zdroje:

https://www.cnews.cz/skype-2018-end-to-end-sifrovani-zavedeno/

https://en.wikipedia.org/wiki/Signal_Protocol

https://managementmania.com/cs/end-to-end-sifrovani-end-to-end-encryption