

Ukončení podpory zastaralé šifrovací sady

Informace k ukončení podpory zastaralé šifrovací sady

Uživatelům, kteří pro přístup do datové schránky stále používají starší zabezpečení, které přestane být podporováno (nazvané **TLS_DHE_RSA_WITH_AES_256_GCM_SHA384**), byla rozeslána datová zpráva s urgencí a informací, že **podpora této šifrovací sady bude definitivně vypnuta 30. června 2025.**

Pro tyto uživatele to znamená, že pokud neaktualizují software nebo operační systém zařízení, kterým přistupují do své datové schránky, může se stát, **že po tomto datu nebudou moci datovou schránku používat z tohoto zařízení.**

Tato změna je nutná, protože neaktualizovaný software přináší zvýšené riziko napadení, zneužití nebo znepřístupnění systému Vašich datových schránek. Ukončení podpory zastaralé šifrovací sady je v souladu a doporučení Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB).

Nejčastějším důvodem použití zastaralé šifrovací sady je běh aplikace na zastaralém, již nepodporovaném operačním systému, případně použití zastaralé komunikační infrastruktury. **Doporučujeme** Vám obrátit se na svého dodavatele spisové služby či jiné aplikace, kterou používáte, s žádostí o **aktualizaci programového vybavení.**

Pokud pro přístup do datové schránky používáte klientský portál na adrese www.mojedatovaschranka.cz, doporučujeme také používat aktuální verze operačních systémů a internetových prohlížečů.

Aktuálně podporované šifrovací sady v prostředí ISDS jsou uvedeny na stránce <https://info.mojedatovaschranka.cz/info/cs/79.html>.

V případě potřeby dalších informací se můžete elektronicky dotázat na **ePoradnu** datových schránek <https://info.mojedatovaschranka.cz/info/cs/eporadna.html> nebo v případě řešení konkrétního problému s datovou schránkou volat infolinku datových schránek, tel.: 954 200 200, PO-PÁ 8-18 h.