Co je SSH klíč

Poslední aktualizace 10 března, 2026

SSH klíč SSH key) je kryptografický nástroj používaný pro bezpečné přihlašování k serveru pomocí protokolu SSH. Nahrazuje klasické přihlašování heslem a výrazně zvyšuje úroveň zabezpečení vzdáleného přístupu. SSH klíč funguje na principu asymetrické kryptografie – používá dvojici propojených klíčů.

Jak SSH klíč funguje

SSH autentizace pracuje se dvěma částmi:

- **Soukromý klíč (private key) –** zůstává uložený u uživatele a nikdy se nesdílí
- **Veřejný klíč (public key) –** nahraje se na server

Při připojení server ověří, zda uživatel vlastní odpovídající soukromý klíč. Pokud ano, přístup je povolen bez nutnosti zadávat heslo. Tento mechanismus minimalizuje riziko prolomení účtu prostřednictvím brute force attack.