Jak vygenerovat SSH klíč

Poslední aktualizace 23 října, 2026

SSH klíč vám umožní přihlašovat se na server bezpečněji a pohodlněji než heslem. V tomto návodu si ukážeme, jaký typ klíče zvolit, jak ho vygenerovat na Linuxu, macOS i Windows a kam veřejnou část klíče nahrát u VPS a webhostingu Webglobe.

Proč se přihlašovat SSH klíčem místo hesla

SSH klíč tvoří dvojice souborů: privátní klíč, který zůstává jen ve vašem počítači, a veřejný klíč, který nahrajete na server. Při přihlášení váš počítač privátním klíčem podepíše data jedinečná pro dané spojení a server podpis ověří pomocí uloženého veřejného klíče. Privátní klíč ani heslo přitom po síti nikdy neputují.

Oproti heslu má přihlášení klíčem tyto výhody:

- **vyšší bezpečnost**: heslo lze uhodnout nebo prolomit pomocí brute force attack, privátní klíč prakticky ne,
- **pohodlí**: klíč nastavíte jednou a pak se přihlašujete bez zadávání hesla, třeba i automaticky ve skriptech nebo při zálohách,
- **ochrana před phishingem**: nemáte heslo, které byste mohli omylem vyplnit na podvodné stránce.

  Klíč můžete chránit vlastním heslem (tzv. passphrase). To se ověřuje jen u vás v počítači a po internetu se nikdy neposílá.

Jaký typ SSH klíče zvolit

Pro většinu uživatelů je nejlepší volbou **Ed25519**. Při generování se můžete setkat se třemi algoritmy:

Algoritmus	Doporučení	Hlavní vlastnosti
Ed25519	Doporučeno	Moderní, rychlý, krátký klíč s bezpečností srovnatelnou s RSA 3072. Podporovaný od OpenSSH 6.5 (2014).
RSA	Jen pro starší systémy	Nejrozšířenější, pro

		dostatečnou bezpečnost potřebuje délku alespoň 3072 bitů, ideálně 4096 bitů.
DSA	Nepoužívat	Zastaralý. OpenSSH ho od verze 7.0 (2015) ve výchozím nastavení blokuje a ve verzi 10.0 (2025) jeho podporu odstranilo.

Ed25519 má navíc deterministický podpis, takže nehrozí únik klíče kvůli chybnému generátoru náhodných čísel. Pokud se připojujete ke staršímu systému, který Ed25519 nepodporuje, vygenerujte klíč RSA příkazem:

```
ssh-keygen -t rsa -b 4096 -C "vas@email.cz"
```

Jak vygenerovat SSH klíč na Linuxu a macOS

1. Otevřete **Terminal** a zadejte příkaz ssh-keygen -t ed25519 -C „vas@email.cz“.
2. Parametr **-C** je jen komentář, podle kterého klíč později poznáte. Nejčastěji se používá e-mail nebo název počítače.
3. Umístění souboru potvrďte klávesou **ENTER**. Klíč se uloží do výchozí složky **~/.ssh/**.
4. Zadejte passphrase a potvrďte ji. Doporučujeme ji nastavit, protože klíč ochrání i v případě, že by se k němu dostal někdo cizí.

Příkaz vytvoří dva soubory:

- **id_ed25519**: privátní klíč, který nesmí nikdy opustit váš počítač,
- **id_ed25519.pub**: veřejný klíč, který nahrajete na server.

Obsah veřejného klíče si zobrazíte příkazem:

```
cat ~/.ssh/id_ed25519.pub
```

Jak vygenerovat SSH klíč na Windows

Přes PowerShell

Windows 10 a 11 mají klienta OpenSSH přímo v systému, takže postup je stejný jako na Linuxu.

1. Otevřete **PowerShell** a zadejte příkaz ssh-keygen -t ed25519 -C „vas@email.cz“.
2. Potvrďte výchozí umístění a nastavte passphrase.

Klíče se uloží do složky **C:\Users\VašeJméno\.ssh**. Veřejný klíč si zobrazíte příkazem:

```
type $env:USERPROFILE\.ssh\id_ed25519.pub
```

Přes PuTTYgen

Pokud se připojujete přes klienta PuTTY, vytvořte klíč v nástroji PuTTYgen, který je jeho součástí.

1. Spusťte PuTTYgen a jako typ klíče zvolte **EdDSA** s variantou **Ed25519**.
2. Klikněte na **Generate** a pohybujte myší v prázdném poli, dokud se klíč nevygeneruje.
3. Vyplňte **Key passphrase** a **Confirm passphrase**.
4. Privátní klíč uložte tlačítkem **Save private key**. Vznikne soubor s příponou .ppk.
5. Veřejný klíč zkopírujte z pole **Public key for pasting into OpenSSH authorized_keys file**.

   *Soubor .ppk funguje jen v PuTTY. Pokud chcete klíč používat i s klientem OpenSSH, převeďte ho v PuTTYgen přes **Conversions → Export OpenSSH key**.*

Kam nahrát veřejný SSH klíč

Na server vkládejte vždy jen veřejný klíč, tedy obsah souboru s příponou .pub. Jde o jeden řádek, který začíná **ssh-ed25519** (nebo **ssh-rsa**).

VPS

U předinstalovaných aplikací WebApps server, MongoDB, Redis, Node.js a NextCloud se k VPS přihlásíte **pouze pomocí SSH klíče**. Veřejný klíč vložíte takto:

1. Přihlaste se do WebAdminu.
2. Otevřete detail svého VPS.
3. Přejděte do záložky **Správa serveru → SSH klíče** a vložte veřejný klíč.

U vlastních instalací operačních systémů se nejprve připojte k serveru přes konzoli ve VPS adminu nebo přes VNC (postup najdete v článku Vzdálený přístup k serveru s Linuxem). Veřejný klíč pak vložte na samostatný řádek do souboru **~/.ssh/authorized_keys** uživatele, za kterého se budete přihlašovat. Soubor musí mít oprávnění 600 a složka .ssh oprávnění 700.

Pokud se na server zatím přihlašujete heslem, můžete klíč nahrát ze svého počítače jedním příkazem:

```
ssh-copy-id -i ~/.ssh/id_ed25519.pub uzivatel@IP_SERVERU
```

Webhosting

U webhostingu vložte veřejný klíč do souboru **.ssh/authorized_keys** ve svém hostingu. Nejjednodušeji to uděláte přes webovou SSH konzoli, kterou spustíte ve WebAdminu v menu **Hosting → FTP soubory → WebSSH**.

Pro aktivaci SSH konzole musíte mít u účtu zapnuté dvoufaktorové ověření. Po aktivaci se v té samé sekci zobrazí údaje pro připojení z vlastního počítače v části **SSH přístup**:

- **SSH host**: adresa serveru, například vps1234.webglobe.com,
- **SSH port**: číslo portu, například 20001,
- **Jméno uživatele**: ve tvaru ssh-123456.

WebAdmin vám rovnou nabídne i hotový příkaz pro připojení. S SSH klíčem vypadá takto:

```
ssh -p 20001 -i ~/.ssh/id_ed25519 ssh-123456@vps1234.webglobe.com
```

Běžná SSH konzole platí 1 hodinu od aktivace, pak se přístup automaticky zruší. Pokud se chcete k hostingu připojovat pravidelně, aktivujte si **permanentní SSH konzoli**, kterou můžete využívat bez časového omezení.

Jak se přihlásit pomocí SSH klíče

Jakmile je veřejný klíč na serveru, přihlásíte se příkazem:

```
ssh -i ~/.ssh/id_ed25519 uzivatel@mojedomena.cz
```

Místo **uzivatel** a **mojedomena.cz** použijte své přihlašovací jméno a adresu serveru.

U webhostingu přidejte parametr **-p** s číslem portu, které najdete ve WebAdminu v sekci WebSSH (viz výše). V konfiguračním souboru níže port doplníte řádkem **Port 20001**.

Zjednodušení přihlášení přes konfigurační soubor

Abyste nemuseli pokaždé vypisovat celý příkaz, vytvořte si soubor **~/.ssh/config** s tímto obsahem:

```
Host mojedomena.cz
    HostName mojedomena.cz
    User uzivatel
    IdentityFile ~/.ssh/id_ed25519
```

Pak vám k přihlášení stačí příkaz ssh mojedomena.cz.

> *Nechcete zadávat passphrase při každém přihlášení? Přidejte klíč do SSH agenta příkazem **ssh-add ~/.ssh/id_ed25519**. Passphrase pak zadáte jen jednou za relaci.*

Co dělat, když přihlášení klíčem nefunguje

Pokud vás server místo klíče žádá o heslo nebo spojení odmítne, projděte tyto body:

- **Oprávnění souborů na serveru**: soubor **authorized_keys** musí mít oprávnění 600 a složka **.ssh** oprávnění 700. Při volnějších právech server klíč ignoruje.
- **Celý veřejný klíč na jednom řádku**: při kopírování se klíč nesmí zalomit ani zkrátit. Každý klíč patří na samostatný řádek.

- **Správný uživatel**: klíč musí ležet v souboru **authorized_keys** toho uživatele, za kterého se přihlašujete.
- **Firewall u VPS**: pro připojení přes SSH musí být ve firewallu povolený port 22.
- **Správný formát klíče v PuTTY**: PuTTY potřebuje privátní klíč ve formátu .ppk. Načtete ho v nastavení **Connection → SSH → Auth → Credentials**.

Podrobný výpis toho, co se při připojení děje a kde se zasekne, získáte příkazem:

```
ssh -v uzivatel@mojedomena.cz
```

Jak s SSH klíčem zacházet bezpečně

Pro každý počítač si vytvořte vlastní klíč. Když o zařízení přijdete, stačí ze serveru odebrat jen jeden veřejný klíč a ostatní přístupy zůstanou funkční.

> ***Pozor:*** *privátní klíč nikomu neposílejte, nenahrávejte ho do cloudových úložišť a negenerujte klíče přes online generátory. Klíč, který vznikl mimo váš počítač, už nemůžete považovat za tajný.*