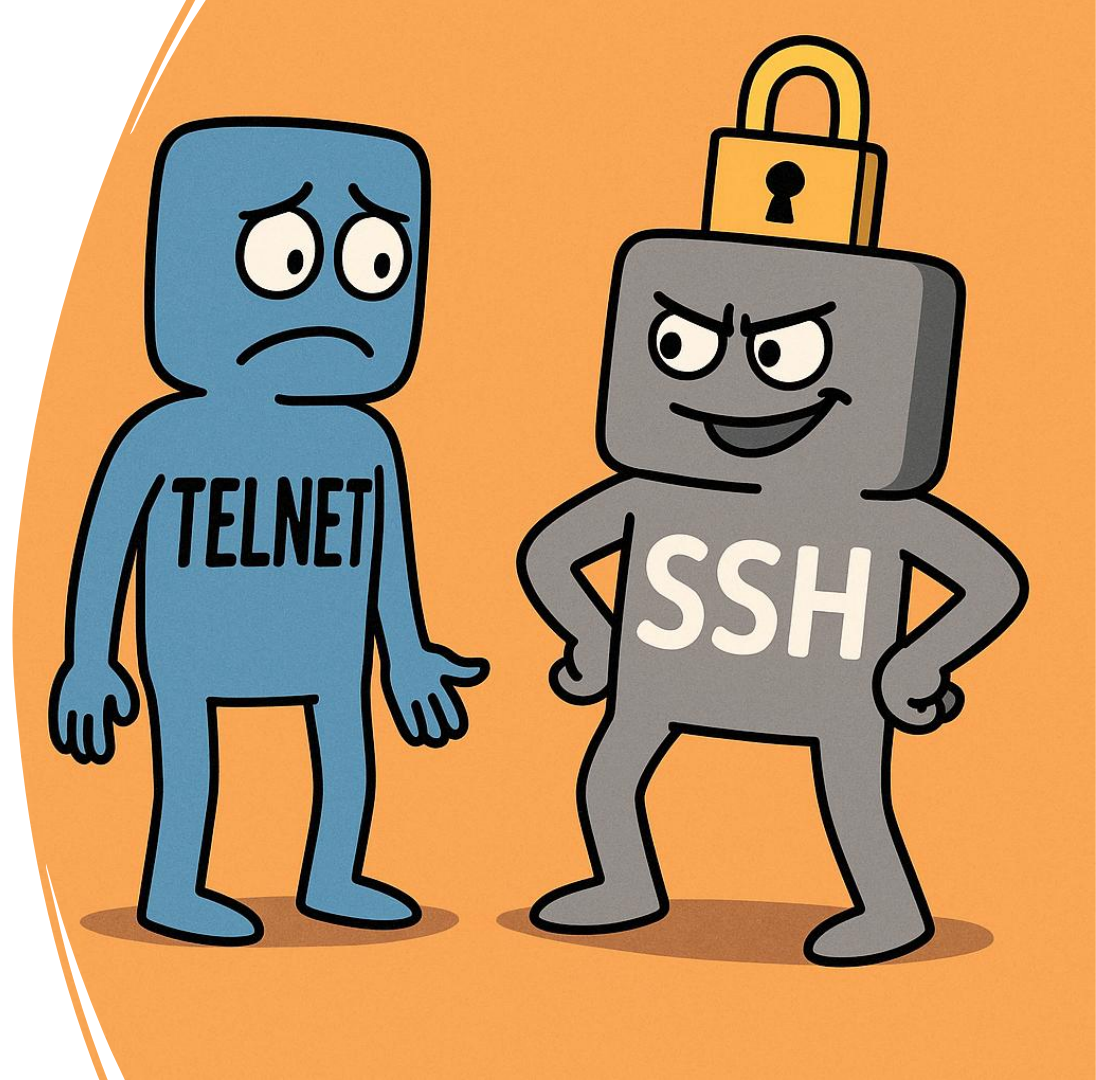


TELNET, SSH

Ing. Petr Orvoš

SOŠ a SOU NERATOVICE



VZDÁLENÉ PŘÍSTUPY K ZAŘÍZENÍ

Základní vzdálené přístupy k síťovým zařízením umožňují správu, konfiguraci a monitoring zařízení (např. routerů, switchů, serverů) bez fyzické přítomnosti u nich. Tyto přístupy se liší dle úrovně zabezpečení, použité technologie i účelu. Zde jsou nejčastější metody:

SSH (Secure Shell)

Telnet

RDP (Remote Desktop Protocol)

VNC (Virtual Network Computing)

HTTPS / Webové rozhraní

SNMP (Simple Network Management Protocol)

VPN (Virtual Private Network)

CO JE TELNET?

TELNET = TELEcommunication NETWORK

- síťový protokol z roku 1969
- umožňuje připojení k jinému zařízení přes síť (např. k routeru, serveru)
- funguje na principu klient-server – připojení přes TERMINÁL

Telnet umožňuje ovládat vzdálený počítač

„jako bychom seděli u něj“.

úvodní VIDEO (klikni na ikonu)







JAK TELNET FUNGUJE?

- pracuje na **transportní vrstvě** TCP/IP modelu
- používá **port 23 (TCP spojení)** ➡ přenáší data „bez chyb“!

Klient odešle příkaz → server provede → výsledek se zobrazí zpět

Vhodné pro:

- konfiguraci síťových zařízení
- přístup ke vzdálenému shellu

-  Klient (např. náš počítač)
-  TCP spojení (port 23)
-  Server (např. router, switch, server)
-  Přes Telnet se posílají čisté textové příkazy

PŘÍKLAD POUŽITÍ?

Používá se například pro:

- konfiguraci Cisco zařízení v laboratořích
- připojení k Linux serverům
- testování otevřených portů (např. telnet google.com 80)

```
telnet 192.168.1.1
```

```
Username: admin
```

```
Password: ****
```

```
Router>
```

VÝHODY a NEVÝHODY?

- ✓ Jednoduchá implementace
- ✓ Nízká režie přenosu
- ✓ Rychlé spojení

- ✗ Bez šifrování
- ✗ Možnost odposlechu
- ✗ Nahrazen SSH

Všechna komunikace probíhá jako prostý text (údaje jako jméno a heslo jsou přenášeny v čitelné podobě, což je velké riziko).

To znamená, že útočník může vše snadno odposlechnout, pokud má přístup do stejné sítě!

CO JE SSH?

SSH = Secure Shell – moderní nástupce TELNETU

- vznikl v roce 1995
- je to bezpečný síťový protokol pro vzdálený přístup k jinému zařízení přes internet nebo místní síť
- komunikuje přes port: 22 (TCP)
- přenos dat: šifrovaný – zajišťuje důvěrnost a integritu

PŘÍKLAD POUŽITÍ a VÝHODY

Používá se například pro:

- bezpečné přihlášení na vzdálený počítač přes síť
- konfigurace a správa serverů, síťových zařízení, Linux systémů
- přenos souborů (např. pomocí SCP nebo SFTP)


Výhody:


- ✓ šifrování celé komunikace – ochrana proti odposlechu a útokům
- ✓ ověření identity (heslem, klíčem)
- ✓ dnešní standard pro administrátory, vývojáře i správce sítí

JAK FUNGUJÍ SSH KLÍČE

SSH klíče jsou dvojice souborů, které spolu „pasují“ jako zámek a klíč.

Rozeznáváme:

 **privátní klíč** (private key) – je super tajný, uložený u vás na počítači **(NIKDY NESDÍLET!)**

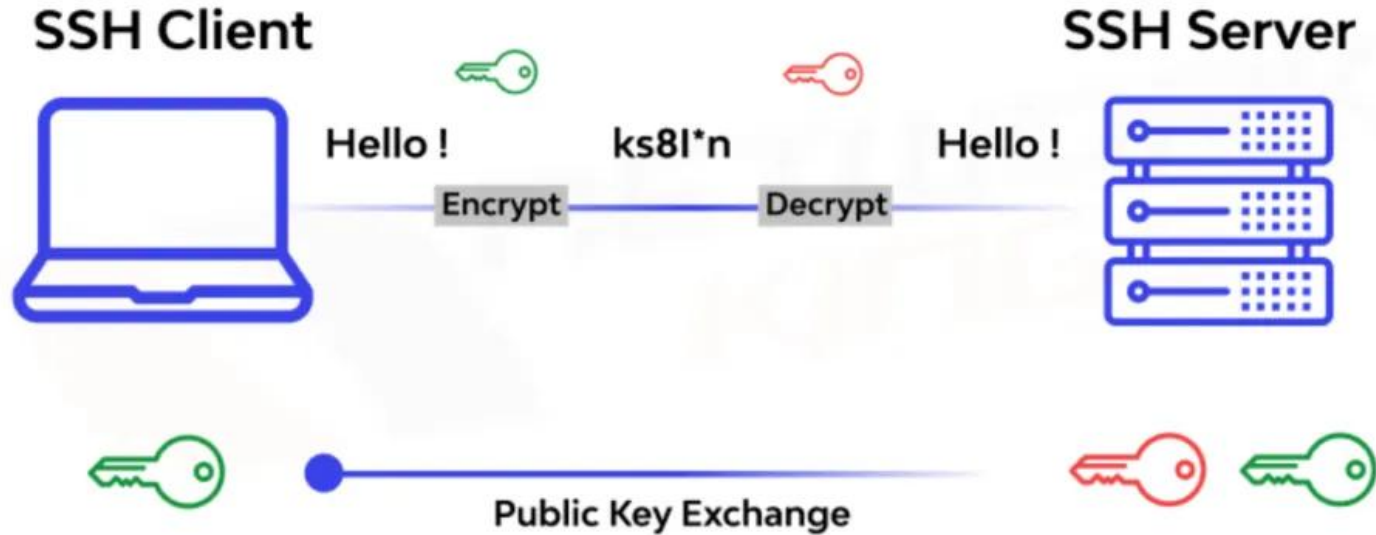
 **veřejný klíč** (public key) – ten můžete rozesílat, např. na servery, ke kterým se chcete přihlašovat **(MŮŽETE SDÍLET!)** Lze ho vygenerovat ze soukromého klíče.

Dohromady tvoří tzv. asymetrickou kryptografii – šifrování, které funguje na principu dvou různých klíčů.





... více o klíčích ve VIDEU (klikni na ikonu)



JAK FUNGUJÍ SSH KLÍČE



SROVNÁNÍ SSH a TELNET

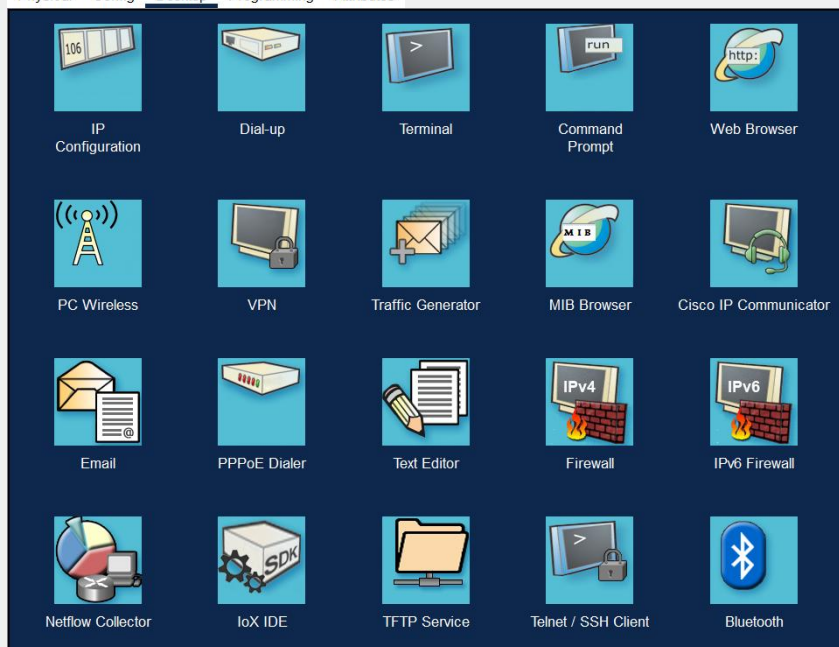
<i>vlastnost</i>	<i>TELNET</i>	<i>SSH</i>
Port	23	22
Šifrování	 Ne	 Ano
Bezpečnost	 Nízká	 Vysoká
Autentizace	Heslo (v textu)	Heslo / Klíč
použití dnes	Výuka, testy	Běžná praxe

KONFIGURACE SSH NA SWITCHI CISCO

Krok	Příkaz	Popis / Poznámka
1	enable	přepnutí do privilegovaného režimu
2	configure terminal	vstup do globální konfigurace
3	hostname SW1	nastavení názvu zařízení
4	ip domain-name sosasou.cz	nastavení doménového jména
5	username <i>admin</i> secret <i>cisco123</i>	vytvoření uživatele pro SSH přihlášení
6	crypto key generate rsa	generování RSA klíče (zadej 1024 bitů)
7	line vty 0 15	vstup do konfigurace VTY linek
8	transport input ssh	povolení pouze SSH (zakáže Telnet)

KONFIGURACE SSH NA SWITCHI CISCO

Krok	Příkaz	Popis / Poznámka
9	login local	přihlášení pomocí lokálních účtů
10	ip ssh version 2	aktivace bezpečnější verze SSH
11	ip ssh time-out 60	(volitelné) Timeout přihlášení
12	ip ssh authentication-retries 2	(volitelné) počet pokusů o přihlášení
13	end	ukončení konfigurace
14	write memory	uložení konfigurace do NVRAM



KONFIGURACE SSH NA SWITCHI CISCO - OVĚŘENÍ

Telnet / SSH Client

Session Options

Connection Type

SSH

Host Name or (IP address)

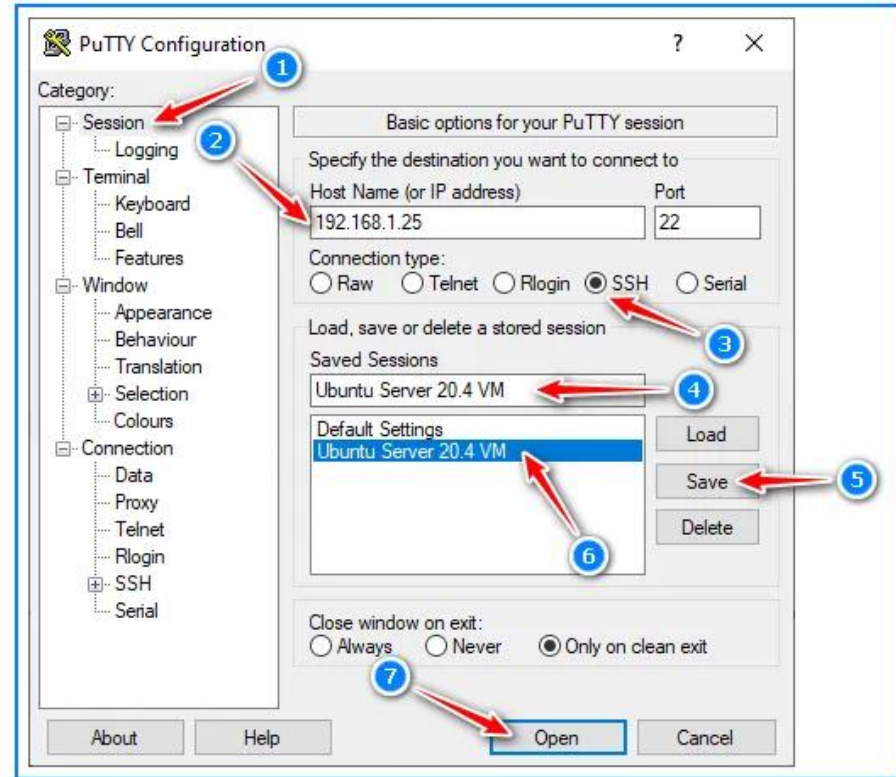
Username

Connect

PUTTY – terminálový program

ale o tom podrobněji jindy ...

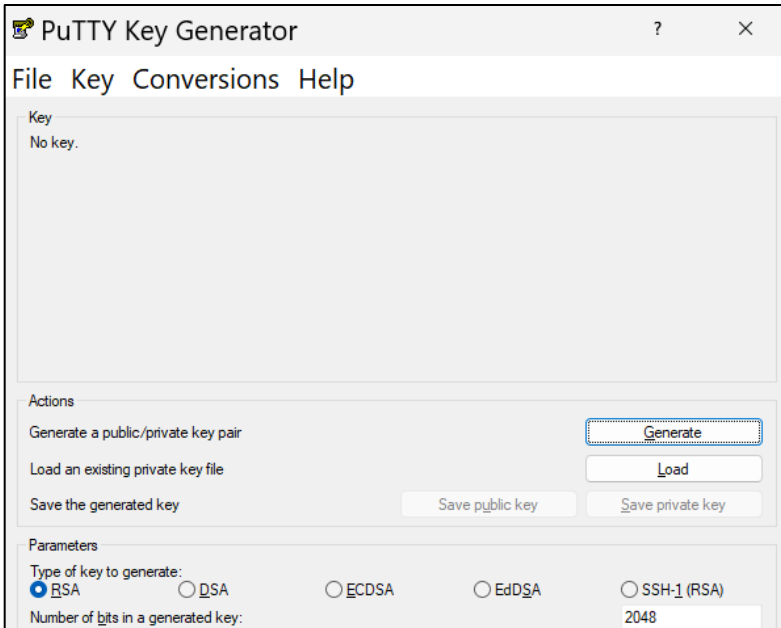
**POZOR NA FALEŠNÉ
PUTTY ve Windows
(odkud stahujete)!**



PUTTY – generování SSH klíčů

Program PUTTY umí generovat SSH klíče. Děje se tak pomocí utility **puttygen**.

1. stiskni WIN+R a otevři dialogové okno „Spustit“
2. zadej příkaz „puttygen“
3. otevře se Putty Key Generator a následně stiskneme „Generate“ a pohybujeme myší při tvorbě klíčů (v parametrech vidíme typy klíčů, např. RSA)

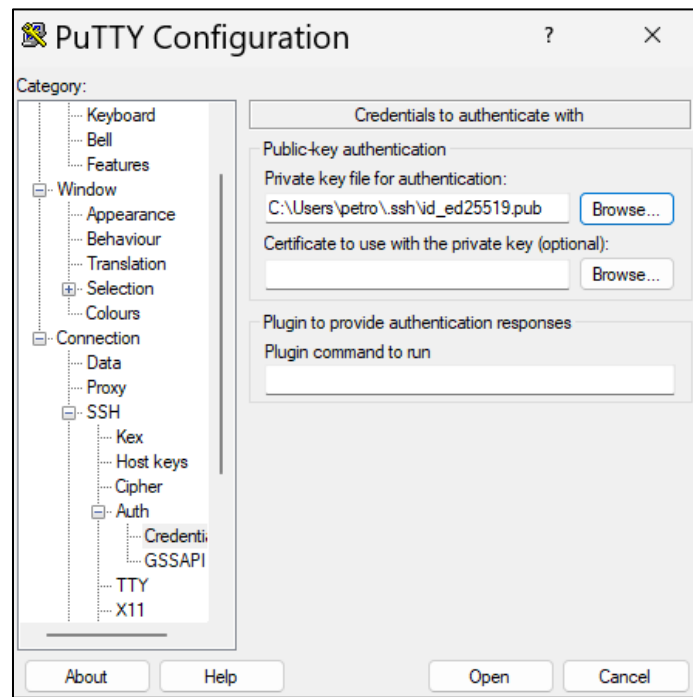
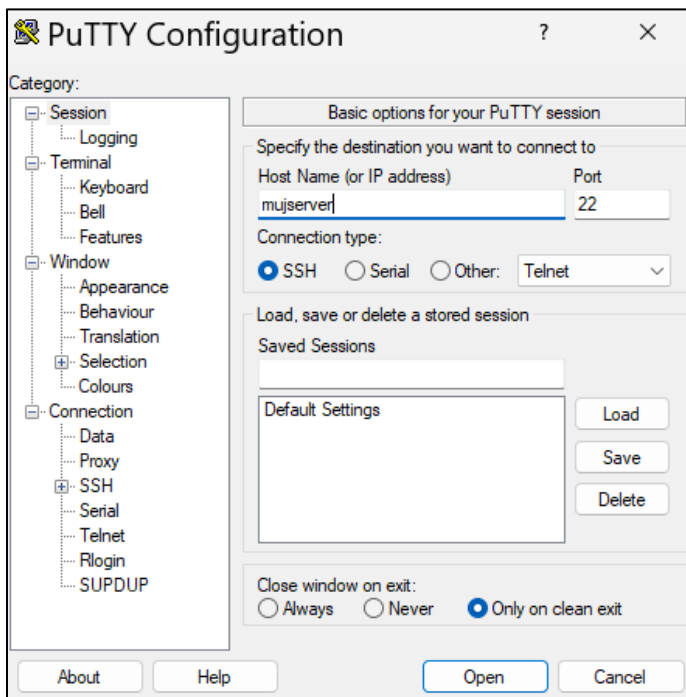


4. uložíme oba klíče do adresářů, u privátního klíče (standardně přípona .ppk), ale ještě si uděláme konverzi do OpenSSH (pro jistotu a kompatibilitě) – **Chraňte si soukromý klíč!**
5. veřejný klíč (public key, ukládáme s příponou .pub) můžete dát majiteli serveru na který chcete pomocí SSH přistupovat (majitel si ho nainstaluje).



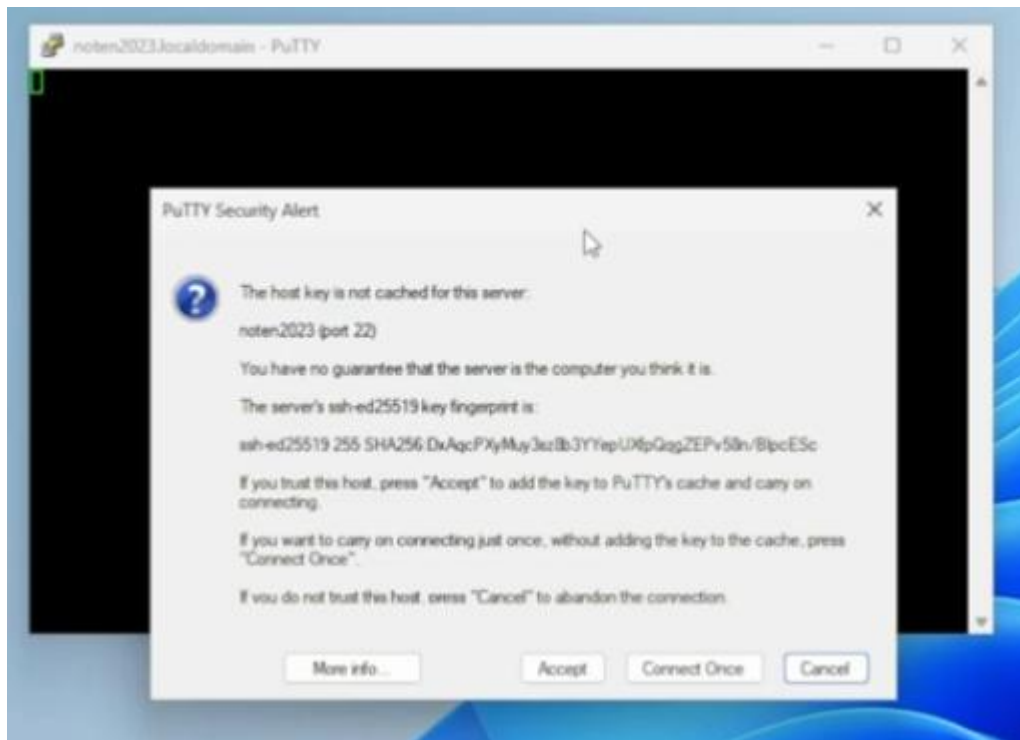
PUTTY – použití SSH klíčů

1. z přechozího: majitel si nainstaloval na serveru veřejný SSH klíč, který jsi mu zaslal
2. spustíme program Putty a zadáme ke komu se připojujeme (např. mujserver)
3. jdeme do Connection-SSH-Auth-Credentials, nahraji si veřejný SSH klíč z adresáře a kliknu na „Open“.



PUTTY – použití SSH klíčů

1. otevře se první připojení k serveru, který poskytne klíč (podpis), klikni na „Accept“
2. otevře se okno a zadáte login a svoje heslo k privátnímu klíči (pokud jste zadali)



KONFIGURACE SSH NA POČÍTAČI ve WINDOWS

Máme k dispozici:



svůj počítač (např. s Linuxem nebo Windows s WSL) – tomu budeme říkat **klient**.



vzdálený počítač / server / Raspberry Pi – tomu budeme říkat **server**.

Chceš, aby ses mohl z klienta přihlásit na server **bez zadávání hesla**, ale **bezpečně** – pomocí SSH klíčů.

KONFIGURACE SSH NA POČÍTAČI - PŘÍKLAD

1.  Vygeneruj SSH klíč u sebe na počítači (klientovi)

V terminálu (PowerShell) Windows zadej příkaz: **ssh-keygen**

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\petro> ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\petro\.ssh/id_ed25519): |
```

Když se zeptá: Kde uložit klíč? – potvrď enter (uloží se do ~/.ssh/id_rsa)

KONFIGURACE SSH NA POČÍTAČI - PŘÍKLAD

```
PS C:\Users\petro> ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\petro/.ssh/id_ed25519):
Created directory 'C:\\Users\\petro/.ssh'.
Enter passphrase (empty for no passphrase): |
```

dále se zeptá: **Enter passphrase** (volitelné heslo)? – můžeš ho zadat nebo nemusíš, ale pro extra bezpečnost doporučuji zadat

 Výsledkem budou dva soubory:

~/.ssh/id_rsa – privátní klíč (zůstává u tebe, nikomu ho nedávej)

~/.ssh/id_rsa.pub – veřejný klíč (ten se nahrává na server)

KONFIGURACE SSH NA POČÍTAČI - PŘÍKLAD

```
PS C:\Users\petro> ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\petro/.ssh/id_ed25519):
Created directory 'C:\\Users\\petro/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\petro/.ssh/id_ed25519
Your public key has been saved in C:\Users\petro/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:LaBsQ2GQtDiNBqHG/7nSPZR7gMgldqrcAnCNWP3goqM petro@GEO-SHADOW
The key's randomart image is:
+--[ED25519 256]--+
|  ++              |
| ..o=o=           |
| .=.+*oo          |
| + =*o+...        |
| .ooo@ . S .      |
| + =.o.+ .        |
| +.o .oo o        |
| E+ o ..+ .       |
|   .. o           |
+-----[SHA256]-----+
PS C:\Users\petro> |
```

Adresář, kde
jsou uložené
klíče

algoritmus pro šifrování
Edwardsův, mohl by
např. být i rsa (ale
údajně není tak
bezpečný)



POUŽITÁ LITERATURA a ZDROJE

PowerCert Animated Videos: SSH and TELNET. YouTube kanál [online video]. YouTube. [cit. 2025-04-24]. Dostupné z: <https://www.youtube.com/watch?v=tZop-zjYkrU&t=1s>

ASK Leo: How Do I Create and Use Public Keys with SSH? YouTube kanál [online video]. YouTube. [cit. 2025-04-24]. Dostupné z: <https://www.youtube.com/watch?v=5K7Xco3-RQc>