Gerando uma chave SSH no Windows - PuTTY

PuTTY

O PuTTy é um software de emulação de terminal grátis e de código livre. Suporta SSH, destinado a suportar o acesso remoto a servidores via shell seguro e a construção de "túneis" cifrados entre servidores. Também suporta conexão direta, telnet, rlogin e por porta serial.

Está disponível para download em:

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

Gerando as chaves pública e privada

Após instalar, procure no menu iniciar um atalho com o nome "PuTTYGen" e o execute.

RSA

Com o programa aberto, verifique na seção *Parameters* se a opção RSA está selcionada. Agora, basta pressionar o botão *Generate* e mover o cursor aleatoriamente pela parte "vazia" do programa, a fim de gerar movimentos aleatórios que serão usados para gerar sua chave.

puttyGen.jpg
Image not found or type unknown

Caso deseje criptografar sua chave privada, informe uma senha nos campos `Key passphrase` e `Confirm passphrase`.

Agora salve suas chaves usando os botões `Save public key` e `Save private key`. Lembre-se de guardar bem estes arquivos!

ED25519

Na seção *Parameters*, escolha `EdDSA`, opção `Ed25519 (255 bits)`, que é suportada por uma ampla gama de serviços. Depois, clique em *Generate*, na seção *Actions*. Agora, basta mover o cursor aleatoriamente pela parte "vazia" do programa, a fim de gerar movimentos aleatórios que serão usados para gerar sua chave.

Captura de tela 2024-07-25 141021.png

Image not found or type unknown

Há a possibilidade de adicionar uma camada extra de segurança adicionado uma senha à chave privada criada, porém, é opcional. Utilize o campo *key_comment* para adicionar algum comentário relevante: data criação, email, nome...

Captura de tela 2024-07-25 141648.png

Image not found or type unknown

Agora, salve suas chaves usando os botões "`Save public key`" e "`Save private key`", lembre-se de guardar bem estes arquivos! Não se esqueça, a chave privada deve ser armazenada em segurança e ninguém, além de você, deve ter acesso a ela.

Conclusão

Em resumo, ED25519 e RSA são algoritmos criptográficos de chave pública populares usados para transmissão segura de dados. O ED25519 é geralmente considerado mais seguro e eficiente que o RSA, enquanto o RSA oferece um nível alto de segurança devido ao seu tamanho de chave maior. A escolha entre estes dois algoritmos depende da aplicação específica e do nível de segurança e eficiência exigidos.

Referências

https://tecdicas.com/como-criar-e-utilizar-chaves-ssh-no-windows-e-linux/

https://medium.com/@sahil-awasthi/ed25519-or-rsa-which-one-is-better-18416fb51d0b

---

Revision #11
Created 10 June 2024 21:26:38 by Francisco Diego Garrido da Silva
Updated 26 July 2024 00:00:18 by Francisco Diego Garrido da Silva