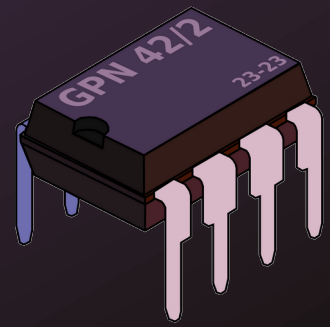
Noch besser leben mit SSH



#gpn21

@LEYRER [@chaos.social]
https://martin.leyrer.priv.at

Sven Guckes

bruttl

@bruttl@chaos.social

shitpoßt SHOW LESS

OH: So, in German, do you use ssh or ßh?

07 Jun 2023, 22:35 · · 23 · 33

https://chaos.social/@bruttl/110504846628125622

PREVIOUSLY ON 24

Besser leben mit SSH

No Usernames

```
Host demo bastion
    HostName ssh-server.example.com
    User leyrer
```

ssh leyrer@ssh.example.com

ssh demo

ssh-keygen

```
$ ssh-keygen -t ed25519 \
    -a 420 \
    -f ~/.ssh/demo.ed25519 \
    -C "Dem leyrer sein key (gpn20)"
```

~/.ssh/config

```
Host demo bastion
    HostName ssh.example.com
    User leyrer
    PreferredAuthentications publickey
    IdentityFile ~/.ssh/demo.ed25519
```

Connect without passphrase

```
ssh-add ~/.ssh/demo.ed25519

ssh demo
```

Sane Defaults

```
Host demo bastion
    HostName ssh.example.com
    User leyrer
    PreferredAuthentications publickey
    IdentityFile ~/.ssh/demo.ed25519
...
Host *
    IdentitiesOnly yes
    UseRoaming no
    SendEnv LANG LC_*
    Compression yes
```

Elegant “Jumping”

```
Host demo bastion
    HostName ssh.example.com
    User leyrer
    PreferredAuthentications publickey
    IdentityFile ~/.ssh/demo.ed25519

Host internal
    HostName target.local
    ProxyJump bastion
    User leyrer
    PreferredAuthentications publickey
    IdentityFile ~/.ssh/demo.ed25519
```

Public/Private Key

They are free !!!

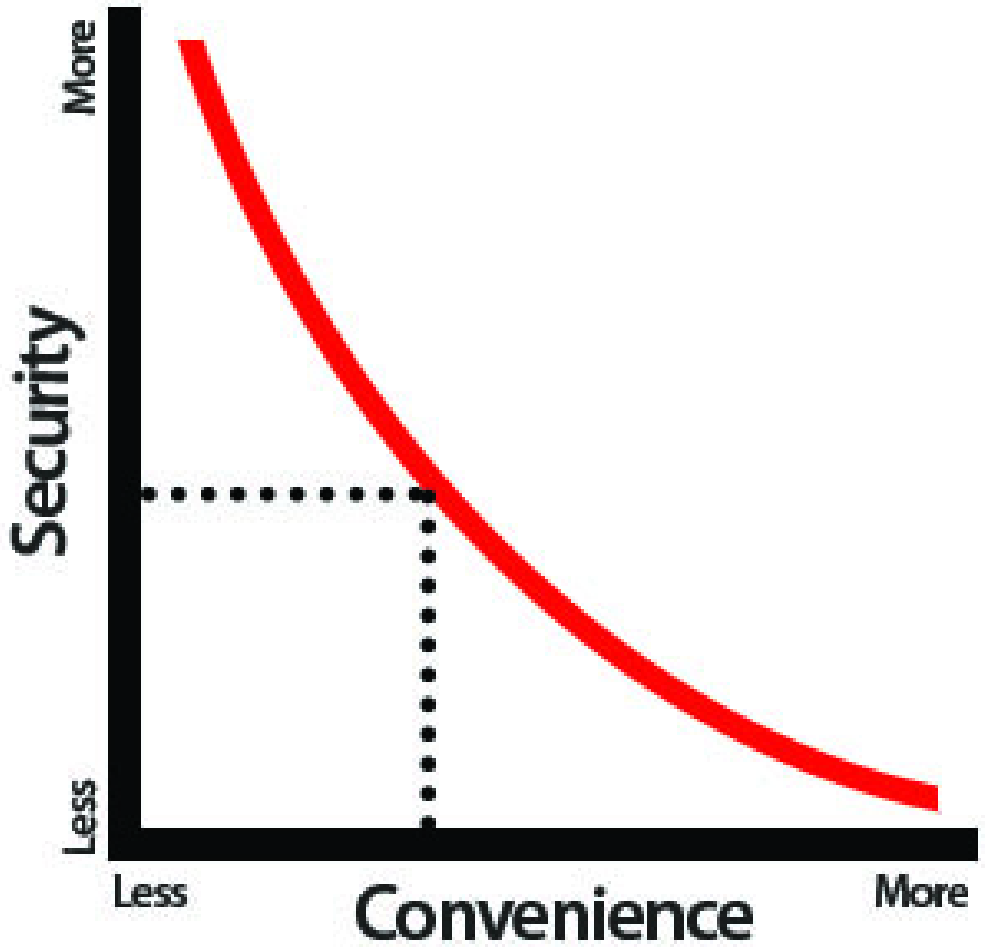
Create one for each server, customer or service you connect to.

ssh-keygen

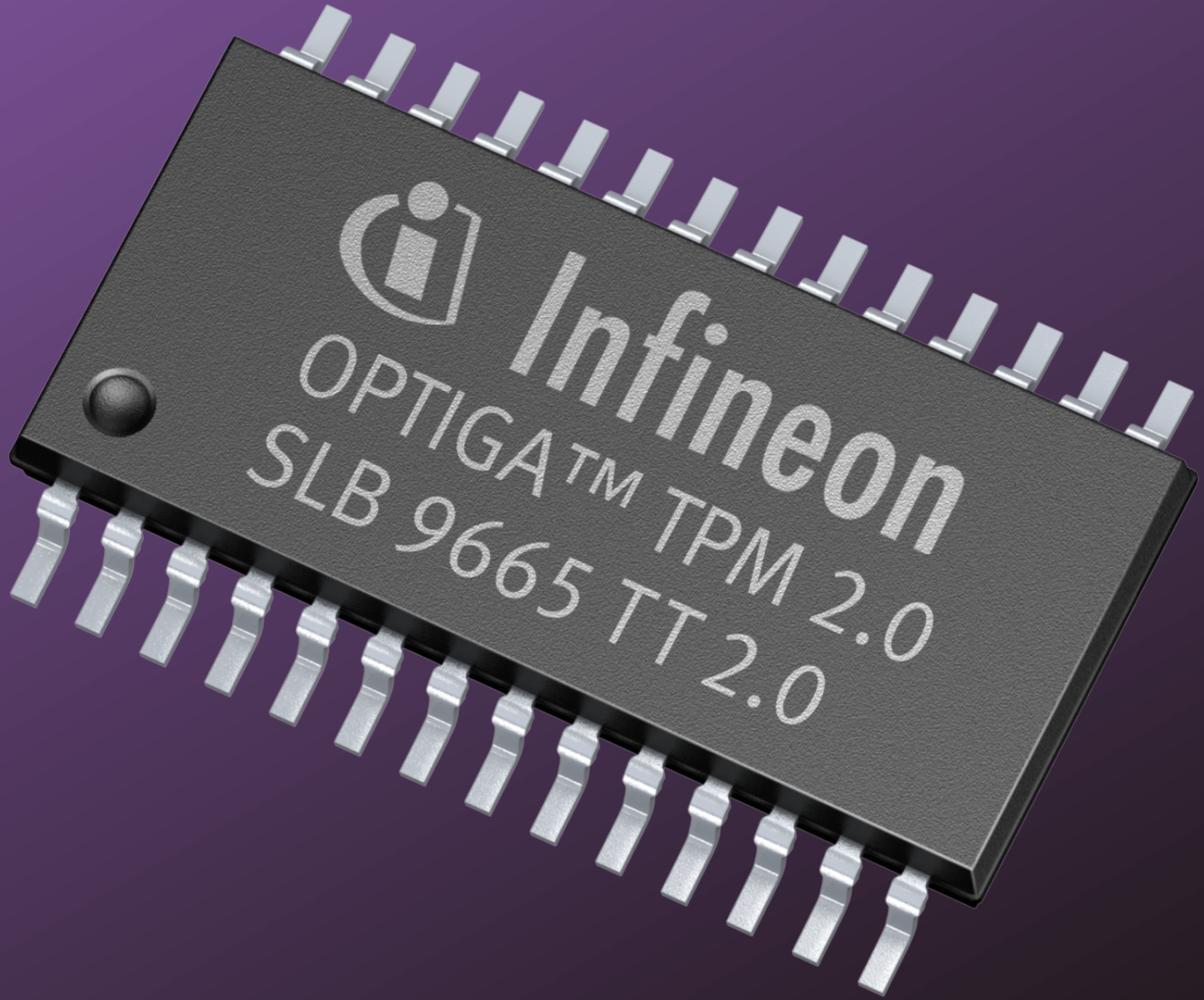
```
$ ssh-keygen -t ed25519 \
    -a 420 \
    -f ~/.ssh/demo.ed25519 \
    -C "Dem leyrer sein key (gpn21)"

~/.ssh/demo.ed25519 ~/.ssh/demo.ed25519.pub
```

Security vs. Convenience



SSH key im TPM


Infineon
OPTIGA™ TPM 2.0
SLB 9665 TT 2.0

tpm2-pkcs11

- 2014: main TPM 2.0 specifications published
- 2018: project tpm2-pkcs11 was created
- February 2019: Fedora 29
- September 2019: CentOS 8
- April 2020, Debian sid
- April 2021, Ubuntu 21.04 Hirsute Hippo
- August 2021, Debian 11 Bullseye

Install

```
sudo apt install libtpm2-pkcs11-tools
libtpm2-pkcs11-1
```

Verify

- Check whether /dev/tpm0 exists
- Check whether the command tpm2_getcap properties-fixed
  displays some data

Prerequisites

```
sudo usermod -a -G tss "$(id -nu)"
```

TPM für SSH initalisieren

```
tpm2_ptool init

tpm2_ptool addtoken --pid 1 \
  --label sshgulasch \

  --userpin 1234 \
  --sopin 1234
```

Key erstellen

```
tpm2_ptool addkey \
  --label=1234 \
  --userpin=1234 \
  --algorithm=ecc256 \
  --key-label "TPM Key GPN"
```

Hashing Algorithms

- rsa1024
- rsa2048
- rsa3072
- rsa4096
- aes128
- aes256
- ecc224
- ecc256
- ecc384
- ecc521
- hmac:sha1
- hmac:sha256
- hmac:sha384
- hmac:sha512

Public Key anzeigen

```
ssh-keygen -D /usr/lib/x86_64-linux-gnu/libtpm2_pkcs11.so.1
```

```
ssh-keygen -D /usr/lib/x86_64-linux-
gnu/libtpm2_pkcs11.so.1

ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIb
mlzdHAyNTYAAABBBIl0ZDd3q5ViXRMBUf4W/
3I3bg5etPrxRg99wfM0NibmtkIEUwQkd+ysh9
WSvMzS+9omR7YQvrfvPhT206YJxJ0= TPM
Key GPN
```

Manual Copy

- copy public key to clipboard
- paste it into `~/.ssh/authorized_keys` on servers

~/.ssh/config

```
Host gulasch
  HostName ssh-server.example.com
  User gulasch
   PKCS11Provider /usr/lib/x86_64-linux-gnu/libtpm2_pkcs11.so.1
   PasswordAuthentication no
```

Connect

```
ssh gulasch
```

TPM and existing SSH keys

tpm2-pkcs11 Pull Requests #681

--passin option

TPM: keys without password

more secure than key files as the protected key cannot be extracted from the TPM

tpm2-pkcs11 Pull Requests #695

- empty-user-pin option

Securing SSH keys with YubiKey Security Keys U2F

Voraussetzungen

OpenSSH 8.2 oder höher

```
$ ssh -V
OpenSSH_9.2p1 Debian-2, OpenSSL 3.0.9 30 May 2023
```

Yubico libsk-libfido2.so installiert

```
$ sudo apt install libfido2-1 libfido2-dev \
                   libfido2-doc fido2-tools
```

Empfehlung

YubiKeys firmware 5.2.3 oder höher

Solo Key funktioniert auch, aber …

```
$ lsusb -v 2>/dev/null | grep -A2 Yubico |
grep "bcdDevice" | awk '{print $2}'

4.37
```

Schlüssel erzeugen

```
$ ssh-keygen -t ecdsa-sk \
    -f ~/.ssh/demo.yubikey \
    -C "GPN KEY"
```

Public key

```
$ cat ~/.ssh/demo.yubikey.pub
```

```
sk-ecdsa-sha2-nistp256@openssh.com
AAAAInNrLWVjZHNhLXNoYTItbmlzdHAyNTZAb3BlbnNzaC5jb
20AAAAIbmlzdHAyNTYAAABBBFfBajDaBdRiAgi1EVtHunUh9o
Alf150n5vwtbjKvEfUGATM+IpMWrz5TEKKjsmMt29zlpJngcp
SYs4gF2w9C2kAAAAEc3NoOg== ubuntu-17-02-2020-
4432343
```

Manual Copy

- copy public key to clipboard
- paste it into `~/.ssh/authorized_keys` on servers

~/.ssh/config

```
Host gulasch
  HostName ssh-server.example.com
  User gulasch
  IdentityFile ~/.ssh/gpn.yubikey
```

Connect

```
ssh gulasch
```

Knopflos-SSH (VORSICHT !!!)

ssh-keygen -Ono-touch-required -t ecdsa-sk -f ~/.ssh/id_ecdsa_notouch_sk -C “notouch”

Server: .ssh/authorized_keys:

no-touch-required sk-ecdsa-sha2-nistp256@openssh.com AAAAInNrLWVjZHNhLXNoYTItbmlzdHAyNTZ... notouch

2FA (TOTP)

sudo apt-get install libpam-google-authenticator

/etc/pam.d/sshd:

auth required pam_google_authenticator.so

/etc/ssh/sshd_config:

KbdInteractiveAuthentication yes

Als User am Server (!) ausführen: google-authenticator

Fragen, Anregungen, weitere Tools?

Martin Leyrer

https://martin.leyrer.priv.at

@leyrer@chaos.social