

# Inhaltsverzeichnis

- Download und install** ..... 3
- PreRequisites ..... 3
- herunterladen, konfigurieren und kompilieren ..... 4



# Trusted Platform Module

"Don't ask what you can do for TPMs, Ask what TPMs can do for you"

Der TPM Chip ist praktisch eine erweiterte SmartCard. Warum also nicht den TPM benutzen zum speichern der privaten Keys für z.B. SSH oder TLS Zertifikate oder für die HDD Verschlüsselung mit [LUKS](#)?

Andreas Fuchs erklärt das am 36c3 in einem halbstündigen Vortrag.

[Hacking \(with\) a TPM](#)

TPM2 Software Community Homepage: [tpm2-software.github.io](https://tpm2-software.github.io)

## Download und install

### PreRequisites

[inst-prereq.sh](#)

```
sudo apt -y install \  
  autoconf-archive \  
  libcmocka0 \  
  libcmocka-dev \  
  procps \  
  iproute2 \  
  build-essential \  
  git \  
  pkg-config \  
  gcc \  
  libtool \  
  automake \  
  libssl-dev \  
  uthash-dev \  
  autoconf \  
  doxygen \  
  libjson-c-dev \  
  libini-config-dev \  
  libcurl4-openssl-dev \  
  uuid-dev \  
  qrencode \  
  pandoc \  
  libltdl-dev
```

Es kann sein, dass das Paket bei euch auch uuid-dev statt libuuid-dev heisst. Ich habe es oben mal so angepasst. libqrencode wurde bei mir auch nicht gefunden, ich hab's durch quencode ersetzt.

## herunterladen, konfigurieren und kompilieren

[build.sh](#)

```
sudo chmod go+rw /dev/tpmrm0
for i in tss tss-engine pkcs11 totp tools; do
git clone --depth=1 \
https://github.com/tpm2-software/tpm2- $\{i\}$ .git \
&& pushd tpm2- $\{i\}$  \
&& ./bootstrap \
&& ./configure --enable-plymouth --sysconfdir=/etc \
&& make -j$(nproc) \
&& sudo make -j install \
&& popd
done
tpm2_getcap properties-fixed
```

Fehler habe ich bekommen, weil `--enable-pymouth` als Option nicht erkannt wurde. Und die ManPages wurden nicht installiert, weil das Paket `pandoc` nicht installiert ist.<sup>1)</sup>

Dann kommen Warnungen wegen OpenSSL 3.0 `RAS_free`, `EC_KEY_free`, `ENGINE_by_id`, `ENGINE_init`, `ENGINE_get_name`, `ENGINE_ctrl`, `EVP_MD_CTX_md`, ... is deprecated

Wenn alles geklappt hat, dann gibt der Befehl `tpm2_getcap...` die capabilities des TPM Chips aus. Ein einfacher Test ist z.B. der Zufallszahlengenerator, mit `tpm2_getrand 4` werden 4 zufällige Bytes ausgegeben.

So, was können wir nun damit machen?

[Hardware](#), [Security](#), [SecureStorage](#), [KeyGen](#), [Token](#), [Zertifikat](#)

<sup>1)</sup>

ich hab's den PreRequisites bereits hinzugefügt

From:

<https://aha-it.ch/wiki/> - **AHa-IT**

Permanent link:

<https://aha-it.ch/wiki/lx/tpm?rev=1668240561>

Last update: **12.11.2022 08:09**

