

Qubes OS and TPM 2.0





TPM 2.0 support in Qubes OS

Michał Żygowski





Michał Żygowski
Firmware Engineer

-  @_miczyg_
-  michal.zygowski@3mdeb.com
-  [linkedin.com/in/miczyg](https://www.linkedin.com/in/miczyg)
-  [facebook.com/miczyg1395](https://www.facebook.com/miczyg1395)
- PC Engines platforms maintainer
- interested in:
 - advanced hardware and firmware features
 - coreboot

- Anti-Evil Maid supports only TPM 1.2
- Qubes HCL report utility does not detect TPM 2.0?

Possibly no Linux kernel driver?

<https://www.qubes-os.org/doc/anti-evil-maid/>

All the TCG/TPM config options seem to be in the place on 4.9 stable:

<https://github.com/QubesOS/qubes-linux-kernel/blob/stable-4.9/config#L3545>

```
CONFIG_TCG_TPM=m
CONFIG_TCG_TIS_CORE=m
CONFIG_TCG_TIS=m
CONFIG_TCG_TIS_I2C_ATMEL=m
CONFIG_TCG_TIS_I2C_INFINEON=m
CONFIG_TCG_TIS_I2C_NUVOTON=m
CONFIG_TCG_NSC=m
CONFIG_TCG_ATMEL=m
CONFIG_TCG_INFINEON=m
CONFIG_TCG_XEN=m
CONFIG_TCG_CRB=m
CONFIG_TCG_VTPM_PROXY=m
CONFIG_TCG_TIS_ST33ZP24=m
CONFIG_TCG_TIS_ST33ZP24_I2C=m
```

But what with stable 4.14 and 4.19?

<https://github.com/QubesOS/qubes-linux-kernel/blob/stable-4.14/config-base#L3652>

<https://github.com/QubesOS/qubes-linux-kernel/blob/stable-4.19/config-base#L3832>

```
# CONFIG_TCG_TIS_SPI is not set
# CONFIG_TCG_TIS_I2C_ATMEL is not set
# CONFIG_TCG_TIS_I2C_INFINEON is not set
# CONFIG_TCG_TIS_I2C_NUVOTON is not set
# CONFIG_TCG_XEN is not set
# CONFIG_TCG_VTPM_PROXY is not set
# CONFIG_TCG_TIS_ST33ZP24_I2C is not set
# CONFIG_TCG_TIS_ST33ZP24_SPI is not set
```

Testing Qubes OS R4.0 on Intel i6-6500U (Skylake) based platform with coreboot firmware and Infineon SLB9556 TT 2.0 dTPM connected.

From dmesg:

```
[    0.000000] Linux version 4.14.18-1.pvops.qubes.x86_64 (user@build-fedora4)
(gcc version 6.4.1 20170727 (Red Hat 6.4.1-1) (GCC)) #1 SMP Thu Feb 8 20:01:16 UTC 2018
[    0.000000] Command line: placeholder root=/dev/mapper/qubes_dom0-root
ro rd.luks.uuid=luks-06bd3edc-4272-43d1-8d61-bc1deae5700d rd.lvm.lv=qubes_dom0/root
rd.lvm.lv=qubes_dom0/swap i915.alpha_support=1 rhgb quiet
...
[   25.457741] tpm_tis 00:05: 2.0 TPM (device-id 0x1A, rev-id 16)
```

Qubes HCL report:

Qubes release 4.0 (R4.0)

...

Xen: 4.8.3
Kernel: 4.14.18-1

RAM: 3994 Mb

CPU:

Intel(R) Core(TM) i7-6500U CPU @ 2.50GHz

Chipset:

Intel Corporation Xeon E3-1200 v5/E3-1500 v5/6th Gen Core Processor \\
Host Bridge/DRAM Registers [8086:1904] (rev 08)

...

HVM: Active
I/O MMU: Active
HAP/SLAT: Yes
TPM: Device not found
Remapping: yes

The HCL utility determines the TPM presence by checking PCR availability (requires kernel support);

```
PCRS=`find /sys/devices/ -name pcrs`
```

```
...
```

```
if [[ $PCRS ]]
then
  # try to run tcscd and: grep the logs, try get version info.
  TPM="Device present"
else
  TPM="Device not found"
  TPM_s="unknown"
fi
```


Some implementations of automatic disk decryption with LUKS and TPM 1.2:

1. <https://github.com/fox-it/linux-luks-tpm-boot>
2. <https://github.com/shpedoikal/tpm-luks>
3. <https://resources.infosecinstitute.com/linux-tpm-encryption-initializing-and-using-the-tpm/>
4. <https://ranzbak.nl/tpmluks/> (very straightforward)

Notes:

- using only TPM 1.2
- requires tpm-tools and trousers packages
- used with GRUB or TrustedGRUB

Some implementations of automatic disk decryption with LUKS and TPM 2.0:

1. <https://github.com/vchatterji/tpm2-luks>
2. <https://github.com/WindRiver-OpenSourceLabs/cryptfs-tpm2>
3. <https://blog.dowhile0.org/2017/10/18/automatic-luks-volumes-unlocking-using-a-tpm2-chip/>

Notes:

- option 1 and 2 requires TPM2 software from <https://github.com/tpm2-software>
- option 3 proposes the usage of Clevis <https://github.com/latchset/clevis>
- the development on TPM2 software is rather rapid

- What are the pros and cons of having TPM 2.0 support in Qubes?
- What is exactly required (or what blocks) the TPM 2.0 usage in Qubes OS?
- Does Anti-Evil Maid is so crucial, that Qubes only respects TPM 1.2?
- Solutions for TPM and LUKS integration are comparable in terms of availability (one can find comparable number of results when searching)
- TPM 2.0 is becoming the new standard superseding the TPM 1.2, is there a reason to cling to the old hardware?

Q&A