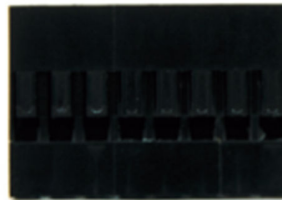# LetsTrust TPM Information

updated 2019/05

Installation & Configuration

1. Product contents

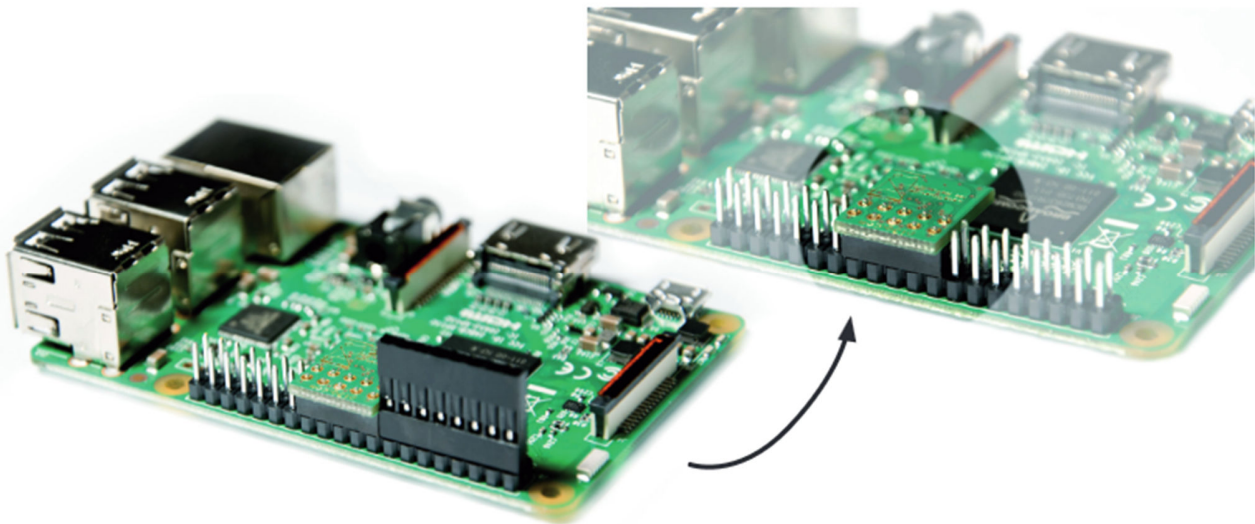1. LetsTrust TPM Module (12.7 x 17.5 mm)
2. female header (2x8 pin)

2. Install LetsTrust TPM

The supplied female header helps you plug
in the LetsTrust TPM in the correct position, but **it is not necessary to operate the LetsTrust TPM Module.**

Please insert the female header starting with pin 1 (on the far left, see picture below) into the Raspberry Pi GPIO header. Our picture shows the Raspberry Pi 3 Model B.

LetsTrust TPM is, of course, also compatible with other Raspberry Pi models.

Next, insert the LetsTrust TPM module directly next to the female header. (The TPM module will be installed starting with pin 17, facing downwards with the chip, and oriented towards the HDMI port.)

3. Configuration & Activation with Raspbian

The LetsTrust TPM module is supported directly by Linux, starting with Kernel 4.14.85. Please refer to www.letsTrust.de for further information. Update to the newest RaspberryPi OS and activate the TPM as **/dev/tpm0**using the following commands:

```
sudo apt-get update && sudo apt-get upgrade
sudo nano /boot/config.txt
```

dtparam=spi=on
dtoverlay=tpm-slb9670   ⟵   *add these two lines at the bottom of /boot/config.txt*

```
sudo reboot
```

4. Usage examples

The best projects for the TPM module come from the community, we are supplying the hardware. Already, several core software packages are available:

Link	Description
https://github.com/tpm2-software	TCG TPM2 software stack
https://github.com/wolfSSL/wolfTPM	wolfTPM Software Stack for microcontrollers
https://github.com/Infineon/eltt2	ELTT2 Infineon Embedded Linux TPM Toolbox 2 for TPM 2.0 – test, diagnostics and essential state changing of the Infineon TPM chip
https://github.com/PaulKissinger/LetsTrust	Useful resources & script to get you started with the TPM, and compilation / installation of the TPM 2.0 Tools.

We link application samples, documentation, and additional information from thecommunity homepage www.letsTrust.de

If you have interesting application examples, or are developing applications yourself, weask you to send us an e-mail at support@pi3g.com or info@letstrust.de

FAQ & Good to know

Which chip does the TPM use?

We use the Infineon OPTIGA™ SLB 9672 TPM 2.0 with Firmware 15.23 or later. This chip is compliant to the TCG TPM 2.0 Specification, revision 1.59.

Starting with Firmware Version 15.23, the SLB 9672 is certified with Common Criteria EAL4+and FIPS 140-2.

Can SPI still be used?

Yes, CS0 can still be used. The TPM module uses CS1.

It is possible to address the TPM module using CS0, by 1) moving the 0-Ohm resistor fromposition R3 to R2, AND 2) patching the device tree overlay to talk to the module on CS0.

The component placing can be found here:

https://www.letstrust.de/uploads/letstrust-v2.2.placement.cs1.pdf

Can I download a circuit diagram?

Yes! A circuit diagram is available here:

https://www.letstrust.de/uploads/letstrust-v2.2.schematic.pdf

How do I get support?

Many questions are already answered in the blog entries on: www.letsTrust.de
If you have additional in-depth questions, please get in touch with us: support@pi3g.com

Can you supply custom versions of the TPM module?

Starting at just 100 modules, we can modify the design for you.

Contact us here for inquiries:

support@pi3g.com