LetsTrust TPM Information

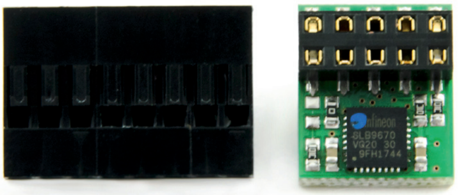
Installation & Configuration

updated 2019/05

pi3g
www.pi3g.com
Change the world.

1. Product contents

1. LetsTrust TPM Module (12,7 x 17,5 mm)
2. female header (2x8 pin)

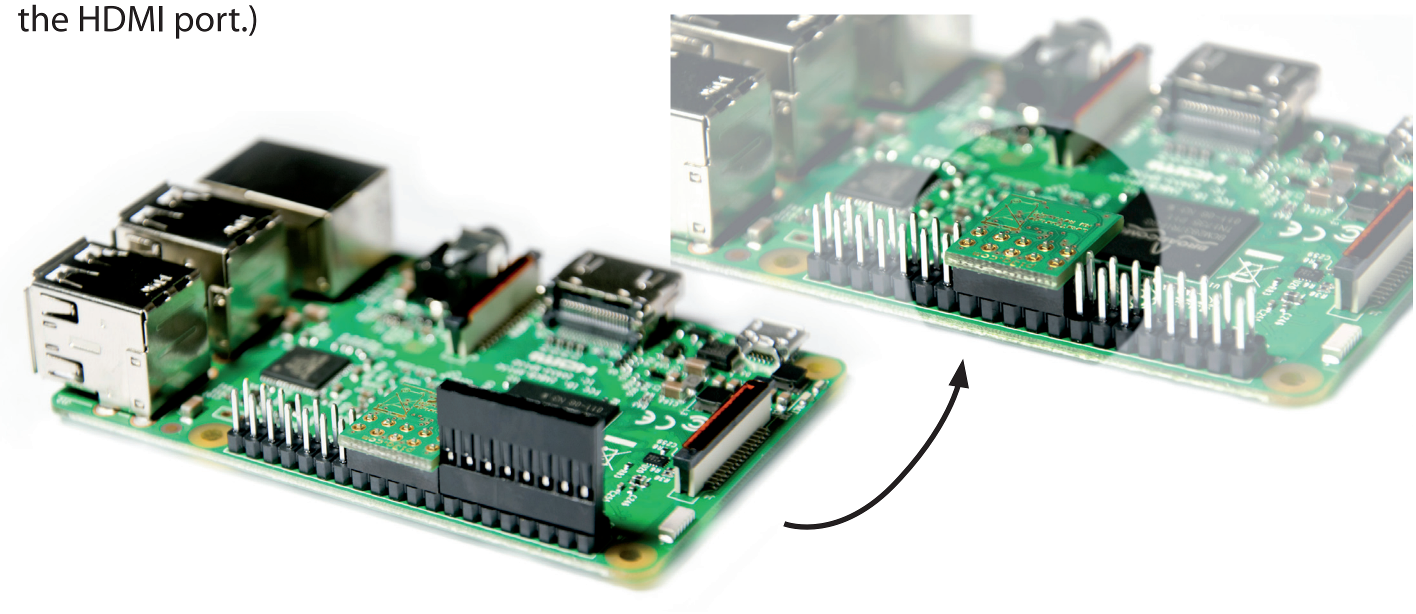


2. Install LetsTrust TPM

The supplied female header helps you to plug in the LetsTrust TPM at the right position. **It is not necessary for correct operation.**

Please insert the female header starting with pin 1 (*on the far left, see picture*) 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 under 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 Raspbian Stretch 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

sudo reboot
```

add these two lines at the bottom of /boot/config.txt

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/01org/tpm2.0-tools	Tools to use the TPM
https://github.com/01org/TPM2.0-TSS	TCG TMP2 software stack
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 a lot of additional information from the community homepage www.letsTrust.de
If you have interesting application examples, or are developing applications yourself, we ask 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 9670 TPM 2.0 with Firmware 7.85 or later. This chip is compliant to the TCG TPM 2.0 Specification, revision 1.38.

Starting with Firmware Version 7.85 the SLB 9670 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 from position 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-v2.0.placement.pdf

Can I download a circuit diagram?

Yes! A circuit diagram is available here:

https://www.letstrust.de/uploads/letstrust-v2.0.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