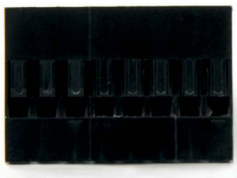
LetsTrust TPM

pi 3g
www.pi3g.com



EAN 0700729578049

Delivery Contents:

- LetsTrust TPM module
- 8-pin header

Please note: The 8-pin header is an auxiliary tool for correct positioning of the TPM module on the Raspberry Pi GPIO header. It is not necessary for correct operation.

Description

The pi3g LetsTrust TPM implements a hardware TPM solution based on the Infineon Optiga™ TPM SLB 9670 TPM2.0, as an add-on module for the Raspberry Pi and compatible platforms.

A TPM (*trusted platform module*) is an important component in your chain of trust and assurance in the integrity of your hardware and software systems. In times of increasing distributed autonomous systems (IoT, Industrie 4.0), security is becoming an ever more critical component of sustained and reliable operations.

IEC 62443 requires hardware security

In the IEC 62443 standard to secure Industrial Automation and Control Systems (IACS), for instance, hardware security is required for Security Levels 3 and 4. The reason: A dedicated hardware-based security co-processor is much harder to attack than purely software-based security solutions. One simple example clarifies this:

Using public-key cryptography, private keys are stored in a protected area inside the TPM. Contrast this with a software-based solution, where the private key must be kept in the RAM of the host computer at certain peri-

pi3g e.K.

Sales & Technical Inquiries:

phone: +49 341 392 858 42
email: support@pi3g.com
web: www.pi3g.com

WEEE Reg Nr:

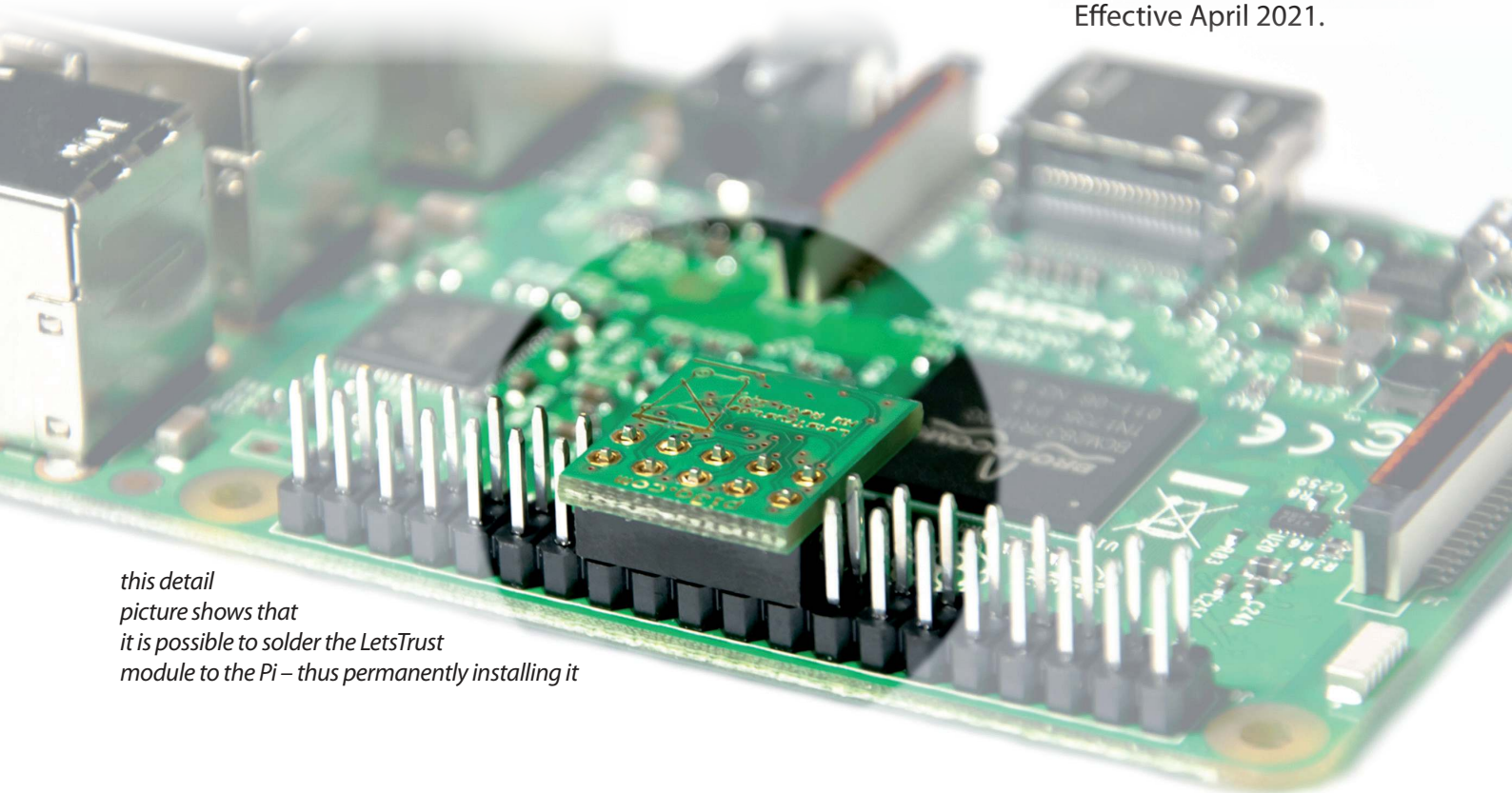
DE21378482

Company Register Nr:

HRA18308

LetsTrust TPM Datasheet

Hardware Version 2.0
Effective April 2021.



this detail picture shows that it is possible to solder the LetsTrust module to the Pi – thus permanently installing it

ods of time. Debuggers, the operating system, and other potentially harmful software could access and steal the private key. The TPM uses its own dedicated hardware and firmware to avoid being exposed to such and other vulnerabilities in the operating system and applications.

Cryptographic features & protection for your application

The TPM module supports you with cryptographic features essential for good security, such as a true hardware random number generator, secure generation and protection of cryptographic keys, remote attestation and sealed storage. The TPM protects against dictionary attacks on your passwords for instance by enforcing increasingly longer waiting times between guesses.

Remote attestation means that the state of your hardware and software can be communicated in a trustworthy and dependable way to a dedicated controller - thereby alerting you to unauthorized and potentially harmful changes to your systems. Sealed storage allows you to lock data unless a certain system configuration is reached, thereby protecting it from abuse.

Using the Endorsement Key or the Endorsement Certificate - with which every single LetsTrust TPM is personalized, and certified to be manufactured by Infineon - you can limit access to communications & control to only authorized devices in your network. Stolen or rogue devices can be efficiently removed from the list of trust, thereby limiting possible damage to your assets.

Control over your IP

Embedding a TPM solution in your hardware and/or software design allows you to control the distribution and usage of your IP. For example, imagine you have developed a hardware-add-on for the Raspberry Pi platform, and invested heavily into a supporting software stack. Another company could simply make a low-cost knock-off of your hardware design and benefit from your software stack. Using a TPM module, and registering allowed Endorsement Keys / Certificates allows your software stack to verify that the user is indeed using your hardware to run with the software.

LetsTrust TPM: a solid choice

The LetsTrust TPM is supported on the Raspberry Pi today, with multiple software stacks available – running on Linux and Windows 10 IoT Core.

The LetsTrust TPM can be used to evaluate the Optiga™ TPM for your design, but also as a ready-made component for your mass-market product. By using an Infineon hardware-based security application you will benefit from reduced engineering and support costs, compared to a custom-built security solution. To assist you with your needs, we provide hardware customization starting from 100 units.

How to get in touch with us

Please get in touch with us under **support@pi3g.com** with your application to discuss how the LetsTrust TPM platform can be of benefit to you today.

pi 3g
www.pi3g.com

pi3g e.K.

Sales & Technical Inquiries:
phone: +49 341 392 858 42
email: support@pi3g.com
web: www.pi3g.com

WEEE Reg Nr:
DE21378482

Company Register Nr:
HRA18308

LetsTrust TPM Datasheet

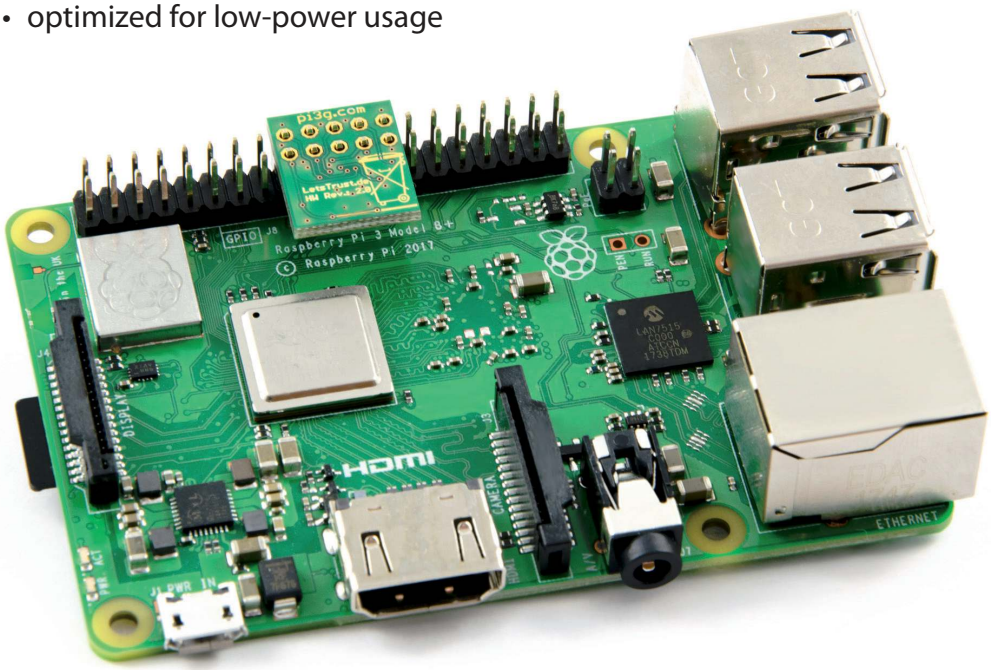
Hardware Version 2.0
Effective April 2021.

Core Hardware Specifications

- Infineon Optiga™ TPM SLB 9670 TPM2.0
- Compliant to TPM Main Specification, Family „2.0“, Level 00, Rev 01.16
- Common Criteria (EAL4+) certified
- Firmware >= 7.63 for TPM 2.0
- Certified TRNG (true hardware random number generator) built-in

Optiga™ TPM Specifications

- Full personalization with Endorsement Key (EK) and EK certificate
- 24 PCRs (SHA-1 or SHA-256)
- 7206 Byte free NV memory
- Up to 8 NV counters
- optimized for low-power usage



LetsTrust TPM is compatible with the Pi 3B+

pi3g e.K.

Sales & Technical Inquiries:

phone: +49 341 392 858 42
email: support@pi3g.com
web: www.pi3g.com

WEEE Reg Nr:

DE21378482

Company Register Nr:

HRA18308

LetsTrust TPM Datasheet

Hardware Version 2.0
Effective April 2021.

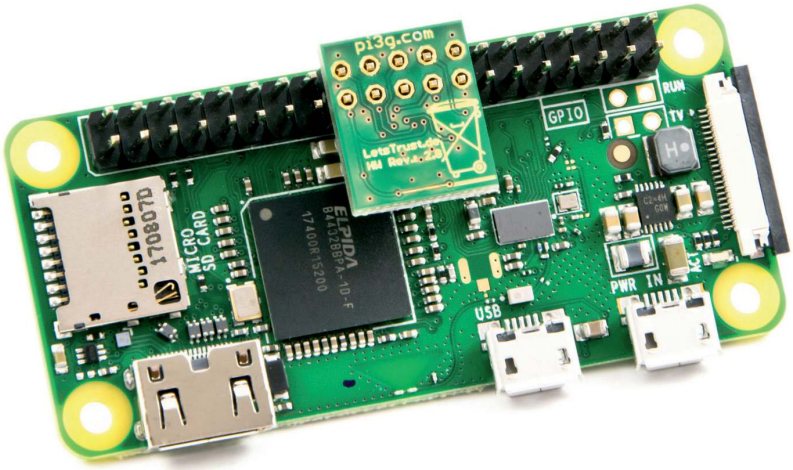
Raspberry Pi Hardware Support

- compact footprint - 2x5 pin header
- fits in most Raspberry Pi cases
- connects to Raspberry Pi GPIO pins 17 - 26
  - *the other GPIO pins of the Raspberry Pi can be freely used for other purposes*
- uses SPI to interface with the Raspberry Pi
  - *uses CS0.1 (SPI 0, chip select 1)*
  - *optional change to CS0.0 (SPI 0, chip select 0) possible by resoldering the resistor R3_CS1 to the position R2_CS0*
  - *please note: the warranty expires with this and any other soldering modifications*
  - *max SPI frequency: 33 MHz*
- reset & interrupt pins connected to the Raspberry Pi
- can be permanently installed on the Raspberry Pi by soldering

Software & Hardware Compatibility:

- compatible with all Raspberry Pi models
  (Pi Zero / Zero W / Pi 1/1B+ / 2 / 3, Pi 3B+)
- compatible with other SBCs following the Raspberry Pi header standard

- compatible with Raspbian and TPM2-Tools
  - *Mainline Linux Kernel support available since v4.10.*
  - *For Raspbian the support has to be enabled by recompiling the kernel*
  - *we provide an image for your convenience – alternatively use the WolfTPM software stack*
- compatible with Windows 10 IoT (Pi 2 / 3 / 3B+)
- compatible with TPM2-Software Stack (SAPI/ESAPI)
  - *TCG compliant software stack, including openSSL integration*
  - *https://github.com/tpm2-software*
- compatible with WolfTPM software stack
  - *portable TPM 2.0 project designed for embedded use*
  - *easy portability to different platforms – with examples for the Raspberry Pi platform*
  - *no kernel patching necessary*
  - *https://github.com/wolfSSL/wolfTPM*



LetsTrust TPM is compatible with the Pi Zero W

pi3g e.K.

Sales & Technical Inquiries:

phone: +49 341 392 858 42
email: support@pi3g.com
web: www.pi3g.com

WEEE Reg Nr:

DE21378482

Company Register Nr:

HRA18308

LetsTrust TPM Datasheet

Hardware Version 2.0
Effective April 2021.

Ratings & Ranges

- useful lifetime of the device:
  - *5 years+ (powered on 100 % of the time, used for calculations 5 % of the time)*
  - *7 years+ (powered on 70 % of the time, used for calculations 5 % of the time)*
- power consumption:
  - *18 mA while generating keys*
  - *<0.5 mA standby (@ 3,3 V)*
- temperature range:
  - *-20°..+85° C*
- dimensions:
  - *12.70 mm x 15.24 x 5.40 mm (width x length x height)*
- weight:
  - *1.11 g (LetsTrust TPM module)*
  - *3.12 g (packaged)*
- RoHS compliant

Application & Industry Examples

pi 3g
www.pi3g.com

Example Target Applications & Industries:

- Industrie 4.0
- industrial automation
- corporate access security
- IoT products
- industrial lighting products
- consumer products
- medical products
- security products
- cryptocurrency applications *(key storage, not calculation)*

Applications / Usage Examples:

- resource access and control management
- hardware & software protection against pirated copies / imitation products
- True Hardware Random Number Generator (thwrng)
  - *useful for generating secure SSH and session keys*
- Authentication / Signatures (Sign & Verify)
- Encryption
- secure key storage
- removable key-storage
- password protection
  - *(by preventing automated dictionary attacks)*
- home-partition encryption
- system integrity verification
- measured boot
  - *(not implemented yet on the Raspberry Pi platform)*

pi3g e.K.

Sales & Technical Inquiries:

phone: +49 341 392 858 42
email: support@pi3g.com
web: www.pi3g.com

WEEE Reg Nr:

DE21378482

Company Register Nr:

HRA18308

LetsTrust TPM Datasheet

Hardware Version 2.0
Effective April 2021.

pi 3g
www.pi3g.com

The pi3g Advantage

- developed & assembled in Germany
- short lead times for volume orders
- TPM is shipped with the newest available firmware
- hardware customization service available starting from 100 modules – inquire with **support@pi3g.com**