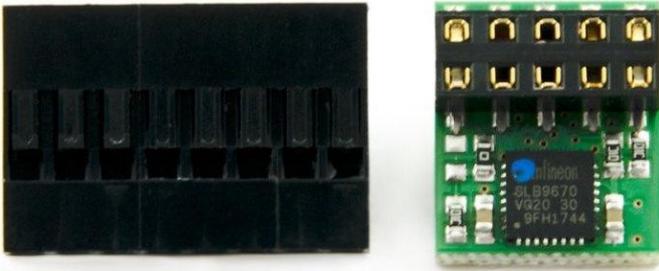




## LetsTrust TPM Kryptographiemodul für Raspberry Pi

pi<sup>3g</sup>

<b>N.º artículo:</b>	PI3G-LETST
<b>Hersteller:</b>	pi3g
<b>EAN:</b>	0700729578049
<b>Herkunftsland:</b>	Deutschland
<b>Zolltarifnummer:</b>	84718000
<b>Gewicht:</b>	0.003 kg



LetsTrust TPM ist eine einfach zu nutzende TPM (Trusted Platform Module) Lösung für den Raspberry Pi, basierend auf dem Infineon Optiga SLB 9670 TPM 2.0.

Ein Hardware TPM hat vielfältige Einsatzmöglichkeiten, unter anderem zur Authentifizierung / Signaturen, Speichern von Kryptoschlüsseln, u.v.m.

Das Modul kann auch als True Hardware Random Number Generator (TRNG) eingesetzt werden, wenn man eine gute Quelle für Zufall braucht!

LetsTrust TPM nutzt die SPI Schnittstelle um mit dem Pi zu kommunizieren. Es ist zu allen Raspberry Pi Singleboard Computern kompatibel (Pi 4, Pi 3B+, Pi 3, Pi 2, Pi 1, Pi Zero, Pi 400 mit Adapterkabel).

Kompakter Footprint, damit weitere GPIO-Pins ohne Probleme genutzt werden können: 2x5 Pins von Pin 17 bis Pin 26 sind durch LetsTrust belegt.

### **Rückgabebestimmungen**

Bitte beachten Sie, da es sich hier um ein Sicherheitsprodukt handelt, und dieses vom Widerruf ausgeschlossen ist, wenn Sie die Verpackung öffnen.

### **Technische Daten**

#### **TPM Features**

- Infineon Optiga SLB 9670 TPM 2.0
- Konform mit TPM Spezifikation 2.0 Rev. 01.38
- Firmware >= 7.85
- TRNG (Echter Zufallszahlengenerator) - True Hardware Random Number Generator

#### **Bauform & Schnittstelle**

- Schnittstelle zum Pi: SPI
- Kompatibel mit allen bisher erschienenen Raspberry Pi Modellen (u.a. Pi 3, Pi Zero, etc.)



- Kompakte Baugröße durch 2x5 Pinheader, dadurch bleiben die restlichen GPIO-Pins frei zur Verfügung
- mit Raspberry Pi Pins fest verlötbar
- passt in gängige Standardgehäuse mit herein

## Softwareunterstützung

- ab Raspbian Stretch mit dem Kernel 4.14.85 build in Support mit einem Device Tree Overlay
- Built-In Support für Windows 10 IoT (auf Pi 2, 3, 3B+)

## Software - Downloads

- [TPM2 Software](#)
- [ELTT2 Infineon Embedded Linux TPM Toolbox 2 for TPM 2.0](#) - Test, Diagnostik, etc. für den Infineon TPM Chip
- [Skriptbeispiele für den Einstieg & die Installation der TPM 2.0 Tools](#)

## Lieferumfang:

- LetsTrust TPM Modul
- 8-Pin Header (Installationhilfe, um korrekte Position für das TPM Modul ohne abzählen zu ermitteln)

## Besonderheiten:

- Die LetsTrust TPM Platine wird in Deutschland entwickelt
- Die Platinenfertigung von LetsTrust TPM erfolgt ausschließlich bei einem bayerischen Bestücker
- Das TPM ist optional fest verlötbar

## Weitere Bilder:

