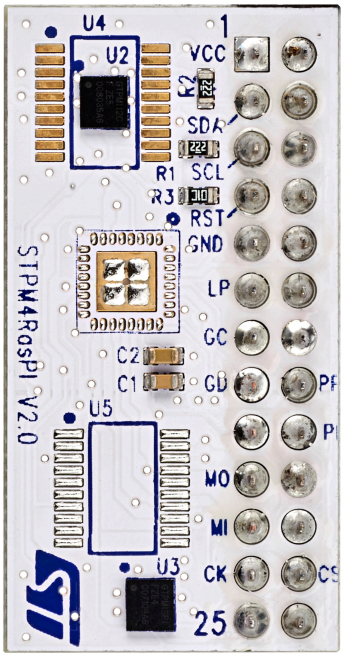
# STPM4RasPIV2

Data brief

## Raspberry Pi® extension board with an ST33 trusted platform module




## Features

- *I²C TPM*-compatible serial interface
- *SPI TPM*-compatible serial interface
- 26-pin female connector to plug to the Raspberry Pi®
- P1 connector (optional) to measure the TPM power consumption
- Features two STSAFE-TPM devices on the same board:
  - ST33GTPMISPI and ST33GTPMII2C
- For the evaluation of the:
  - ST33GTPMISPI and ST33GTPMII2C industrial-grade products
  - ST33GTPMASPI and ST33GTPMAI2C automotive-grade products

## Description

The STPM4RasPI is an official extension board to connect the STSAFE-TPM products to the Raspberry Pi® device. It is designed for development, proof of concept or demonstration activities. The board is shipped with one trusted platform module soldered (see ordering information for TPM product availability).

| Product status link |
| --- |
| STPM4RasPIV2 |

# 1 Main features

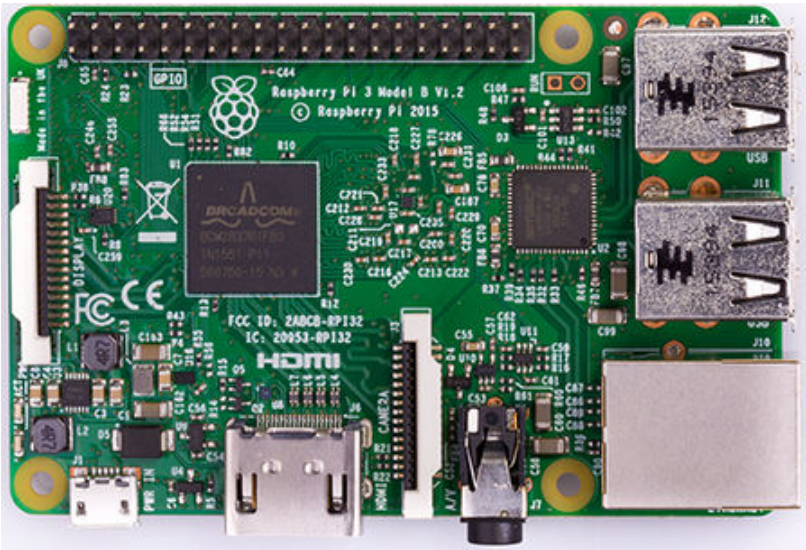
This section details the main features of STPM4RasPI, official extension board to connect the ST33 Arm®-based TPM products to the Raspberry Pi device.

*Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.*

## 1.1 Raspberry Pi® introduction

The Raspberry Pi 3 Model B is the third generation Raspberry Pi.

**Figure 1. Raspberry Pi 3 Model B**




The differences with the Raspberry Pi 2 are listed below:

- 1.2 GHz 64-bit quad-core ARMv8 CPU
- 802.11n wireless LAN
- Bluetooth® 4.1
- Bluetooth® low energy (BLE)

The common features with the Raspberry Pi 2 are listed below:

- 1-Gbyte RAM
- 4 USB ports
- 40 GPIO pins
- Full HDMI® port
- Ethernet port
- Combined 3.5 mm audio jack and composite video
- Camera interface (MIPI CSI-2®)
- Display interface (MIPI DSI®)
- microSD™ card slot (now push-pull rather than push-push)
- VideoCore® IV 3D graphics core

More details on this Raspberry Pi 3 are available on www.raspberry.org.

The STPM4RasPIV2 is compatible with all Raspberry Pi versions supporting 40 GPIO pins.

## 1.2 Raspberry SPI/I²C connectivity by GPIO

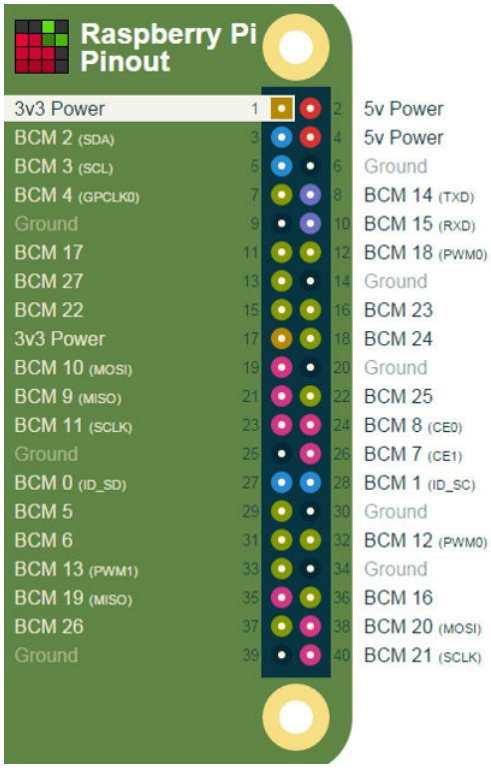
The SPI TPM products use the following signals:

- MOSI (pin 19)
- MISO (pin 21)
- SCLK (pin 23)
- CE0 (pin 24)
- VCC (pin 17)
- GND (pin 25)
- RST (pin 7)
- PIRQ (pin 18)
- PP (pin 16)

The I²C TPM products use the following signals:

- SDA (pin 3)
- SCL (pin 5)
- VCC (pin 1)
- GND (pin 6)
- RST (pin 7)
- PIRQ (pin 18)
- PP (pin 16)

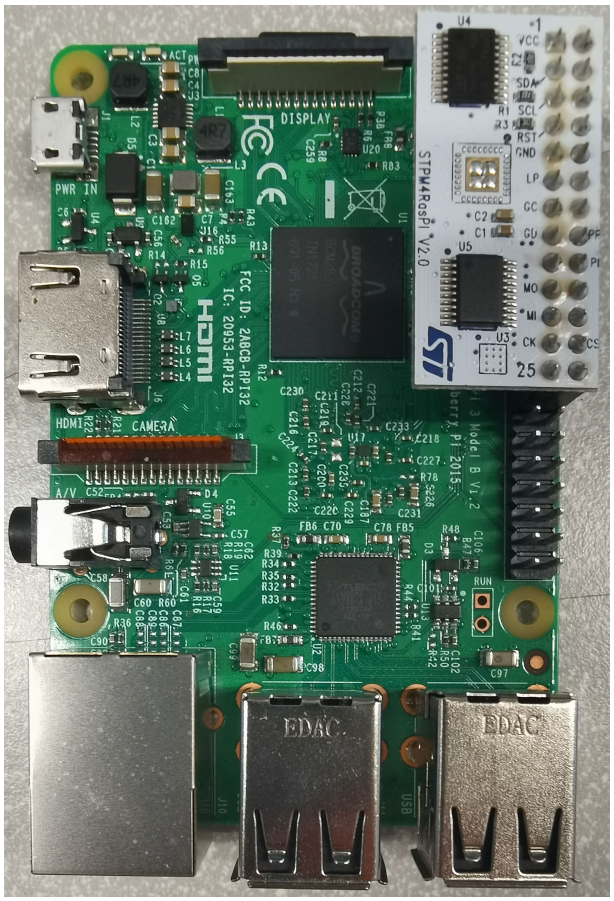
**Figure 2. Raspberry Pi GPIO**



## 1.3 STPM4RasPIV2 setup

The STPM4RasPIV2 fits perfectly in the standard Raspberry Pi® box. The STPM4RasPIV2 is connected to pins 1 to 26 of the Raspberry Pi® connector to provide compatibility with all Raspberry Pi® formats.

**Figure 3. STPM4RasPIV2 embedded in the Raspberry Pi® board**



# 2 Linux® integration requirements

## 2.1 TPM Linux® driver installation

Refer to AN5714 available from https://www.st.com, for information on TPM Linux® driver installation.

The information provided in this document is also compatible with the ST33GTPMISPI, ST33GTPMII2C, ST33GTPMASPI and ST33GTPMAI2C TPM devices.

**Caution:** Update the `spi-max-frequency` and `clock-frequency` in the *dts* file for the board according to the TPM product capacity.

Example:

```
spi-max-frequency = <15000000>;
clock-frequency = <100000>;
```

## 2.2 Installing both an I²C TPM and an SPI TPM in the Linux® environment

One new feature of the STPM4RasPIV2 compared to the STPM4RasPI is that it allows the connection of two industrial/automotive-grade TPM products to provide both the I²C and the SPI interfaces. The TPM products delivered with the board are the:

- ST33GTPMISPI and ST33GTPMII2C industrial-grade TPM products.

The STPM4RasPIV2 extension board can also be used to evaluate the ST33GTPMASPI and ST33GTPMAI2C automotive-grade products.

**Figure 4. STPM4RasPIV2 with the ST33GTPMISPI and ST33GTPMII2C**

In this case, two TPM Linux® drivers, one for I²C, the other for SPI, must be installed independently. This allows the use of the two TPM devices separately over two processes: `/dev/tpm0` and `/dev/tpm1`.

Figure 5. Linux® installation for two TPM devices

```
pi@raspberrypi:~S dmesg | grep -i tpm
[       13.553793] tpm_tis_spi spi0.0: 2.0 TPM (device-id 0x1, rev-id 78)
[       13.559340] tpm tpm0: A TPM error (256) occurred attempting the self test
[       13.559366] tpm tpm0: starting up the TPM manually
[       13.736060] tpm_tis_i2c 1-002e: 2.0 TPM (device-id 0x1, rev-id 78)
[       13.790619] tpm tpm1: A TPM error (256) occurred attempting the self test
[       13.790651] tpm tpm1: starting up the TPM manually
pi@raspberrypi:~S
```

# 3 Ordering information

The table below provides the commercial product name used to order the STPM4RasPIV2 extension board.

**Table 1. Ordering information**

| Commercial product | Description | TPM part numbers |
|---|---|---|
| SCT-TPM-RS2GTPMI | Features two industrial-grade TPM2.0 products (one with an SPI interface and the other with an I²C interface), TCG TPM2.0 spec 1.38, firmware version (3.257 (SPI TPM) 6.257 (I²C TPM)) | ST33GTPMISPI (ST33GTPMWLFZE4) and ST33GTPMII2C (ST33GTPMIWLFZE5) |

*Note: For the description of the soldered products and details on how to order them, refer to the data briefs of the corresponding TPM devices (TPM part numbers defined in the above table).*

*Note: The STPM4RasPIV2 extension board can also be used to evaluate the ST33GTPMASPI and ST33GTPMAI2C automotive-grade products. These products are indeed based on the same hardware platform and TPM firmware as the ST33GTPMISPI and ST33GTPMII2C industrial-grade products.*

## Revision history

Table 2. **Document revision history**

| Date | Revision | Changes |
|---|---|---|
| 03-May-2022 | 1 | Initial release. |

## Glossary

**3D** Three-dimensional

**BLE** Bluetooth® low energy

**CPU** Central processing unit

**GPIO** General purpose input/output

**HDMI®** High-definition multimedia interface

**I²C** Inter-integrated circuit

**LAN** Local area network

**MIPI CSI-2®** MIPI® Camera Serial Interface 2

**MIPI DSI®** MIPI® Display Serial Interface

**RAM** Random access memory

**SPI** Serial peripheral interface

**TCG** Trusted Computing Group®

**TPM** Trusted platform module

**USB** Universal serial bus

# Contents

# List of figures

**IMPORTANT NOTICE – READ CAREFULLY**

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.