Features

- I²C TPM compatible serial interface
- SPI TPM compatible serial interface
- 40-pin female connector to plug on Raspberry Pi®
- 40-pin male connector to probe signal or connect another extension board
- P1 connector (optional) to measure the TPM power consumption
- Supported ST33 TPM devices:
  - ST33TPHF20SPI, ST33TPHF2ESPI, ST33TPHF2XI2C, ST33TPHF20I2C, ST33TPHF2EI2C and ST33TPHF2XSPI in QFN32 package
  - ST33TPM12SPI and ST33TPM12I2C in TSSOP28 package

Description

STPM4RasPI is an official extension board to connect the ST33 TPM products to the Raspberry Pi® device. STPM4RasPI 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).
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.

![Raspberry Pi 3 Model B](image)

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-Byte RAM
- 4 USB ports
- 40 GPIO pins
- Full HDMI port
- Ethernet port
- Combined 3.5 mm audio jack and composite video
- Camera interface (CSI)
- Display interface (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 STPM4RasPI is compatible with all Raspberry Pi versions supporting 40 GPIO pins.
1.2 Raspberry SPI/I2C connectivity by GPIO

The ST33TPHF2xSPI product uses the following signals:

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

The ST33TPHF2xI2C product uses the following signals:

- SDA (pin 3)
- SCL (pin 5)
- SCLK (pin 23)
- VCC (pin 1)
- GND (pin 6)
- RST (pin 18)

Figure 2. Raspberry Pi GPIO
1.3 STPM4RasPI setup
STPM4RasPI fits perfectly in standard Raspberry Pi box. STPM4RasPI lets the GPIO pin available for probing or connect another extension board.

If the height size is critical for the system and the GPIO availability is not needed, some specific STPM4RasPI exists without it (contact the local STMicroelectronics sales office).

**Figure 3. STPM4RasPI embedded in Raspberry Pi board**

![Image of STPM4RasPI embedded in Raspberry Pi board](image1)

**Figure 4. STPM4RasPI embedded in Raspberry Pi box with touch screen**

![Image of STPM4RasPI embedded in Raspberry Pi box with touch screen](image2)

1.4 TPM power consumption
P1 pin header can be soldered to plug multimeter over a 10 Ω resistor (R4) and defined TPM power consumption.

**Figure 5. P1 header location**

![Image of P1 header location](image3)
2 Linux® integration requirements

2.1 TPM Linux driver introduction

The TPM Linux driver is included in Linux/drivers/char/tpm directory:

ST33TPM12I2C with I²C interface and ST33TPM12SPI with SPI interface, use a proprietary Linux driver included under Linux/drivers/char/tpm directory:

ST33TPHF2xSPI for SPI and ST33TPM12LPC for TCG, are TCG compliant and both support the following standard TCG Linux drivers:

- tpm_tis.c
- tpm_tis_spi.c

Figure 6. TPM directory example in Linux kernel

```
Mode Name
-rw-r--- Kconfig
-rw-r--- Makefile
dr-------- st33zp24
-rw-r--- tpm-chip.c
-rw-r--- tpm-dev-common.c
-rw-r--- tpm-dev.c
-rw-r--- tpm-dev.h
-rw-r--- tpm-interface.c
-rw-r--- tpm-sysfs.c
-rw-r--- tpm.h
-rw-r--- tpm1_eventlog.c
-rw-r--- tpm2_cmd.c
-rw-r--- tpm2_space.c
-rw-r--- tpm2_eventlog.c
-rw-r--- tpm_spi.c
-rw-r--- tpm_crb.c
-rw-r--- tpm_eventlog.h
-rw-r--- tpm_nsec.c
-rw-r--- tpm_of.c
-rw-r--- tpm_ppl.c
-rw-r--- tpm_tis.c
-rw-r--- tpm_tis_core.c
-rw-r--- tpm_tis_core.h
-rw-r--- tpm_tis_spi.c
-rw-r--- tpm_vtcm_proxy.c
-rw-r--- tpm_devm.c
-rw-r--- xen-tpmfront.c
```

The TCG TPM driver is functional from Linux kernel 4.8. In the config spec, check if all labels listed below are inserted:

- CONFIG_TCG_TPM = y
- CONFIG_TCG_TIS_CORE = y
- CONFIG_TCG_TIS_SPI = y or m
2.2 Porting new kernel by activating TPM

Follow the steps listed below:
1. Upgrade new Linux kernel (version ≥ 4.8).
2. Check the tutorial available in the documentation/linux/kernel/building page at https://www.raspberry.org.
3. Run the local building: in menu>Preferences>Raspberry PI Configuration, activate the I2C and SPI interfaces item and disable the underscan system item.
4. Open the terminal with the code below.

```
$ sudo -I
#sudo apt-get install bc
#cd /home/pi/Downloads
#git clone -b rpi-4.14.y --depth=1 https://github.com/raspberrypi/linux
```

2.3 Device tree file update for SPI

The DTS (device tree source) configuration (bcm27* files) is done with the following code.

```
#cd /home/pi/Downloads/linux/arch/arm/boot/
#chmod 777 dts
#cd dts
#chmod 777 bcm27*

Replace in all bcm27* files
---------------------------------
spidev0: spidev@0{
    compatible = "spidev";
    reg=<0>; /* CE0 */
    #address-cells = <1>;
    #size-cells = <0>;
    spi-max-frequency = <500000>;
};
----------------------------------

Replace by
st33htpm0: st33htpm@0{
    status="okay";
    compatible = "st, st33htpm-spi";
    reg = <0>;
    #address-cells = <1>;
    #size-cells = <0>;
    spi-max-frequency = <10000000>;
};
```

```
2.4 Device tree file updated for I2C

The I2C TPM driver compatible TCG implementation is not yet available by default in Linux kernel. Contact one local STMicroelectronics sales office to obtain it.

The DTS configuration (bcm27* files) is done with the following code.

```bash
#cd /home/pi/Downloads/linux/arch/arm/boot/
#chmod 777 dts
#cd dts
#chmod 777 bcm27*

Replace in all bcm27* files
---------------------------------
&i2c1 {  pinctrl-names = "default";
    pinctrl-0 = <&i2c1_pins>;
    clock-frequency = <100000>;
};
replaced by
&i2c1 {  pinctrl-names = "default";
    pinctrl-0 = <&i2c1_pins>;
    clock-frequency = <400000>;
    st33htpi: st33htpi@0{
        compatible = "st,st33htpm-i2c";
        reg = <0x2E>;
        status="okay";
    };
};
----------------------------------
```

2.5 Configuration spec update

Update bcmrpi_defconfig and bcm2709_defconfig files with the following code.

```bash
#cd /home/pi/Downloads/linux/arch/arm
#chmod 777 configs
#cd configs
#chmod 777 bcm*

Bcmrpi_defconfig (RPI 1) and bcm2709_defconfig (RPI 2/3) should be updated :
-----------------------------------
Config spec we add TCG TPM driver directly in Linux kernel (in Red SPI Only in Purple I2C only): m means modules driver is not loaded in linux kernel during platform starting. Modules should be enabled.
-----------------------------------
CONFIG_TCG_TPM=y
CONFIG_CRC_CCITT=y
CONFIG_TCG_TIS_CORE=y
CONFIG_TCG_TIS_SPI=m
CONFIG_TCG_TIS_I2C=m
CONFIG_TCG_TIS_ST33SP24=m
CONFIG_TCG_TIS_ST33SP24_SPI=m
CONFIG_TCG_TIS_ST33SP24_I2C=m
```
2.6 Kernel compilation
The kernel compilation is done with the following code.

```
---------------------
Configuration to compile RPI 2/3
---------------------
#cd /home/pi/Downloads/
#cd linux
#KERNEL=kernel2
#make bcm2709_defconfig
or
---------------------
Configuration to compile RPI
---------------------
#cd /home/pi/Downloads/
#cd linux
#KERNEL=kernel
#make bcmrpi_defconfig
---------------------
Start to compile
---------------------
#sudo apt-get install bc
#make -j4 zImage modules dtbs
#sudo make modules_install
#sudo cp arch/arm/Boot/dts/*.dtb /boot/
#sudo cp arch/arm/boot/dts/overlays/*.dtb* /boot/overlays/
#sudo cp arch/arm/boot/dts/overlays/README /boot/overlays/
#sudo ./scripts/mkknlimg arch/arm/boot/zImage /boot/$KERNEL.img
```

2.7 TPM driver loading check
When the TPM driver is loaded, /dev/tpm0 and /dev/tpmrm0 are present, as shown in the figure below.

*Figure 7. Raspbian windows*
The STPM4RasPI extension board can be ordered using commercial product names listed in the table below.

### Table 1. Ordering information

<table>
<thead>
<tr>
<th>Commercial product</th>
<th>Description</th>
<th>Product soldered</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCT-TPM-RASPIAF3</td>
<td>TPM2.0 only, TCG TPM2.0 spec 1.16, firmware version 4A.00, SPI interface</td>
<td>ST33HTPH2032AAF3</td>
</tr>
<tr>
<td>SCT-TPM-RASPIHB4</td>
<td>TPM2.0 (default)/TPM1.2, TCG TPM2.0 spec 1.16, firmware version 49.04, SPI interface</td>
<td>ST33HTPH2E32AHB4</td>
</tr>
<tr>
<td>SCT-TPM-RASPIHC0</td>
<td>TPM2.0 (default)/TPM1.2, TCG TPM2.0 spec 1.38, firmware version 49.08, SPI interface</td>
<td>ST33HTPH2E32AHC0</td>
</tr>
<tr>
<td>SCT-TPM-RASPIHC1</td>
<td>TPM2.0 (default)/TPM1.2, TCG TPM2.0 spec 1.38, firmware version 4A.08, SPI interface</td>
<td>ST33HTPH2032AHC1</td>
</tr>
<tr>
<td>SCT-TPM-RASPIHC2</td>
<td>TPM2.0 (default)/TPM1.2, TCG TPM2.0 spec 1.38, firmware version 49.09, I2C interface</td>
<td>ST33HTPH2E32AHC2</td>
</tr>
</tbody>
</table>
Revision history

Table 2. Document revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-Mar-2019</td>
<td>1</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
List of figures

Figure 1. Raspberry Pi 3 Model B .............................................................. 2
Figure 2. Raspberry Pi GPIO ................................................................. 3
Figure 3. STPM4RasPI embedded in Raspberry Pi board ............................................. 4
Figure 4. STPM4RasPI embedded in Raspberry Pi box with touch screen .................................. 4
Figure 5. P1 header location ................................................................. 4
Figure 6. TPM directory example in Linux kernel. .................................................... 5
Figure 7. Raspbian windows ........................................................................ 8
IMPORTANT NOTICE – PLEASE 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 acknowledgement.

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, please 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.

© 2019 STMicroelectronics – All rights reserved