TPM hardware components

Contents

TPM hardware components

Stable: 19.02.2019 - 08:53 / Revision: 13.02.2019 - 07:18

Template:ArticleMainWriter Template:ArticleApprovedVersion

Contents

1 Article Purpose

TPM is an international standard for a secure cryptoprocessor[1] designed to secure hardware through integrated cryptographic keys.

TPM includes a high security level and a security certification, that is graduated with the evaluation assurance level (EAL)[1].

The purpose of this article is to:

- list the TPM hardware components that might be connected to the different boards
- link these components to the corresponding software framework(s)
- point to the component datasheets
- explain, when necessary, how to configure these components.

2 Software frameworks

Do	Peri	Software frameworks	Comment
Cortex-A7	Cortex-A7 no	Cortex-M4	

Domain	Peri	Software frameworks			Comment
secure (OP-TEE)	non-secure (Linux)	(STM32Cube)			
Security	TPM		TPM Software Stack[2]		

3 ST33TPM12

3.1 Description

The ST33TPM12 is built on a 32-bit ARMTemplate:Sup reduced instruction set computing (RISC) processor which provides high cryptographic and general performances. A NESCRYPT crypto-processor is also provided to efficiently support all public key cryptographic algorithms.

With ST33TPM12 devices, ST provides an EAL4+ certified solution embedding a secure cryptoprocessor with dedicated hardware accelerators that improve the global platform security.

Multiples services are available using TPM (mostly in PC and mobile devices):

- Cryptographic keys generation, protection, management and utilization
- Cryptographic device identity
- Secure logging, log-reporting and attestation
- Secure non volatile storage
- Other functions including hashing, random number generator and secure clock

Several use cases are available:

- Platform integrity: the boot process relies on TPM for software integrity and authentication during each boot stage
- Disk encryption: encrypt and decrypt drive using TPM crypto core
- Password protection, ...

The STM33TPM12 is provided with different interfaces:

- I2C : ST33TPM12I2C[3]
- SPI : ST33TPM12SPI[4]
- LPC : ST33TPM12SPI[5]

3.2 Support in Linux Kernel

TPM is ready to be used with OpenSTLinux distribution.
The TPM drivers (I2C and SPI) are part of the following kernel driver bindings:
Documentation/devicetree/bindings/security/tpm/st33zp24-i2c.txt
Documentation/devicetree/bindings/security/tpm/st33zp24-spi.txt
Source code:
drivers/char/tpm/st33zp24/i2c.c
drivers/char/tpm/st33zp24/spi.c
TPM support relies on a TCG[1] open source TPM2 Software Stack (TSS)[2].

3.3 Support in U-BOOT

TPM is supported with existing uclass of the 'Driver Model'.

- tpm
  - uclass: drivers/tpm/tpm-uclass.c .
  - driver: drivers/tpm/tpm_tis_st33zp24_i2c.c
  - driver: drivers/tpm/tpm_tis_st33zp24_spi.c

4 References

- 1.01.11.2 Trusted Computing Group
- 2.02.1 https://github.com/tpm2-software/tpm2-tss
- https://www.st.com/content/st_com/en/products/secure-mcus/authentication-secure-iot/trusted-computing-solutions/st33tpm12i2c.html
- https://www.st.com/content/st_com/en/products/secure-mcus/authentication-secure-iot/trusted-computing-solutions/st33tpm12spi.html
- https://www.st.com/content/st_com/en/products/secure-mcus/authentication-secure-iot/trusted-computing-solutions/st33tpm12lpc.html

Trusted Platform Module

Evaluation Assurance Level

Open Portable Trusted Execution Environment

Inter-Integrated Circuit (Bi-directional 2-wire bus standard for efficient inter-IC control.)

Serial Peripheral Interface

Trusted Computing Group

TPM Software Stack

Category:ST boards

This category groups together all articles related to any STMicroelectronics board.

Pages in category "ST boards"

The following 8 pages are in this category, out of 8 total.

M

- MB1230
- MB1262
- MB1263
- MB1272
- MB1379
- MB1407

S

- STM32MP157C-EV1 - hardware description
- STM32MP157X-DKX - hardware description

Permission error

Stable: 10.10.2019 - 12:43 / Revision: 10.10.2019 - 12:42

You do not have permission to read this page, for the following reason:

The action "Read pages" for the draft version of this page is only available for the groups ST_editors, ST_readers, Selected_editors, sysop, reviewer