



Category:Trusted Firmware-A (TF-A)

---

Category:Trusted Firmware-A (TF-A)



---

## Contents

---

1. Category:Trusted Firmware-A (TF-A) .....	3
2. Clock device tree configuration - Bootloader specific .....	4
3. STM32MP15 TF-A .....	4
4. TF-A - Flash memory configuration .....	4
5. TF-A - How to debug .....	4
6. TF-A overview .....	5



---

A quality version of this page, approved on 17 June 2020, was based off this revision.

This category groups together all articles related to software components managing the Trusted Firmware-A (TF-A) ( with "A" meaning Arm<sup>®</sup>Cortex<sup>®</sup>-A).

Trusted Firmware for Arm Cortex-A

Arm<sup>®</sup> is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.



Cortex<sup>®</sup>



## Pages in category "Trusted Firmware-A (TF-A)"

The following 5 pages are in this category, out of 5 total.

- [TF-A overview](#)
- [STM32MP15 TF-A](#)
- [Clock device tree configuration - Bootloader specific](#)
- [TF-A - Flash memory configuration](#)
- [TF-A - How to debug](#)

Stable: 09.12.2020 - 13:13 / Revision: 07.12.2020 - 12:45

This category groups together all articles related to software components managing the Trusted Firmware-A (TF-A) ( with "A" meaning Arm<sup>®</sup>Cortex<sup>®</sup>-A).

Trusted Firmware for Arm Cortex-A

*Arm<sup>®</sup> is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.* 

**Cortex<sup>®</sup>**

Stable: 08.01.2021 - 14:59 / Revision: 08.01.2021 - 14:59

This category groups together all articles related to software components managing the Trusted Firmware-A (TF-A) ( with "A" meaning Arm<sup>®</sup>Cortex<sup>®</sup>-A).

Trusted Firmware for Arm Cortex-A

*Arm<sup>®</sup> is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.* 

**Cortex<sup>®</sup>**

Stable: 12.10.2020 - 12:02 / Revision: 12.10.2020 - 12:01

This category groups together all articles related to software components managing the Trusted Firmware-A (TF-A) ( with "A" meaning Arm<sup>®</sup>Cortex<sup>®</sup>-A).

Trusted Firmware for Arm Cortex-A

*Arm<sup>®</sup> is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.* 

**Cortex<sup>®</sup>**

Stable: 08.01.2021 - 15:47 / Revision: 08.01.2021 - 15:47

This category groups together all articles related to software components managing the Trusted Firmware-A (TF-A) ( with "A" meaning Arm<sup>®</sup>Cortex<sup>®</sup>-A).

Trusted Firmware for Arm Cortex-A

*Arm<sup>®</sup> is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.* 

**Cortex<sup>®</sup>**


Stable: 17.02.2021 - 19:40 / Revision: 16.02.2021 - 16:25



---

This category groups together all articles related to software components managing the Trusted Firmware-A (TF-A) ( with "A" meaning Arm<sup>®</sup>Cortex<sup>®</sup>-A).

Trusted Firmware for Arm Cortex-A

Arm<sup>®</sup> is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere. 

Cortex<sup>®</sup>