**Trusted Firmware** provides a reference implementation of secure world software for Armv8-A and Armv8-M. It provides SoC developers and OEMs with a reference trusted code base complying with the relevant Arm specifications.

The code on this website is the preferred implementation of Arm specifications, allowing quick and easy porting to modern chips and platforms. This forms the foundations of a **Trusted Execution Environment (TEE)** on application processors, or the **Secure Processing Environment (SPE)** of microcontrollers.

**Available Trusted Firmware Projects**

- TF-A
- TF-M
- OP-TEE
- Mbed TLS
- PSA Crypto
- Hafnium

**Our Members**

- ARM
- Cypress
- Data I/O
- Futurewei Technologies
- Google
- Linaro
- NXP
- Renesas
- STI
- Texas Instruments

**GENERAL ENQUIRIES**

For general and membership enquiries: enquiries@trustedfirmware.org

Harston Mill
Royston Rd, Harston
Cambridge, United Kingdom
CB22 7GG

**LATEST NEWS & BLOGS**

- TF-M open Tech Forum regular call
  - June 25, 2020
- TF-A open Tech Forum regular call
  - June 11, 2020
- Trusted Firmware-A & TF-A-Tests v2.3 ...
  - April 30, 2020
- Renesas Electronics and NXP Semicondu...
  - March 25, 2020
The Trusted Firmware-A project provides a reference implementation of secure world software for Armv7-A and Armv8-A class processors.

The Projects page provides access to all facilities hosted including source code, documentation, Gerrit review for submitting changes, a wiki, the issue/task workboard/tracker as well as showing recent activity in the project.

Contribution guidelines can be found in the documentation and a getting started guide with Gerrit can be found on the wiki.

A project email list can be subscribed to to participate in development discussions.

A bi-weekly Technical Forum call is held to discuss technical subjects.

For general and membership enquiries:
enquiries@trustedfirmware.org

Useful links

- Useful link one
- Useful link two
- Useful link three
- Useful link four
- Useful link five
The Trusted Firmware-A project provides a reference implementation of secure world software for Armv7-A and Armv8-A class processors.

The Projects page provides access to all facilities hosted including source code, documentation, Gerrit review for submitting changes, a wiki, the issue/task workboard/tracker as well as showing recent activity in the project.

Contribution guidelines can be found in the documentation and a getting started guide with Gerrit can be found on the wiki.

A project email list can be subscribed to to participate in development discussions.

A bi-weekly Technical Forum call is held to discuss technical subjects.

For general and membership enquiries:
enquiries@trustedfirmware.org

For general and membership enquiries:
enquiries@trustedfirmware.org

Harston Mill
Royston Rd, Harston
Cambridge, United Kingdom
CB22 7GG

Copyright © 2020 Linaro Limited    |    Legal    |    Contact

LATEST NEWS & BLOGS

TF-M open Tech Forum regular call
June 25, 2020

TF-A open Tech Forum regular call
June 11, 2020

Trusted Firmware-A & TF-A-Tests v2.3...
April 30, 2020

Renesas Electronics and NXP Semicondu...
March 25, 2020