



# TrustedFirmware

OPEN SOURCE SECURE WORLD SOFTWARE

**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.

## Projects available from Trusted Firmware



[GENERAL ENQUIRIES](#)



# What is Trusted Firmware A (TF-A)



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.

## Available resources

**code**index : [trusted-firmware-a.git](#)**docs**[Trusted Firmware-A Documentation](#)**review**[Gerrit : TF-A/trusted-firmware-a](#)**wiki**[Phabricator : Trusted Firmware-A \(TF-A\)](#)**issues**[Phabricator : Trusted Firmware-A \(TF-A\)](#)**security**[Trusted Firmware-A \(TF-A\)](#)[SUBSCRIBE to the TF-A mailing list](#)

## Other projects

TF-M

TF-A  
Testing

OP-TEE

Mbed  
TLSPSA  
Crypto

Hafium

For general and membership enquiries:

[enquiries@trustedfirmware.org](mailto:enquiries@trustedfirmware.org)