TF-A

TF-A

TF-A(Trusted Firmware-A)ARM®TF-AArmv8-A STMicroelectronicsArmv7-A Trusted FirmwareLinaroBSD-3-Clause

Trusted boot chainTF-A FSBL

The global architecture of TF-A is explained in the Trusted Firmware-A design [8] document.

TF-A

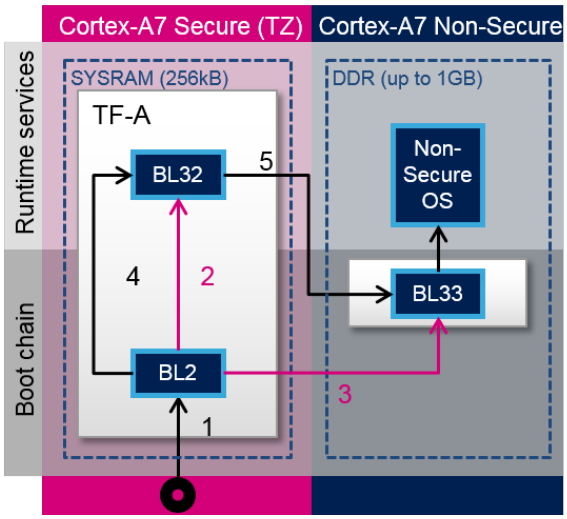
- Boot loader stage 1 (BL1) application processor trusted ROM
- Boot loader stage 2 (BL2) trusted boot firmware
- Boot loader stage 3-2 (BL32) runtime software
- Boot loader stage 3-3 (BL33) non-trusted firmware

BL1, BL2BL32TF-ABL33TF-A

BL1 BL2_AT_EL3BL1PanGuROM codeBL2BL1BL2PanGu

BL33TF-ASSBLPanGuSSBLU-Boot

PanGuBL2 BL32device treebinaryROMSYSRAM



TF-

1. ROM codeTF-A binaryBL2
2. BL2 BL32
3. BL2 BL33
4. BL2 BL32
5. BL32 BL33

TF-A

TF-A

```
$ cd $HOME/PanGu
$ tar xvf arm-trusted-firmware.tar.gz
```

TF-AMakefile.sdk

Makefile.sdk

```
$ mv ~/Makefile.sdk $HOME/PanGu
$ make -f ../Makefile.sdk  TFA_DEVICETREE=stm32mp157a-panguboard
TF_A_CONFIG=trusted ELF_DEBUG_ENABLE='1' all
```

build$HOME/PanGu/buildtf-a-stm32mp157a-panguboard.stm32