We provide a program level file authorization program, which is used to protect a executable file running on the embedded compute such as the Raspberry PI. The program is based on the OP-TEE which is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm.

The program contains 3 part of program:

1. The program to do the file signature/checksum calculation and message encryption which running the TrustZone ( Secure word on the Raspberry PI)
2. The client program running in the normal word to connect to fetch the file need to check and connect to the server.
3. A server program to authorize the Integrity of the file running in the raspberry PI.

We are using the technology provide by OP-TEE c/o Linaro.

--

Our program will do 5 steps to authorize the integrity of the file:

Step1: