

Chapter 1

Background

The smartphone that will be used is a PinePhone which is equipped with ARM TrustZone, it also comes with a component which can be used as Root of Trust to make secure boot possible.

1.1 PinePhone

The PinePhone is an open source smartphone which supports Linux as operating system which adds to it's openness.

1.2 Trusted Execution Environment

A Trusted Execution Environment is a secure, integrity-protected processing environment, consisting of memory and storage capabilities.

1.3 ARM TrustZone

ARM TrustZone is ARM's implementation of a TEE. This is achieved by having a secure and normal world in the System on Chip.

1.4 Chain of Trust

To trust an application, the environment in which this application runs also needs to be trusted which often translates to the operating system, bootloader, hardware,...

1.5 Secure Boot

Secure boot is a booting process in which a Root of Trust is used to make sure that the code used for booting is not tampered with.