BayTrail Verified Boot

Secure Boot with TXE, FSP and coreboot on MinnowBoard Turbot

Description:

This demo presents Secure Boot implementation based on **coreboot** and **FSP** from the system power on to the launch of coreboot payload.

Secure Boot is a process that validates firmware images on the system before they are allowed to execute. Starting with a root of trust, Secure Boot cryptographically validates the **hash** or **digital signature** of all boot components in a boot loader. Secure boot helps to ensure that only authorized code can execute before the operating system loads.

The Secure Boot is achieved by utilizing hardware Root of Trust provided by **Trusted Execution Engine** (TXE), which verifies the Initial Boot Block (IBB). The rest of the firmware components is verified using open source **Verified Boot** implementation.

Elements:

- MinnowBoard Turbot Quad
- RTE used for remote connection and programmer
- monitor with serial output

Visit 3mdeb.com
for more details.