# 1 Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT Nodes

To enforce integrity of IoT devices, the load-time and run-time integrity needs to be taken into account. Using a root of trust and a paging based process integrity measurement method this can be achieved.

## 1.1 Introduction

IoT devices are being attacked in multiple different methods like hardware attacks, OS/firmware attacks and software attacks. ARM TrustZone is used to ensure both load- and run-time integrity. Load-time integrity is achieved by starting from a root of trust and using secure boot. A paging-based process integrity measurement method and attestation is used to achieve run-time integrity.

## 1.2 Background

ARM TrustZone, Secure and Trusted boot.

## 1.3 System overview

The attackers are assumed to be able to launch hardware, OS/framework and software attacks. It is assumed that programs in On Chip ROM, SW runtime and the remote attestation servers are all secure. Attacks like bus snooping, cold boot and cache side channel are out of scope.

## 1.4 Hybrid booting approach

The Root of Trust is established using the eFuse and the OCROM. Secure boot is used for the Secure World to ensure it's integrity. First the second-stage bootloader image and secure OS kernel are measured and signed offline. Secondly a Chain of Trust is established by verifying the images before giving them control. The Secure World forms the trusted base for the trusted boot of the Normal World. The trusted boot for the NW involves two phases: the offline hash chain calculation phase, and the online trusted boot phase. Furthermore, the remote attestation key needs to be securely stored in the flash memory.

## 1.5 Paging-based process integrity measurement and attestation method

The programs of the normal world need to be attested during run-time because attackers could inject malware or exploit vulnerabilities. The text

section of the code is divided into pages, every page is hashed and this value is saved on the attestation server. The secure world measures the code segments of each process periodically. These measurements are sent to the attestation server to complete the attestation process.

## 1.6 Evaluation

## 1.7 Security analysis and limitations

## 1.8 Related work

## 1.9 Conclusion