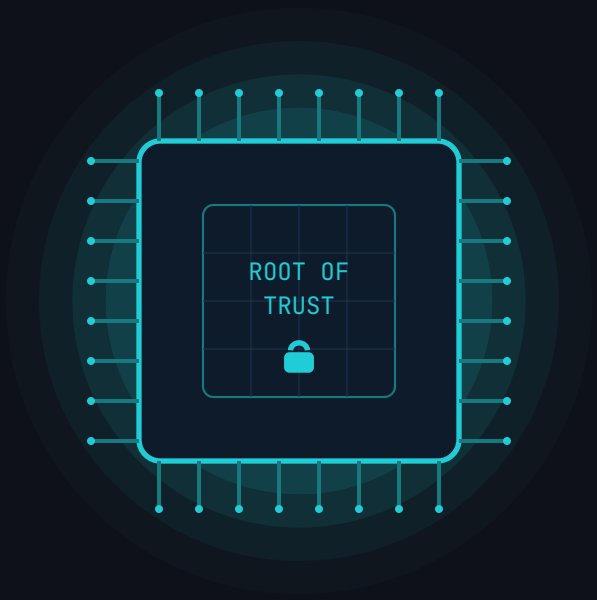


Secure Boot

A Visual Guide

Root of Trust • Hardware Fuses • Public Key Cryptography
Digital Signatures • Bootloader Chains • Certificate Chains

Understanding how modern devices establish trust from power-on

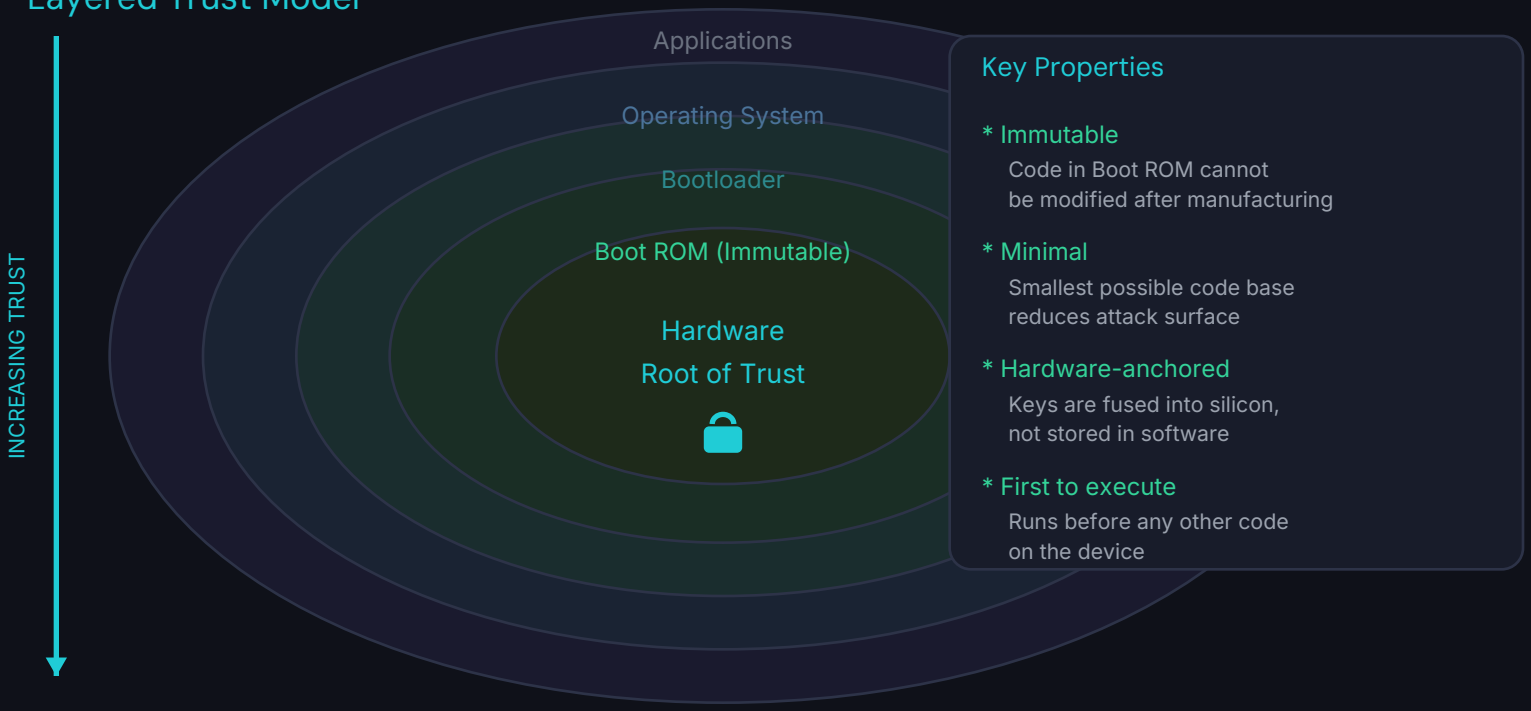
Contents

01 Root of Trust

The immutable foundation all security builds upon

The Root of Trust (RoT) is a hardware component that is inherently trusted because it cannot be modified. Everything in the secure boot chain derives its trust from this single, immutable starting point burned into the silicon at manufacturing time.

Layered Trust Model



Key Properties

* **Immutable**
  Code in Boot ROM cannot be modified after manufacturing
* **Minimal**
  Smallest possible code base reduces attack surface
* **Hardware-anchored**
  Keys are fused into silicon, not stored in software
* **First to execute**
  Runs before any other code on the device

Real-World Implementations

AMD PSP
ARM Cortex-A5 co-processor embedded in SoC

ARM TrustZone
Hardware partitioned secure/non-secure worlds

Apple Secure Enclave
Dedicated security processor with own Boot ROM

Qualcomm SPU
Secure Processing Unit in Snapdragon