Concept	Definition	Relation
Root of Trust (RoT)	A hardware-anchored, immutable block of code that the CPU always executes first; is a source that can always be trusted within a cryptographic system	Every other check ultimately relies on the RoT's public key that's embedded into silicon or one-time-programmable (OTP) memory
Cryptographic Signature	A digital fingerprint created with a private key (PrK); anyone with the matching public key can verify integrity and authenticity	Gives mathematical concept to the RoT and every subsequent stage: each image in the boot flow must have a valid signature
Secure Boot	The process that, on every reset, lets code run only if its signature checks out; execution halts on any failure	Operationalizes the RoT: the immutable code performs the first signature check, then delegates to the next stage
Chain of Trust	A step-by-step extension of trust where each stage (Boot ROM, 1st-stage bootloader, OS/RTOS, app) authenticates the next before handing over control	Break one link and the chain (boot) stops
Arm TrustZone-M	Hardware partitioning that splits the MCU into Secure and Non-Secure worlds, each with its own code, data, and interrupt space	Protects secret keys & RoT code from Non-Secure firmware. Only after a stage is authenticated does the chain cross the Secure/Non-Secure boundary