

Bootloader Extension Verified Firmware Boot

Overview

Verified Firmware Boot is an optional upgrade of the firmware update bootloader. Instead of only checking the technology firmware (TFW) with a CRC32 for accidental corruption, the bootloader authenticates it cryptographically before it ever runs.

An ECDSA P-256 / SHA-256 signature over the entire firmware image is verified at every device start-up and again immediately after every firmware update. If the check fails, the device stays in the bootloader and unauthenticated code never runs; in this safe state it still accepts a new update.

Functional Description

Both places in the bootloader that can hand control to the firmware route through the same signature check first, there is no third path into the application image. In signature mode a 64-byte signature at offset 0x204 replaces the 4-byte CRC32 of the standard build. The size field is authenticated and the signature field itself is hashed as zero; application code starts at offset 0x244.

Features

- Signature: ECDSA, NIST P-256 (secp256r1); hash: SHA-256 over the entire image
- Public key (64 bytes) embedded in the bootloader, not writable via the update channel
- Fails closed: unauthenticated code never runs
- Fault-injection resistant: the signature check cross-validates an independent fault-check result
- Crypto library: STMicroelectronics CMOX (X-CUBE-CRYPTOLIB)
- Additional footprint: RAM +2.0 kB / Flash +18.75 kB (vs. the standard CRC32 build)

Security Notes

- No rollback protection: a validly signed older firmware image can still be reflashed
- Root of trust: the bootloader and its embedded key must remain immutable in the field
- Enable the MCU readout/debug protection (RDP) on production units

Integration Note

- The image header must reserve the full 68 bytes: 4-byte size plus 64-byte signature
- Reserving only the older 8-byte CRC layout lets the signing tool overwrite application code
- Enabled per production build; contact TEConcept to enable it for your build

