FOR EMBEDDED DEVICE MANUFACTURERS

Signing and device identity for embedded teams. Live in days, not months.

The PKI and signing platform for CRA-ready devices

EU CYBER RESILIENCE ACT

CRA Annex I requires integrity protection, secure updates and protection against unauthorised access. Secure boot, signed firmware and device identity are the technical controls behind these requirements.

11 Sep 2026
Vulnerability and incident reporting obligations apply

11 Dec 2027
Full obligations: secure by design, conformity assessment, CE marking

EUR 15M or 2.5%
Maximum penalty, of global annual turnover

THREE PILLARS

Built for embedded

We speak your silicon and your update format, with a step-by-step guide for each.

Onboarding in days

LAAVAT plugs into the tools your team already uses. Connect your identity provider (Entra ID or Google), and your engineers sign from their own pipeline within days.

One platform for keys and signing

HSM-protected key management, secure boot and update signing, image encryption and device identity from factory to field. Governed by approvals and a complete audit trail.

TECHNICAL FACTS

Secure boot	NXP HAB and AHAB, AMD/Xilinx Bootgen, MCUboot on STM32, Nordic, Renesas and Microchip, Texas Instruments, Raspberry Pi, ESP32, UEFI secure boot
Update formats	FIT, RAUC, Mender, SWUpdate
Other signing	OP-TEE apps, OCI containers, Windows binaries, kernel modules, IMA
Device identity	IEEE 802.1AR IDevID and LDevID, issued over REST or EST (RFC 7030)
Key protection	Every CA and signing key generated and used inside FIPS-validated HSMs; only signatures and public keys leave
Governance	SSO with Entra ID or Google, group-based policies, quorum approvals, exportable audit trail
Integration	Yocto recipes for NXP, Toradex, PHYTEC and Variscite BSPs, the LAAVAT signing tool (pip), REST and EST APIs
Cryptography	ECC, RSA, post-quantum ML-DSA and hybrid schemes
Deployment	EU-hosted SaaS by default; on-premises deployment available on request. Key export designed in
Compliance	ISO/IEC 27001 certified. Mapped to CRA, RED, NIS2 and IEC 62443-4-1/4-2

TRUSTED BY

KONE VAISALA TREON KEMPPI

"The LAAVAT solution for centrally managing cryptographic keys used for digital signing and encryption plays an important role in ensuring trust in KONE's software supply chain."

Jussi Valkiainen, Head of Product and Application Security, KONE

"Overall, with LAAVAT we have made a huge improvement in our product security."

Ari Alanko, Director R&D, Vaisala

Before you decide, ask each vendor for their MCUboot or HAB integration guide. Ours is public: docs.laavat.io/solutions

Meet us at Embedded World 2027, Nuremberg, 16-18 March, stand 5-381

Free evaluation: sign your first image on day one with the LAAVAT signing tool. No infrastructure to install.

www.laavat.io
docs.laavat.io