LAAVAT

TECHNICAL OVERVIEW FOR EMBEDDED DEVICE MANUFACTURERS

The PKI and signing platform for CRA-ready devices

EU-hosted · Crypto-agile · Post-quantum ready

LAAVAT runs your PKI, signs your firmware for devices based on the silicon you choose, and gives every device a trusted identity. Keys are generated and used inside FIPS-validated HSMs; only signatures and public keys come back to your build. Engineering teams sign from their own pipeline on day one.

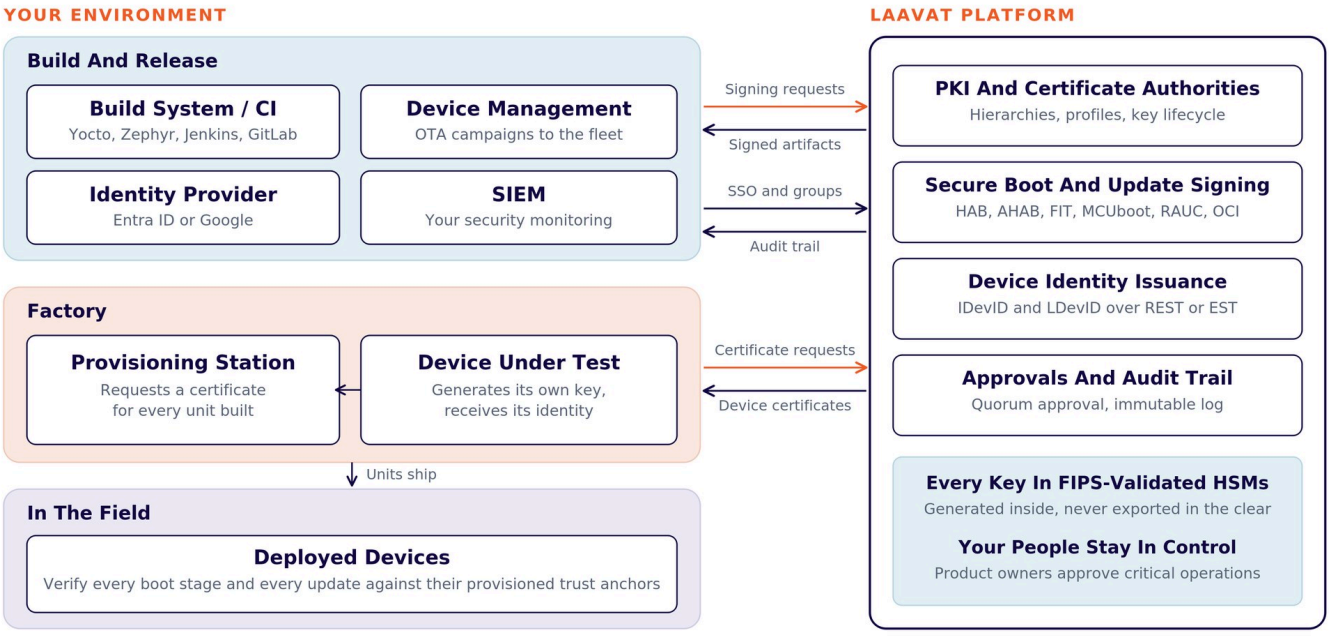
FROM CRA REQUIREMENT TO ENGINEERING CONTROL

Requirement (CRA Annex I)	Device mechanism	What LAAVAT provides
Integrity of software, protection against unauthorised modification	Secure boot from a hardware root of trust; each boot stage verifies the next	Silicon-specific secure boot signing (HAB, AHAB, Bootgen, MCUboot, UEFI), keys never leave the HSM
Security updates distributed securely	Signed, optionally encrypted update bundles, verified on the device	RAUC, Mender, SWUpdate, FIT and MCUboot signing; AES-GCM-256 image encryption
Protection against unauthorised access	Unique per-device certificates for mutual TLS and attestation	IEEE 802.1AR IDevID and LDevID over REST or EST, under your own or a LAAVAT root
Evidence for conformity assessment	Documented key handling and release process	Quorum approvals and an immutable, exportable audit trail of every key and signing operation

Full mapping, written for engineers: docs.laavat.io/cra-compliance. Also mapped to RED (EN 18031), NIS2 and IEC 62443-4-1/4-2.

REFERENCE ARCHITECTURE

One platform across build, factory and field



Integrate over REST or EST, with ready-made clients for CI pipelines and provisioning stations.

Build

Your pipeline requests a signature and gets the signed image back. The private key never leaves the HSM.

Factory

The provisioning station requests a certificate for every unit built, authenticated per station.

Field

Every boot stage and update is checked against the trust anchors you provisioned.

WHAT THE PLATFORM DOES

PKI, signing and encryption across your whole portfolio

PKI

Full hierarchies with internal or external roots; chain under your existing root CA. ECC, RSA and ML-DSA CA chains. 802.1AR IDevID and LDevID, TLS and code-signing certificates. EST enrolment (RFC 7030), CRL lifecycle. Matter device attestation.

Signing

NXP HAB and AHAB, AMD/Xilinx Bootgen, Texas Instruments, Raspberry Pi, ESP32 and UEFI secure boot. MCUboot on STM32, Nordic, Renesas and Microchip. Updates: FIT, RAUC, Mender, SWUpdate. Also OP-TEE TA, OCI with Cosign, Windows binaries, kernel modules and IMA. ML-DSA-65 and ML-DSA-87, hybrid with ECDSA.

Encryption

AES-GCM-256 image encryption. Secure delivery of wrapped encryption keys to build and manufacturing. Key escrow and secure key export.

SECURITY, OPERATIONS AND DEPLOYMENT

HSM-protected keys

Generated and used in FIPS-validated AWS CloudHSM in an EU region, or in your own HSM. Dev and prod keys separated.

Access and audit

SSO with Entra ID or Google, group-based signing policies, quorum approvals. Immutable, exportable, SIEM-ready audit log.

Integration

Web UI, REST and EST APIs, LAAVAT signing tool (pip), in-build Yocto signing for NXP, Toradex, PHYTEC and Variscite BSPs. CI signs as a service principal.

Deployment

SaaS by default in an EU region; your own HSM in your own cloud account; on-premises available on request. Key export designed in: no lock-in.

IN PRACTICE

Secure boot, signed updates and device identity on an NXP i.MX8M Linux gateway

YOU BRING		LAAVAT PLATFORM		SIGNED AND VERIFIABLE
Secure boot artifacts SPL, U-Boot, FIT, OP-TEE TA	→	**Secure boot signing** HAB with SRK table and fuse hash	→	**Signed boot chain** SRK hash for fusing, FIT and OP-TEE TA public keys
RAUC update bundle rootfs, appfs, manifest	→	**RAUC bundle signing** optional bundle encryption	→	**Signed RAUC bundle** Device verifies against the CA keyring
Device onboarding REST or EST, at the factory or in the field	→	**Device identity issuance** IDevID and LDevID	→	**Device certificate** Chained to your CA

Every operation: HSM-protected keys, role-based access, approval rules, full audit trail

Example designs for each hardware platform and update format: docs.laavat.io/solutions. Interactive walkthroughs: www.laavat.io/in-practice.

TRUSTED BY

KONE VAISALA TREON KEMPPI

ISO 27001

"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

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. Then a proof of concept on one real use case.

www.laavat.io
docs.laavat.io