Securing Our Embedded ARM64 Platform for CRA & NIS2 Compliance

- Objectives:

Regulatory context,
Technical roadmap,
APT/package signing best practices

Regulatory Drivers

- CRA – Secure-by-design, OTA integrity, vulnerability handling
- NIS2 – Governance, reporting, supply chain security
- Non-compliance = penalties

CRA Compliance Timeline

- In force: Dec 2024
- Vulnerability handling: Sep 2026
- Full compliance for new products: Dec 2027

Why This Matters

- Wireless interfaces = high attack surface
- Bootloader/kernel compromise = full device compromise
- CRA covers connected embedded devices

NIS2 Overview

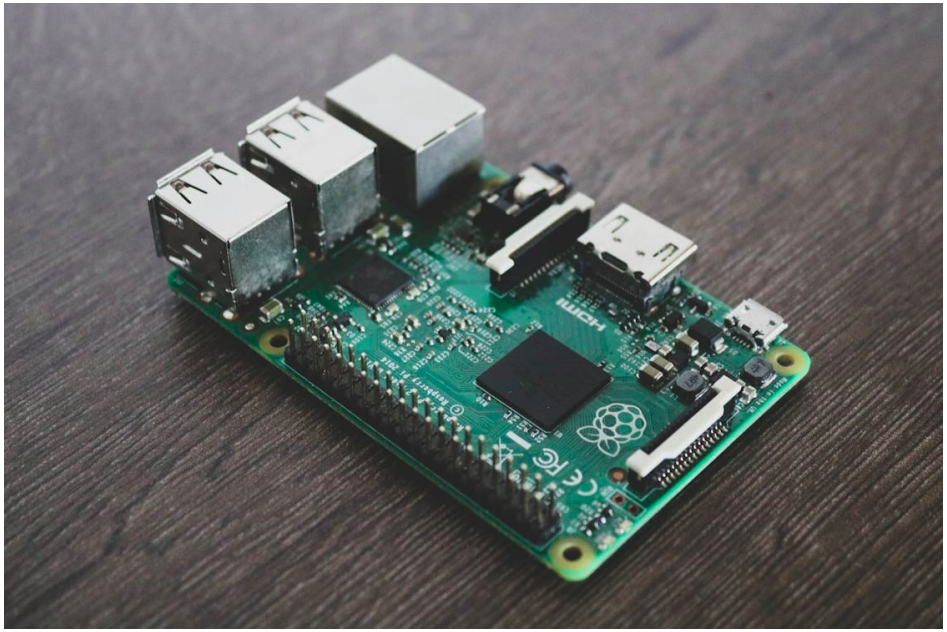
- Critical infrastructure & suppliers included
- Leadership accountability, supply chain controls

CRA Technical Requirements

- Secure boot
- Signed firmware & OTA
- SBOM tracking
- Logging & vulnerability management

Securing the Boot Chain

- ROM → FSBL → U-Boot → Kernel
- Each stage verified before execution
- Hardware root of trust (TPM/TrustZone)



Hardening the Kernel

- Enable lockdown mode
- Disable unused drivers
- Use SELinux/AppArmor

Wireless Attack Vectors

- Bluetooth/Wi-Fi coexistence issues
- Driver vulnerabilities
- Mitigation: disable unused protocols

OTA Update Security

- Firmware signing
- Signature verification in bootloader
- Secure transport (HTTPS, TLS)

APT Package Security

- CRA requires secure update lifecycle
- Repo/key compromise = malicious updates
- Covers kernel, drivers, userland

APT Repo Signing

- apt uses GPG-signed metadata
- Clients verify signatures before install
- Proper key management is critical

Securing GPG Keys

- Generate keys offline
- Store private key in HSM
- Use subkeys for signing

Repository Server Security

- Keys off the repo server
- Sign in CI/CD with isolated key
- Restrict admin access, use MFA

Certificate Management

- Use TLS certificates for repo HTTPS
- Trusted CA or internal PKI
- OCSP stapling for revocation

Key Rotation & Revocation

- Rotate signing keys periodically
- Publish revocation certificates
- Update client trusted keyrings

Client-Side Hardening

- Lock apt to trusted keys/repos
- Disable unauthenticated installs
- Enforce HTTPS + signature verification

SBOM for External Packages

- Track all APT packages & versions
- Check against CVEs
- Automate alerts for vulnerable packages

Compliance Benefits

- Protects customer trust
- Avoids CRA/NIS2 fines
- Strengthens supply chain security

Summary & Call to Action

- Secure boot, kernel, OTA, and repo signing are mandatory
- Immediate next steps: gap analysis, secure key storage, SBOM
- Request: Approve budget/team before Sep 2026