linaro
Connect
2025

Improving supply chain visibility and regulatory compliance for Arm firmware and hardware

Yogesh Deshpande
Julian Hall (both from Arm)

Cybersecurity Regulatory Landscape

- The European Union Cyber Resilience Act (EU CRA) is a legislative initiative aimed at improving cybersecurity standards across digital products within the EU market.
- Required to comply by end of 2027
- Aimed at addressing the fragmented cybersecurity landscape throughout the lifecycle of the digital product
- To protect the consumers and businesses
- Requires maintaining following obligations for open-source deliverables
  1. Ensure technical documentation enlisting details of the product and its design
  2. Ensure Secure integration of OSS components
  3. Supports Vulnerability Management
  4. Demands supply chain transparency
  5. Cost implications to business if non-compliant

Typical Firmware Supply Model Today

- A platform integrator builds and manages a custom firmware integration.
- Often based on firmware maintained by the SoC provider.
- Firmware component versions may not be up-to-date.
- Lack of visibility of firmware composition and provenance.
- Unknown vulnerability status – both FW and HW.
- No clear commitments to support periods, release schedule or response to CVE by upstream open-source projects.

Platform integrator faces challenge of meeting regulatory obligations with little help from upstream suppliers

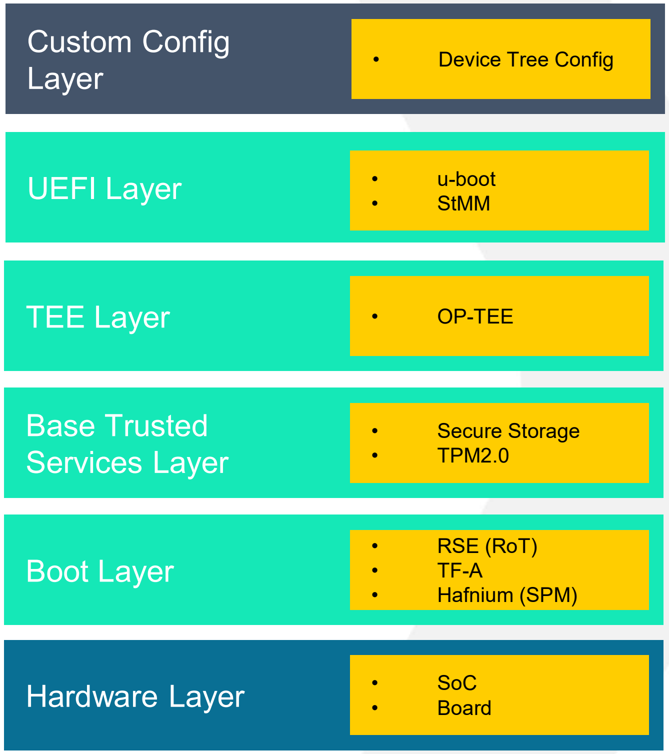
Changes Needed in Supply Chain

- Need more reliance on upstream suppliers to meet CRA obligations
- More use of standard pre-built images, signed and with provenance metadata
- More transparency on release schedules and support periods
- Supply SBOMs & HBOMs
- Introduce secure software processes throughout the supply chain
- Auditability
- Introduce vulnerability management
- Generally simplifying the SW supply chain will reduce cost of compliance

Firmware Composition

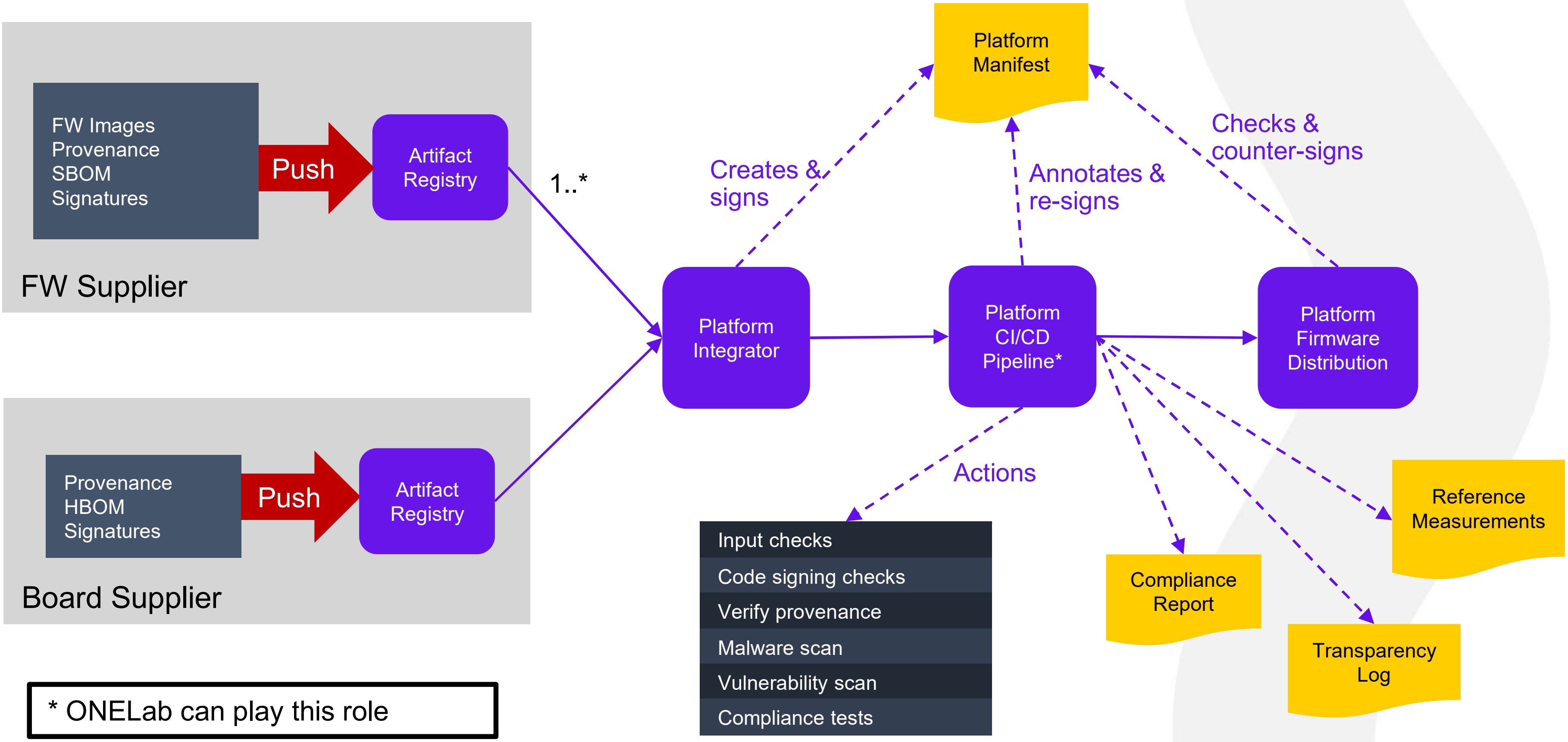
- FW and HW forms the security foundations for Arm based devices.
- Arm firmware composed using multiple independently built images.
- Combination of executable images and configuration data forms basis of platform integration*.
- Firmware components may be grouped by layer to reflect supplier responsibilities.

*Currently no formal definition of a platform integration.



Custom Config Layer	• Device Tree Config
UEFI Layer	• u-boot • StMM
TEE Layer	• OP-TEE
Base Trusted Services Layer	• Secure Storage • TPM2.0
Boot Layer	• RSE (RoT) • TF-A • Hafnium (SPM)
Hardware Layer	• SoC • Board

Evolved FW and HW Supply Chain



FW Supplier

FW Images
Provenance
SBOM
Signatures

Push

Artifact Registry

Board Supplier

Provenance
HBOM
Signatures

Push

Artifact Registry

1..*

Platform Integrator

Creates & signs

Platform Manifest

Platform CI/CD Pipeline*

Annotates & re-signs

Platform Firmware Distribution

Checks & counter-signs

Actions

- Input checks
- Code signing checks
- Verify provenance
- Malware scan
- Vulnerability scan
- Compliance tests

Compliance Report

Transparency Log

Reference Measurements

* ONELab can play this role

New Requirements

Compliance Automation

Signing Infrastructure, Key Management & Tooling

Availability of SBOM/HBOM

Assurance Metadata

Transparency for Conformance Audit

Vulnerability Management

Artifact Distribution

Firmware Composition Definition

Standards Overview

- OpenSSF best security practices
  1. Standards for SBOM Formats SPDX and CycloneDX
  2. SLSA Framework based assurance levels - CRA’s risk-based conformity assessments
  3. SigStore supports digital signing of code & artifacts and provides transparency of supply chain
  4. Vulnerability management

- Consider adoption of standard practices for firmware production and distribution
  1. Model firmware delivery standards on the lines of OCI Artifact specification
  2. Model firmware distribution standards along the lines of OCI distribution specification
  3. Introduce any other standards along the supply chain lines

Collaboration with Linaro ONELab

- ONELab is a trusted ecosystem resource for verifying Arm firmware compatibility across different OS and middleware.
- It automates testing on real hardware.
- Operated independently by Linaro, ONELab provides impartial and trustworthy insights.
- Continuous compliance model fits well with requirement to automate demonstration of CRA compliance.
- Arm is collaborating with Linaro to extend ONELab capabilities to help product manufacturers meet CRA obligations for FW and HW.

Goals

- Provide a blueprint for automating CRA compliance for Arm FW and HW.
- Avoid adoption barriers by reusing existing tooling and practices.
- Promote supply chain interoperability through use of appropriate standards.
- Promote reuse of pre-built images with defined provenance and assurances.
- Extend ONELab to provide a flagship deployment for showcasing continuous compliance measures that can be integrated into production firmware CI/CD pipelines.

Interested in Contributing?

- Please contact:
- Julian Hall (julian.hall@arm.com) – Arm
- Yogesh Deshpande (Yogesh.Deshpande@arm.com) - Arm

linaro Connect 2025

Thank You!

BACK UP SLIDES

Driving Change in the FW and HW Supply Chain

- For OEMs building products on Arm today, changes are needed to meet CRA obligations
- Scope of changes:
  - Improve support lifetime transparency
  - Provide evidence that firmware is actively managed
  - Support security attestation for free and open-source software
  - Improve response to discovered vulnerabilities
  - Share responsibility for vulnerability management
  - Minimize risk related to public release of pre-release firmware
  - Provide due diligence tracking for major functionality changes
  - Offer comprehensive SBOM/HBOM auditing
  - Automate CRA conformity assessment evidence generation

YD0

Managing Supply Chain Complexity

- Define a standard approach of platform integration
- Define a process for producing a reference platform using Arm components
- Produce reference platforms that can be used directly by Platform Integrators (ODMs)
- Introduce re-usability!
- Simplifies the Supply Chain greatly!
- Introduce secure software processes throughout the supply chain
- Encourage Arm Eco-system adoptability

Slide 15

YD0 Check, if it is OK to discuss in public domain, what has been agreed in the EESOP meeting ?

Yogesh Deshpande, 2025-04-23T17:11:41.748

Investigating Potential Solutions

Reuse of OCI container technologies
- Firmware composition definition
- Artifact distribution using OCI image registries (SBOM/HBOM, platform manifest, signatures, pre-built images)
- Provenance annotations generated by CI/CD pipelines
- Tool and infrastructure reuse

Vulnerability management
- SBOM/HBOM requirements
- CVE management
- Use of standards
- Timely response to vulnerabilities

Provenance metadata guidance
- Attributes and assurances
- Standards reuse
- Extensibility

Firmware release process
- Roles and responsibilities
- Signing
- Traceability

Pre-built image reuse
- Reduce need for custom images
- Stronger supplier assurances

Attestation
- Reference measurements
- Supporting policy

Supporting compliance audit
- Transparency log
- Compliance log

Firmware release process
- Roles and responsibilities
- Signing
- Traceability