Arm High Performance IoT Platforms Security Enhancements : fTPM TS Support

Devaraj Ranganna
Gokhan Gokce

Who we are?

Devaraj Ranganna

Staff Software Engineer @ Arm

- 20 years of experience
- Embedded expert with domain knowledge on IoT, Automotive and Process Automation
- Leading and mentoring
- Contributing the joint product roadmaps with Linaro

Gokhan Gokce

Software Technology Manager @ Arm

- 15 years of experience (10 years of product management)
- IoT & Mobile expertise and entrepreneurship background
- Leading 2 software products' roadmaps in Arm
- Contributing the joint product roadmaps with Linaro

Agenda

- Arm & Linaro Collaboration
- Security Solutions from Arm for IoT
- What is fTPM?
- fTPM Trusted Services Integration
- Why fTPM SP?
- fTPM SP Architecture
- Validation
- Further Investigation
- Integration Plan to Upcoming Platforms
- Availability on Cassini & One Lab

Arm & Linaro Collaboration

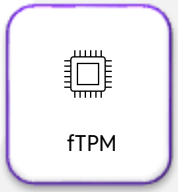
- Arm donated project Cassini to Linaro
- Cassini is a component under Linaro's One Lab
- Arm's IoT-Edge team has member engineers work under Linaro umbrella
- Joint effort to enable ecosystem, new Arm-based platforms and security features

Security Solutions from Arm for IoT

- Arm provides various security solutions for IoT platforms.
- Our member engineers added fTPM (TA) support to a partner platform.
- fTPM **T**rusted **S**ervices support is in our roadmap

Our security solutions:

Security Certification Program



Firmware TPM 2.0

What is fTPM?

- Firmware-based implementation of TPM 2.0
- Runs inside Arm TrustZone
- Separate physical chip is not required
- Ideal for IoT and cost-sensitive devices

fTPM Trusted Services Integration

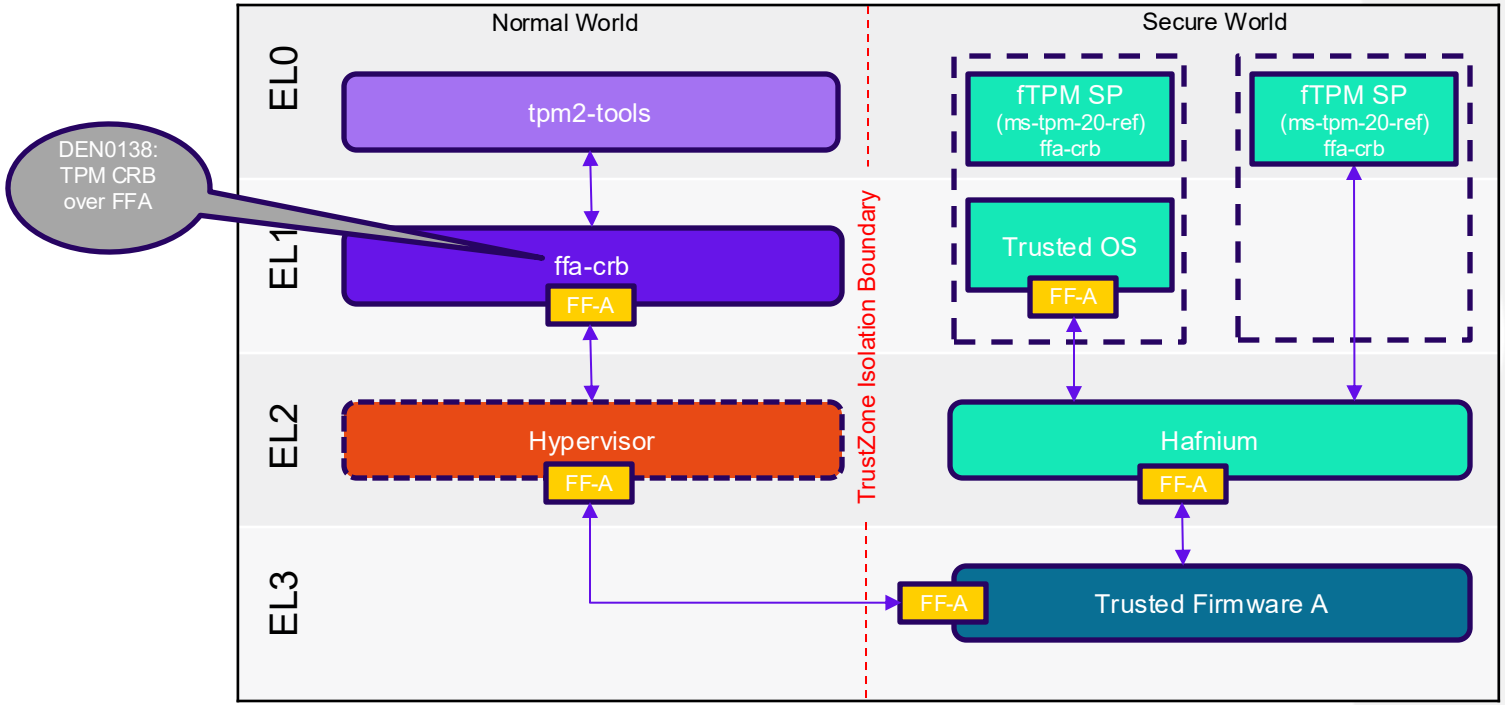
- fTPM SP is firmware TPM 2.0 implementation on top of Trusted Services framework
- 100% API compatibility support with fTPM (TA) and TPM 2.0 implementations
- fTPM SP will be widely used on Arm reference software stacks
- uboot & EDK2 based software stacks will be available on Cassini software stack under One Lab

fTPM SP Integration to Arm High Performance IoT Platfroms

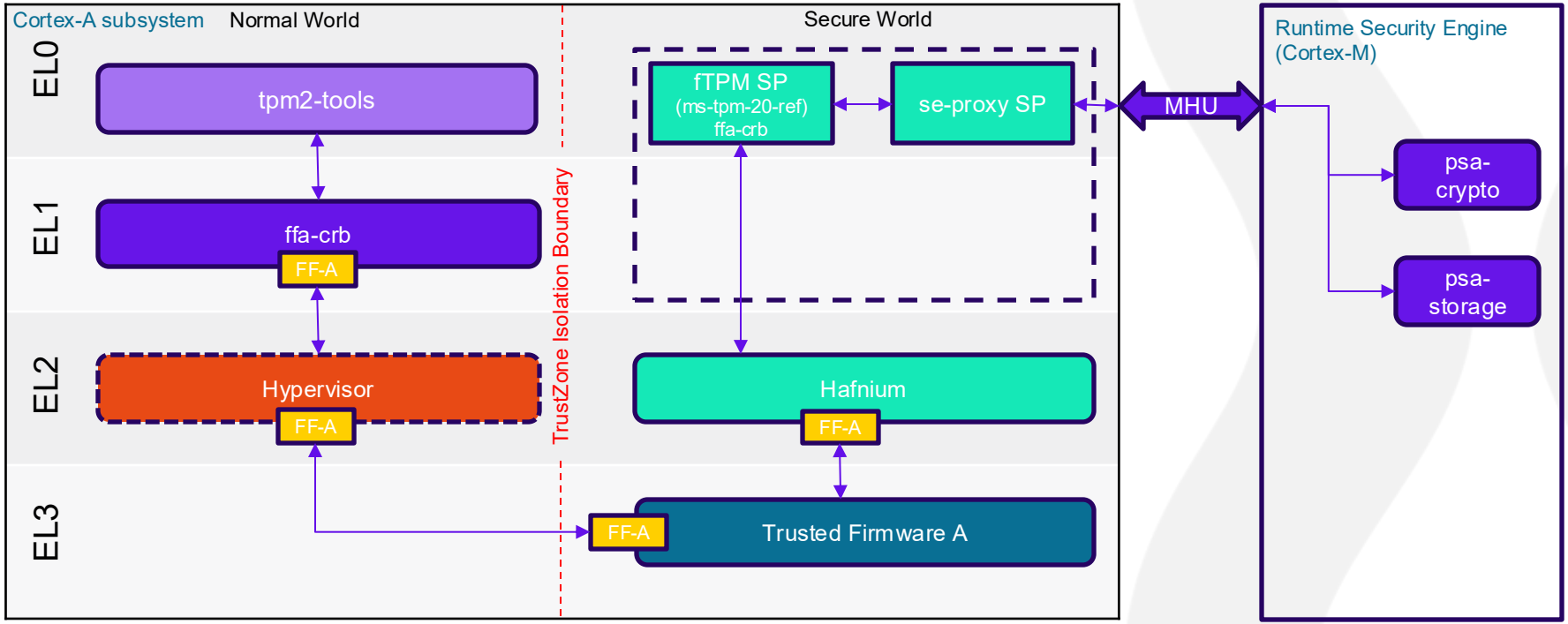
Why fTPM SP?

- Built using the Trusted Services framework, fTPM SP can:
  - Run as EL0 secure service directly on Hafnium at EL2
  - Run as EL0 secure service on top of a Trusted OS at EL1
- Can support psa-crypto backend (currently being investigated)
- Can delegate crypto and storage operations to Runtime Security Engine
- More choices to implement fTPM on Arm platforms

fTPM SP Architecture



fTPM SP Architecture



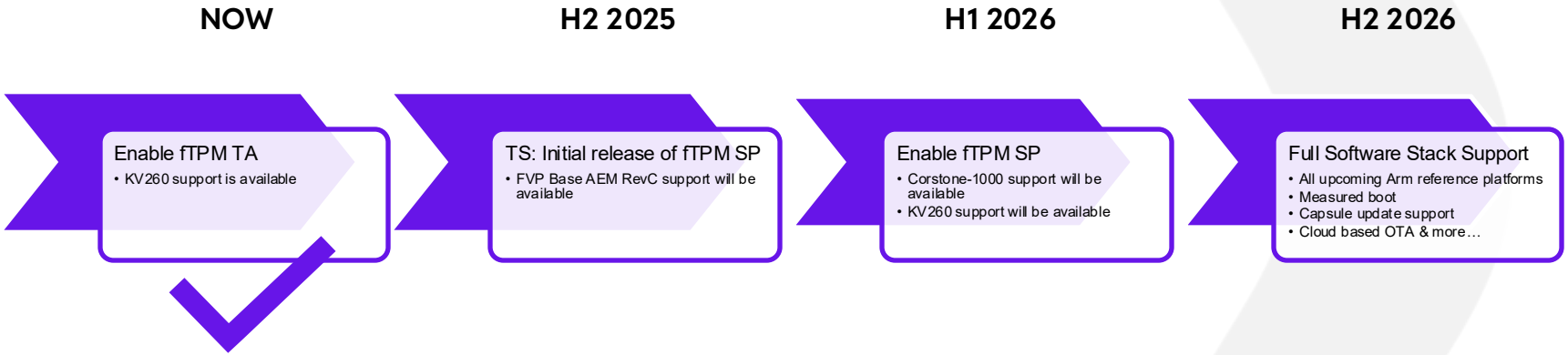
Validation

- tpm2-tools integration tests
- tpm2-PKCS11 and Greengrass IDT tests
  - Key-pair generated for Greengrass device identification
- tpm2-openssl tests

Further Investigation

- Measured Boot
- fTPM provisioning

Integration Plan to Upcoming Platforms



Availability on Cassini & One Lab

- fTPM TA is already available in Cassini
- fTPM SP will be available in Cassini by H2 2026
- Soon after H2 2026, fTPM SP will be available under One Lab, so that partners can:
  - Run TPM test suites
  - Measured Boot
  - fTPM provisioning

Any Questions?

Devaraj Ranganna
devaraj.ranganna@arm.com

Gokhan Gokce
gokhan.gokce@arm.com

Thank You!