arm

Linaro Connect LVC20-112

Secure Partitions in OP-TEE

Miklós Bálint

2020-09-22

Project Goals

- Out-of-box security for rich IoT and infrastructure edge devices
- Reference Platform Security Implementation for Cortex-A in trustedfirmware.org
- Platform Root of Trust services
- Based on Arm® Firmware Framework for Armv8-A (FF-A)
- Enabling devices to be PSA Certified

Recap

Complete Platform Security Offering

Openly Published, Independently Tested.

Analyze

Threat models & security analyses

Methodically developed

Architect

Hardware & firmware architect specifications

Open architecture

Implement

Firmware source code

Open Source

Certify

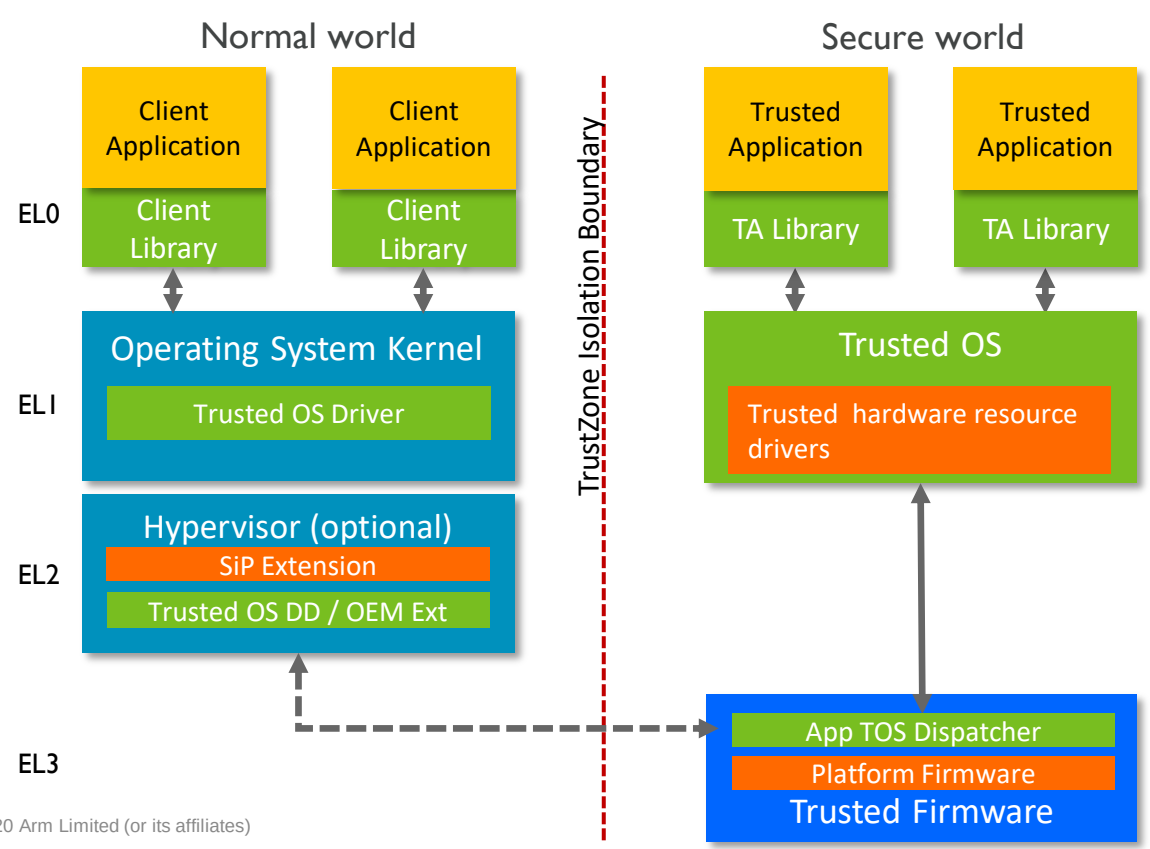
Independently tested

psacertified™

Enabling trust

Secure world software architecture today (TOS)

Recap



Application trusted OS specific
Application provider specific
Generic software
TrustedFirwmare.org
Silicon Vendor specific software

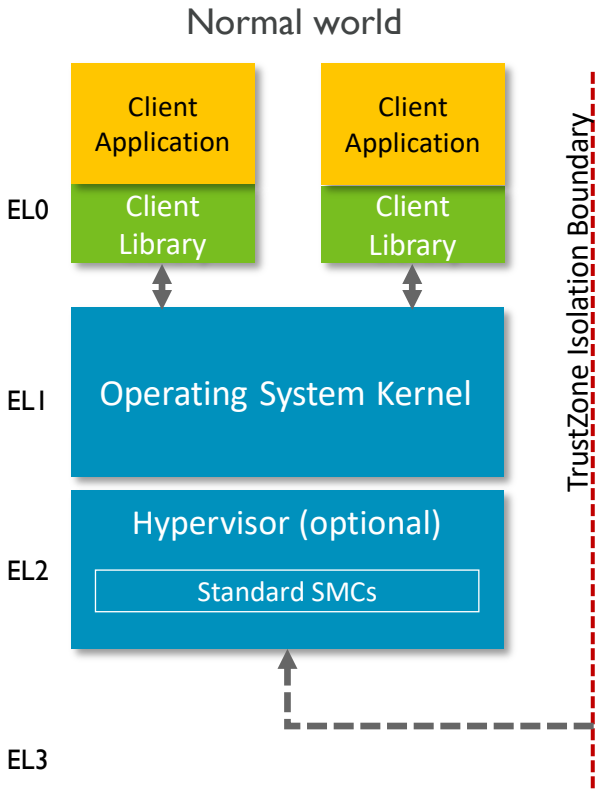
Secure services:

- DRM
- Secure payment
- Secure storage
- Crypto

Platform services:

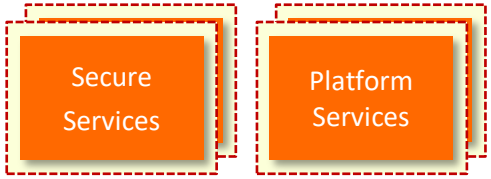
- Trusted boot
- Power management (PSCI)
- Silicon vendor services
- Errata management

Secure world software architecture goal



TrustZone Isolation Boundary

Secure world



	Application trusted OS specific
	Application provider specific
	Generic software
	TrustedFirwmare.org
	Silicon Vendor specific software

Secure services:

- DRM
- Secure payment
- Secure storage
- Crypto

Platform services:

- Silicon vendor services
- Errata management
- BMC communication

Standard/Generic Trusted Firmware

Standard services:

- Trusted boot
- Power (PSCI, SCMI)

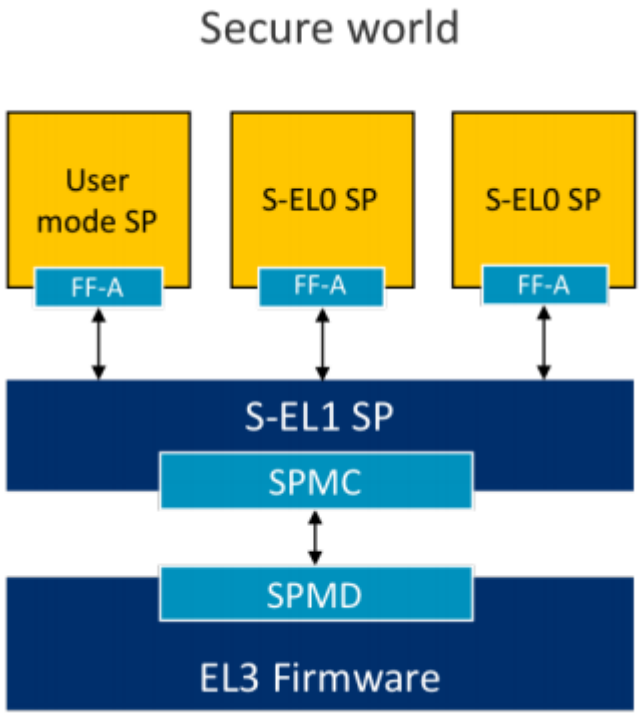
Standard config/transport

- SMCCC/FFA
- DT

Arm® Firmware Framework for Armv8-A (FF-A)

- Describes a software architecture that achieves the following goals:
  - Isolation of software images provided by an ecosystem of vendors from each other
  - Standardization of communication between the various software images
- Introduces
  - Partitions (Virtual Machines and Secure Partitions)
  - Partition manifests
  - Partition Managers (Hypervisor and Secure Partition Manager)
  - Standard interfaces and transport primitives

FF-A SPM without S-EL2

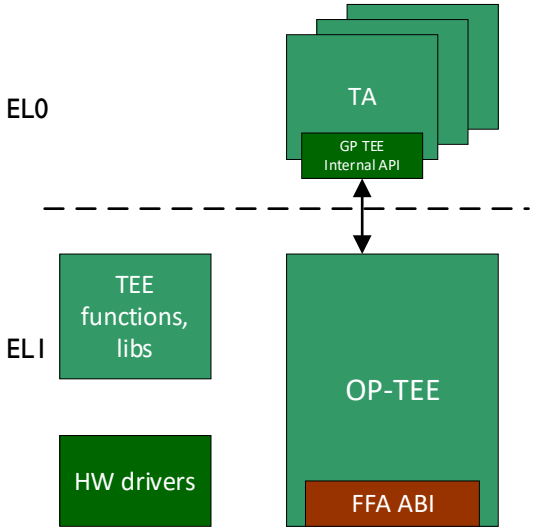


- S-EL0 / User mode SPs
- S-EL1 / Supervisor SPMC
- Standard FF-A transport between components
- Migration path towards Armv8.4-A Secure EL2

Proof of Concept

Baseline

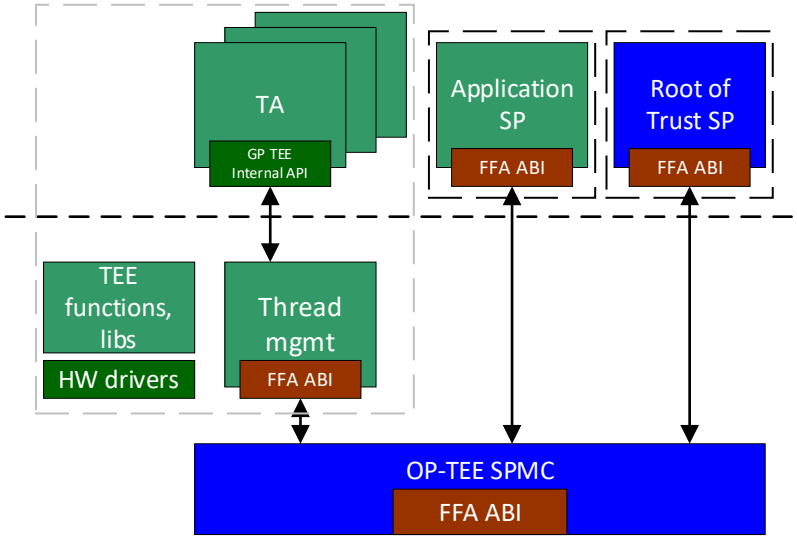
- OP-TEE 3.10.0 release
- `CFG_CORE_SEL1_SPMC=y` config
  - OP-TEE functionality unchanged
  - Physical FFA ABI as SMC transport
  - Single S-EL1 SP
  - (No support for S-EL0 FFA partitions)
- PoC using v8-A Architecture Model as development platform



Proof of Concept

OP-TEE as SPMC

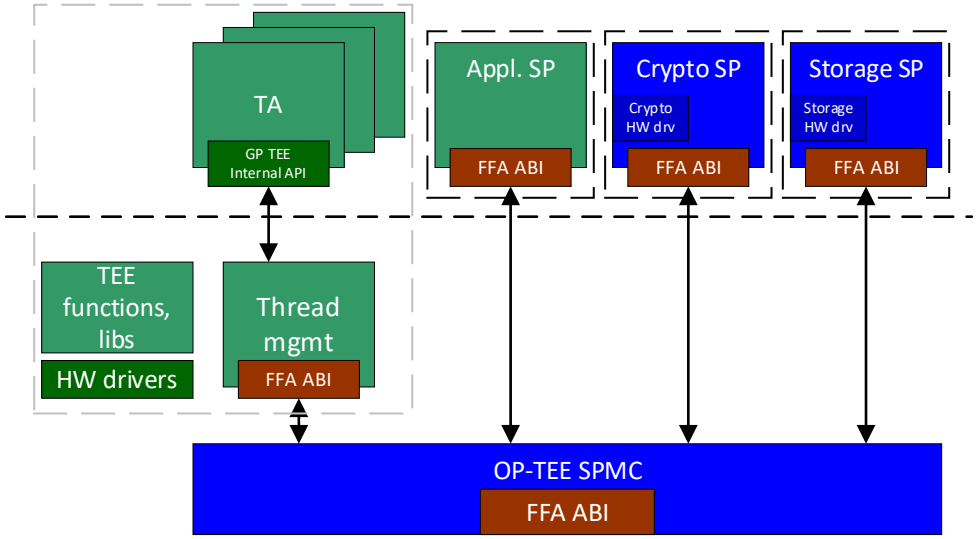
- Minimal SPMC based on FF-A
  - Management of multiple SPs
  - Virtual FFA ABI at SVC
  - Keep impdef interface for S-EL1 SP
- SPs based on early TAs
  - Library to build SPs against: libsp (~ libutee)
  - Deployed as part of OP-TEE binary
  - Started as part of OP-TEE initialisation
- Minimal set of crypto functions in S-EL0 SP



Ongoing work

General improvements

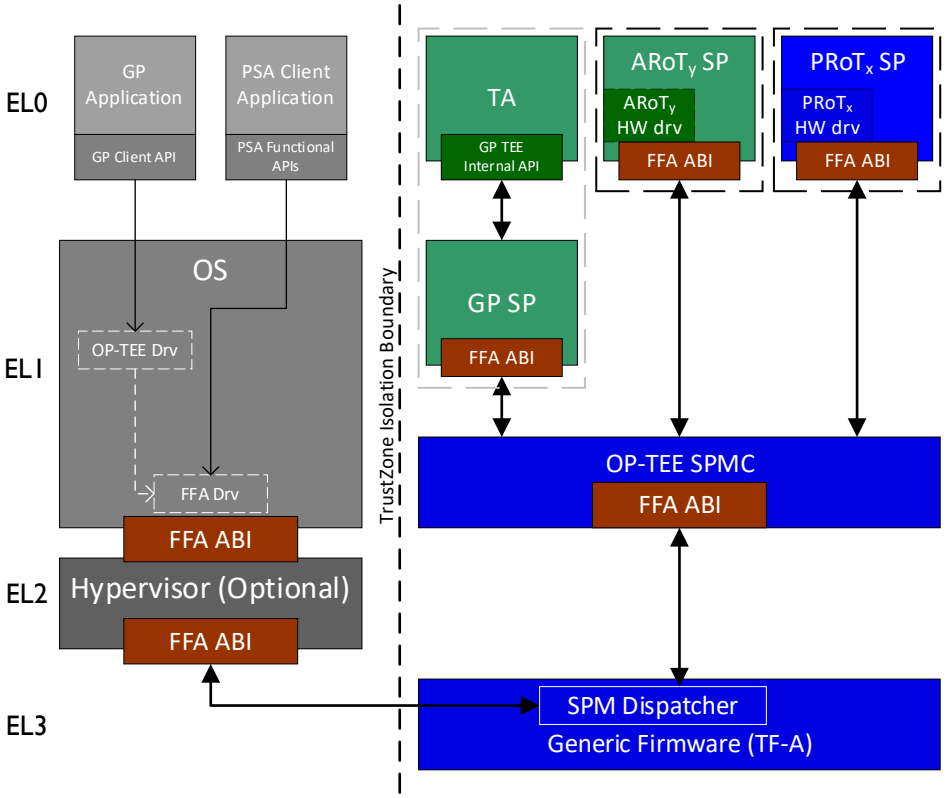
- Internal Trusted Storage Secure Partition
  - Incl. placeholder for HW driver
- Decoupling of partition source and build flow from OP-TEE
- Refactoring, clean-up of SPMC
  - Clean up of TA/SP management code
  - Clearer interface between GP SP and SPMC
- Documentation, test and CI



Next steps, investigations

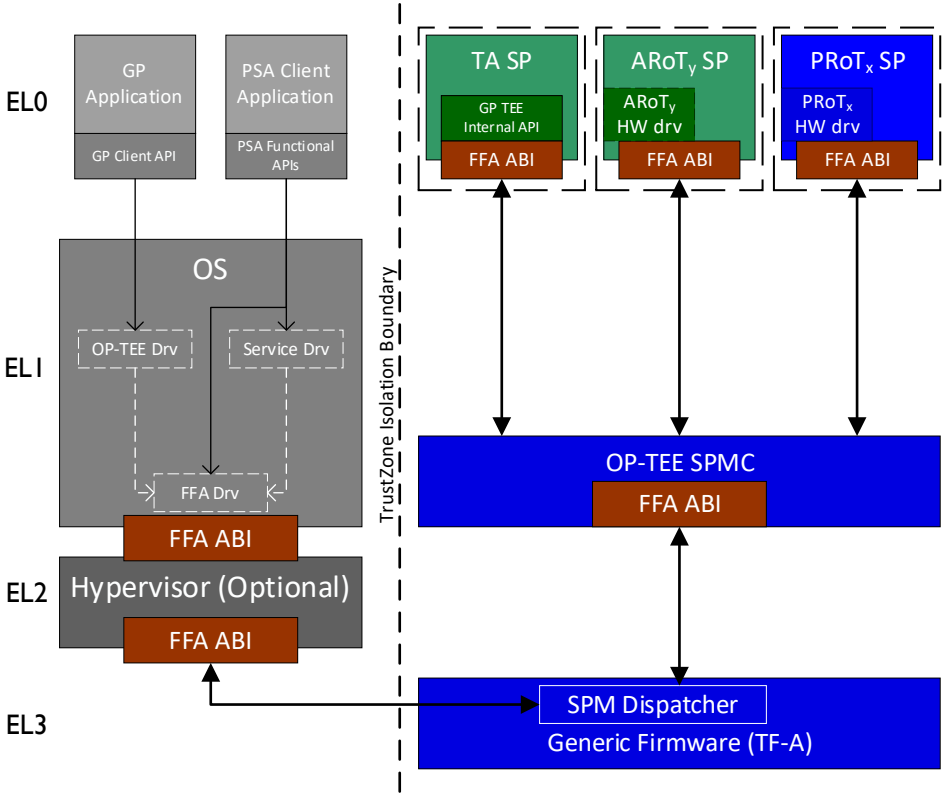
Consolidation

- OP-TEE upstream of SPMC changes
- NWd application using PRoT services
  - Crypto SP to be ready for PSA Certified L1
  - Internal Trusted Storage
- Investigations
  - Attestation service
  - HW management and interrupt handling
  - Map ownership to dedicated Platform SPs



Future directions, opportunities

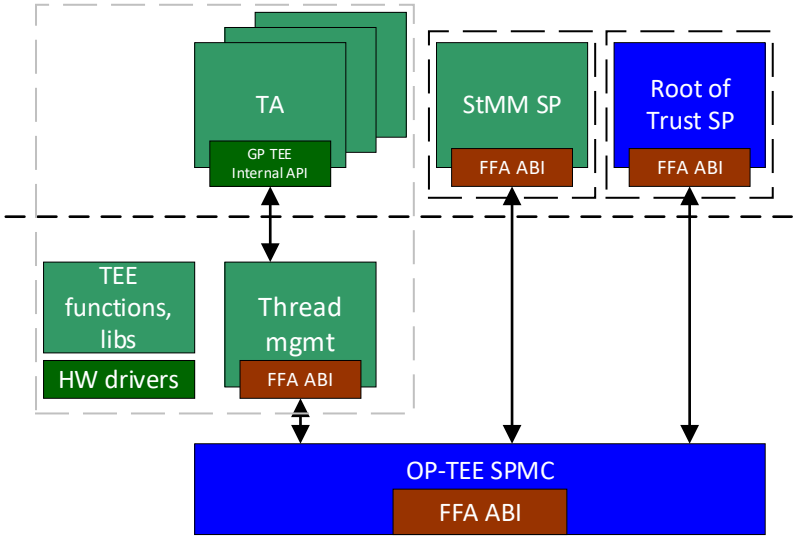
- Packaging, delivery, authentication of SPs
  - Decouple from OP-TEE binary
  - Authentication flow, measurements
- 32-bit support
  - User space SP and service protocols
  - Supervisor mode SPMC
- Reduction of privileged footprint
  - TEE functions mapped to RoT SPs
- Focus on portability of SPs
  - S-EL0 GP adaptation layer for TAs
  - StMM Secure Partition integration
  - S-EL0 SPs services with S-EL1 shim layer for S-EL2 SPMC



StMM Secure Partition

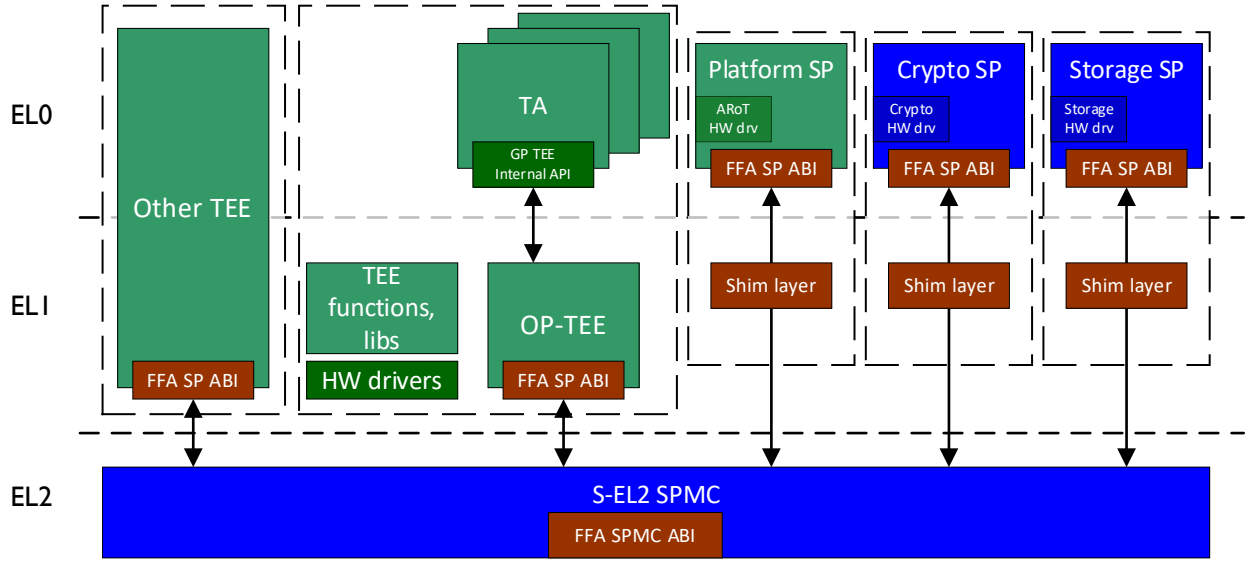
Integration

- Activity started in Linaro EDGE group
- Implements virtual FFA ABI at SVC conduit
- LVC20-302 Enable UEFI Secure Boot using OP-TEE as Secure Partition
- Agnostic to underlying software architecture
- Can use RoT services using FF-A as transport
- HW access using resource mapping or SP dependency



Armv8.4 Secure EL2 Virtualization extension

- Isolation through virtualization in the Secure world
- System-wide isolation
- LVC20-305 Secure Partition Manager (S-EL2 firmware) for Arm A-class devices



Summary

Goals

- Software arch. agnostic S-EL0 Platform Root of Trust SPs
- Platform Security for Rich IoT and Infra Edge in line with Arm Firmware Framework
- Focus on PSA Certified

Get involved

- For the bigger picture: LVC20-113 Trusted Firmware Project update
- Provide feedback: op-tee@lists.trustedfirmware.org
- Active reviews: OP-TEE SPMC reviews
- Questions?

arm

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
תודה