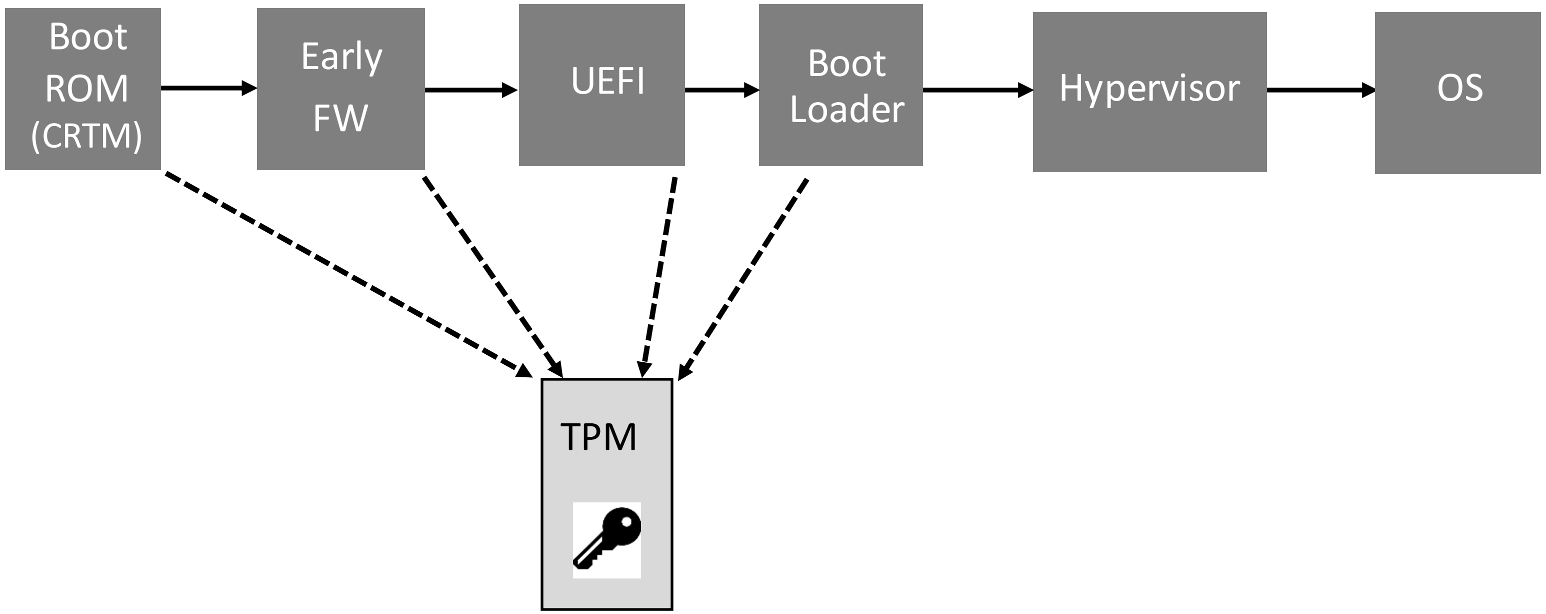
DRTM Overview

10 March 2022

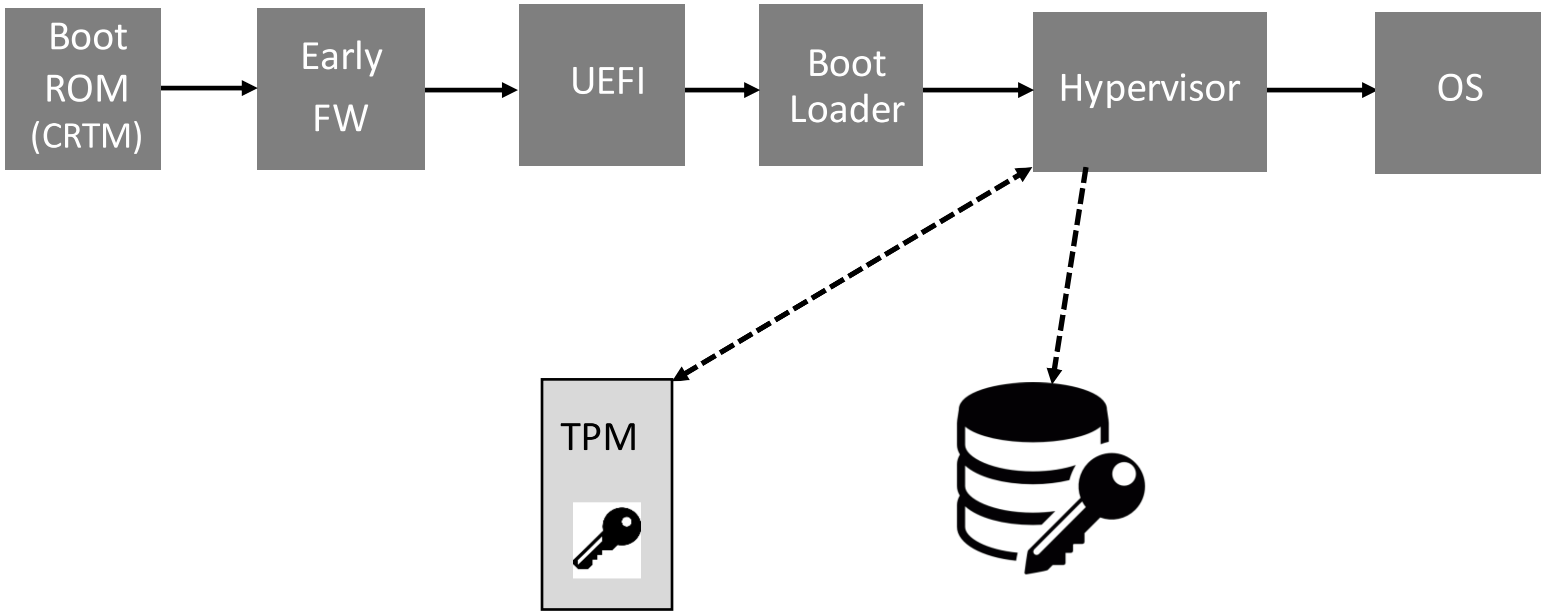
Measured Boot – Static Root of Trust

SRTM Chain of Trust

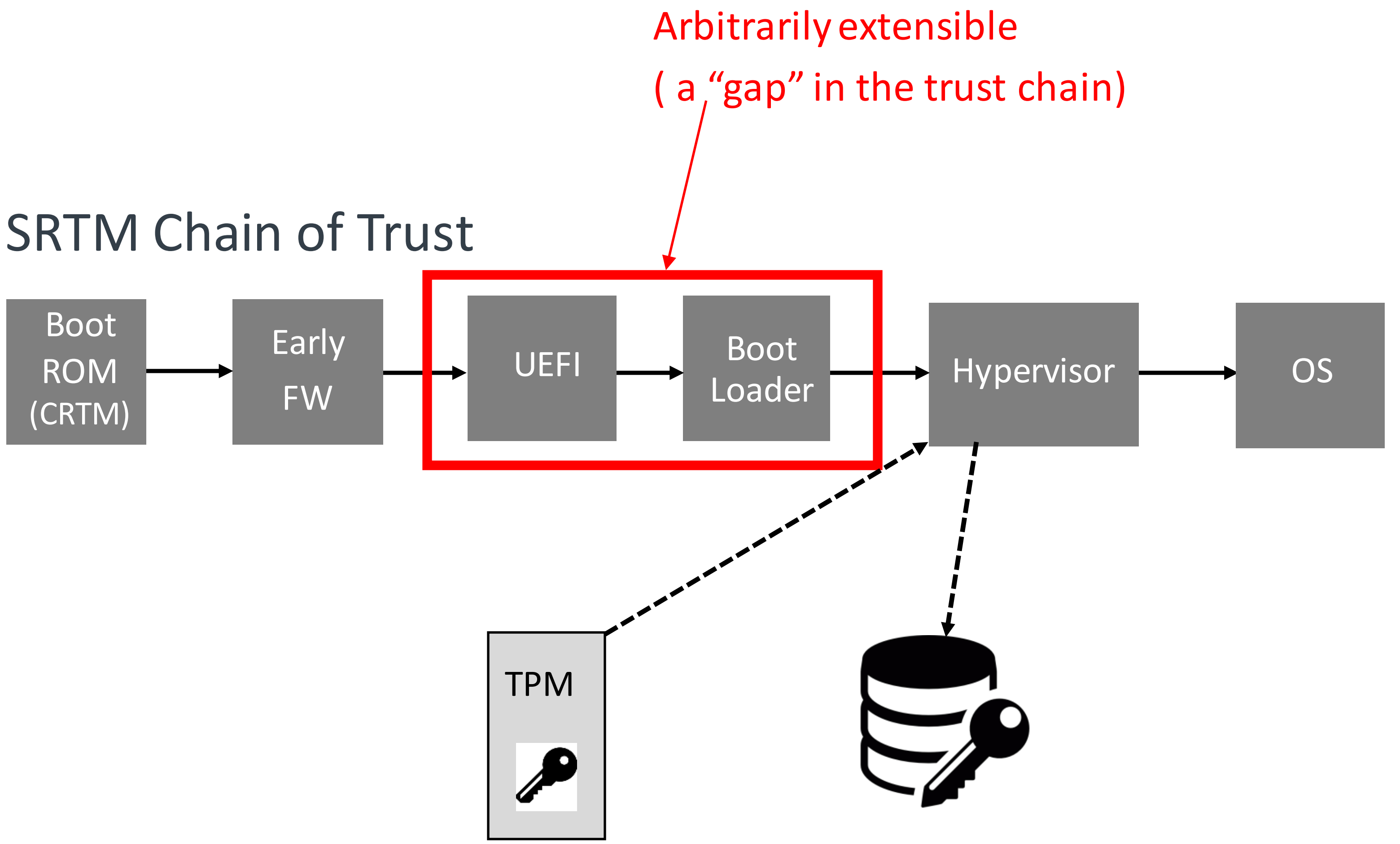


Measured Boot – Static Root of Trust

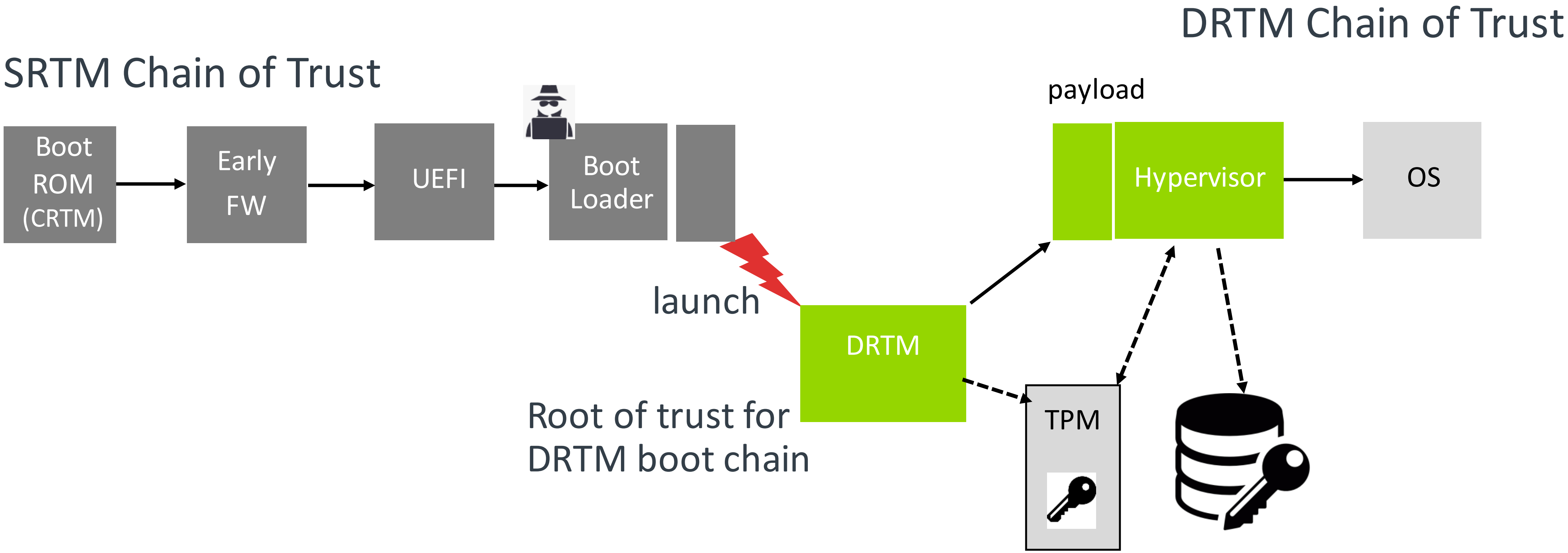
SRTM Chain of Trust



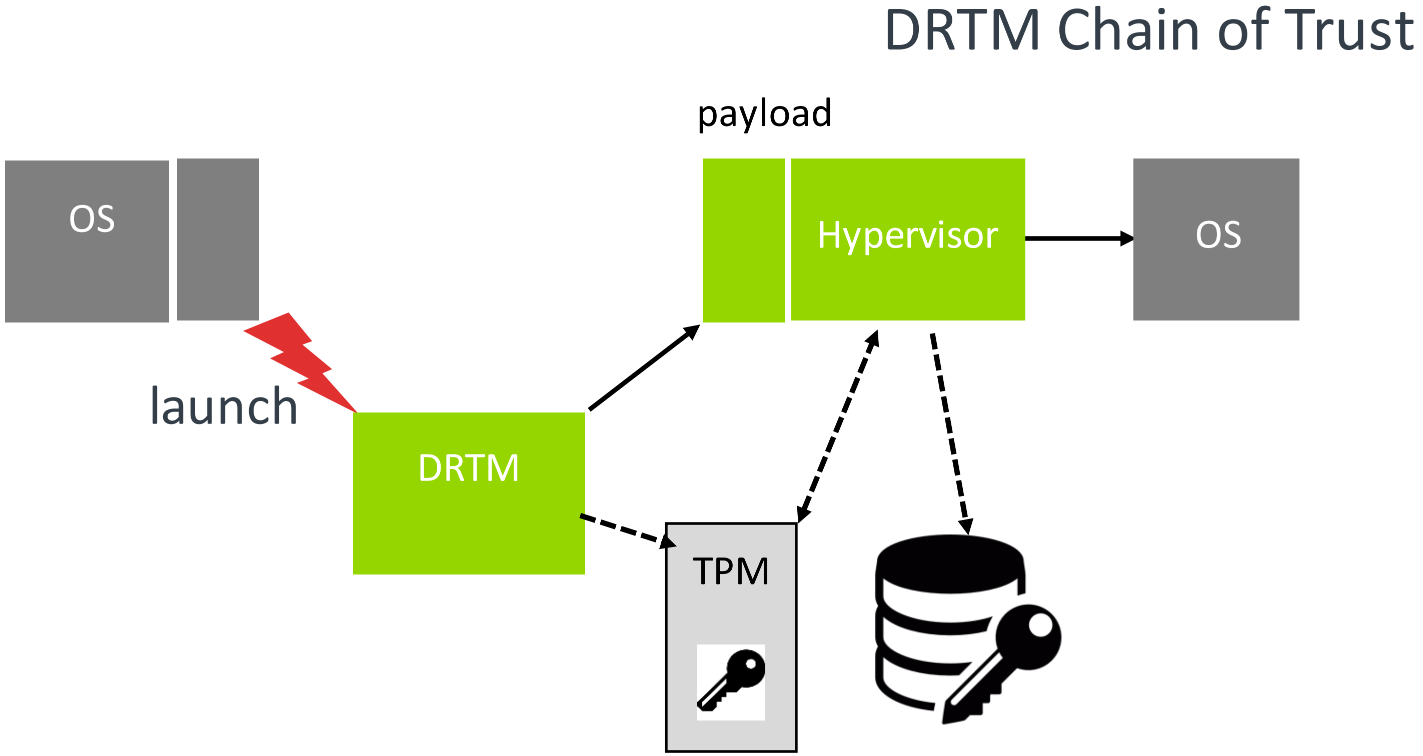
Measured Boot – Static Root of Trust



Dynamic Root of Trust for Measurement



DRTM launch can be done on running system

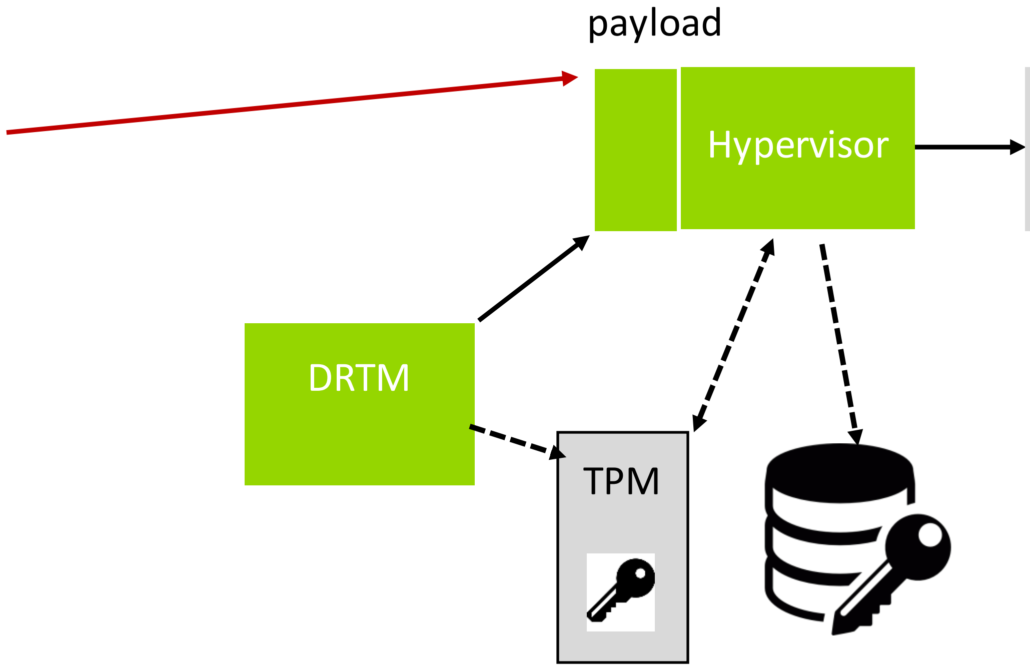


Security Guarantee

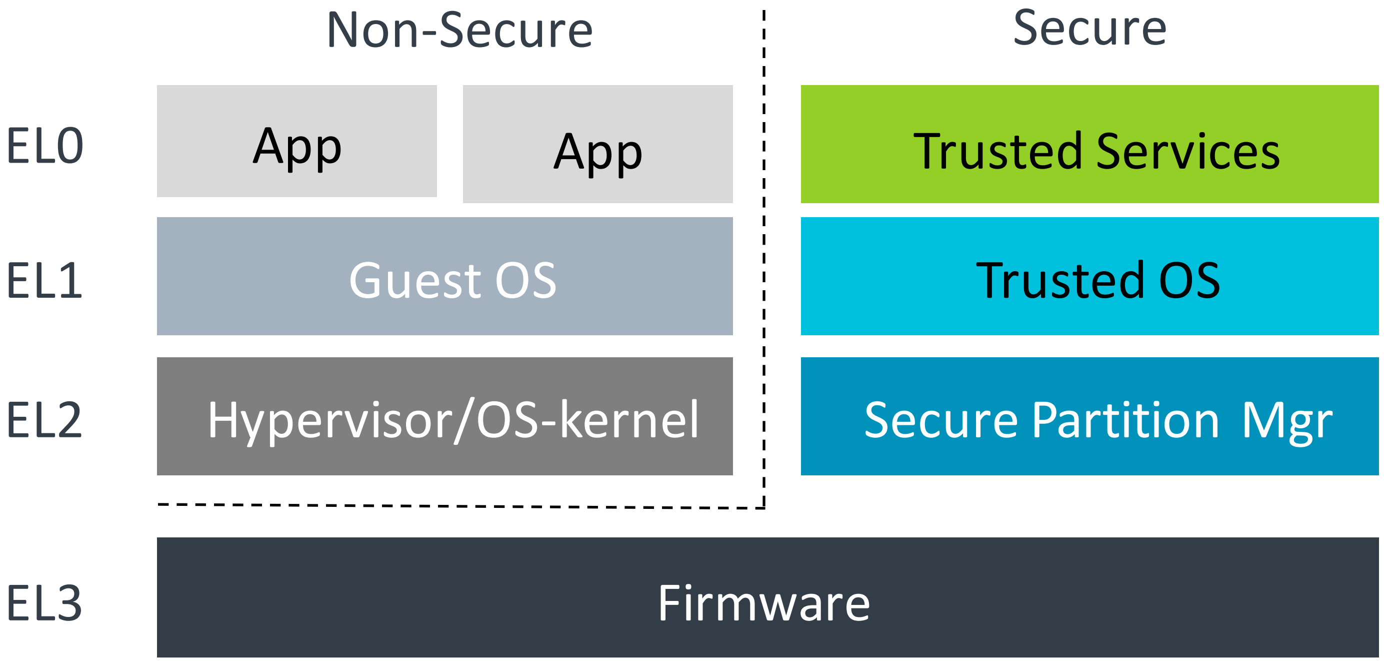
Security guarantee

- Trustworthy measurement of payload and critical system state
- Target image begins in a safe state
  - Single thread of execution
  - Interrupts disabled
  - DMA protections in place
  - Trustworthy memory map and security ACPI tables available

DRTM Chain of Trust



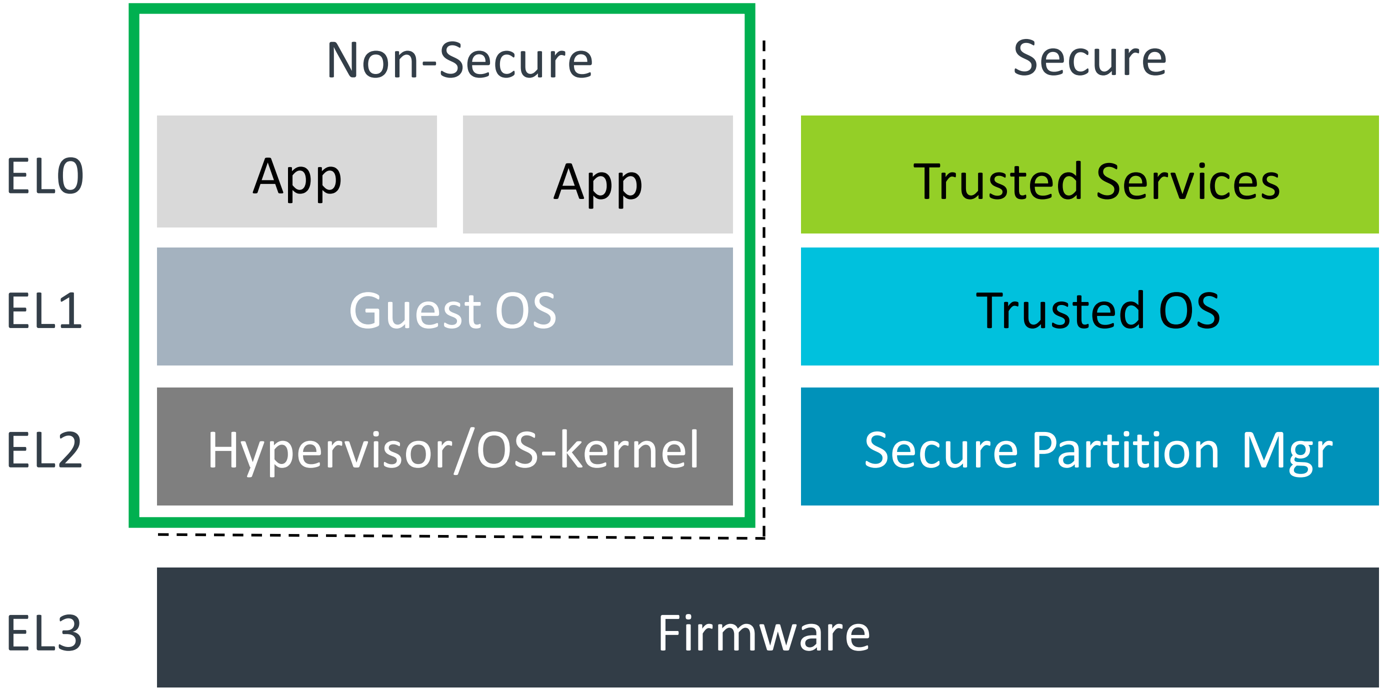
Arm Privilege Levels



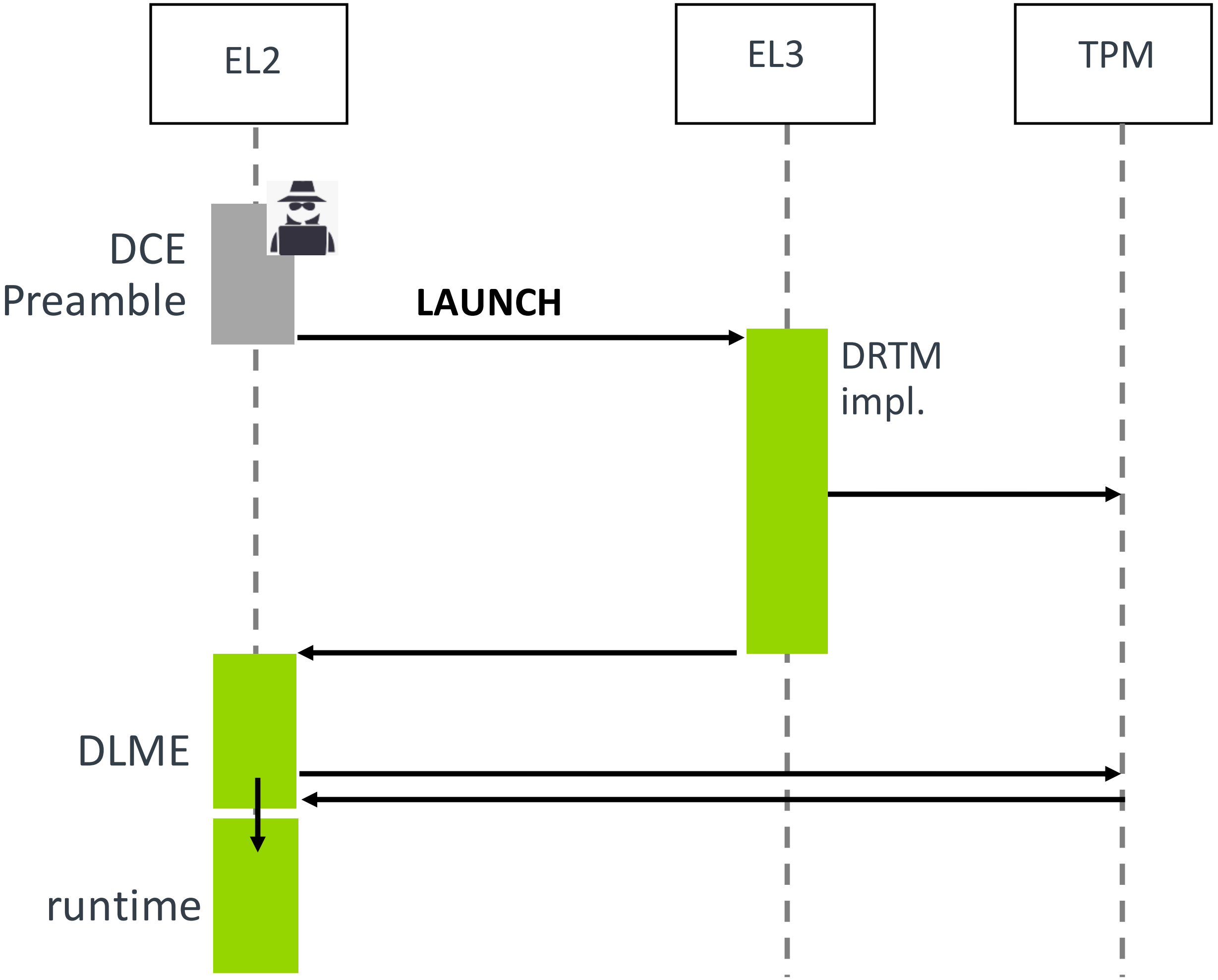
	Non-Secure		Secure
EL0	App	App	Trusted Services
EL1	Guest OS		Trusted OS
EL2	Hypervisor/OS-kernel		Secure Partition Mgr
EL3	Firmware		

Scope of DRTM on Arm

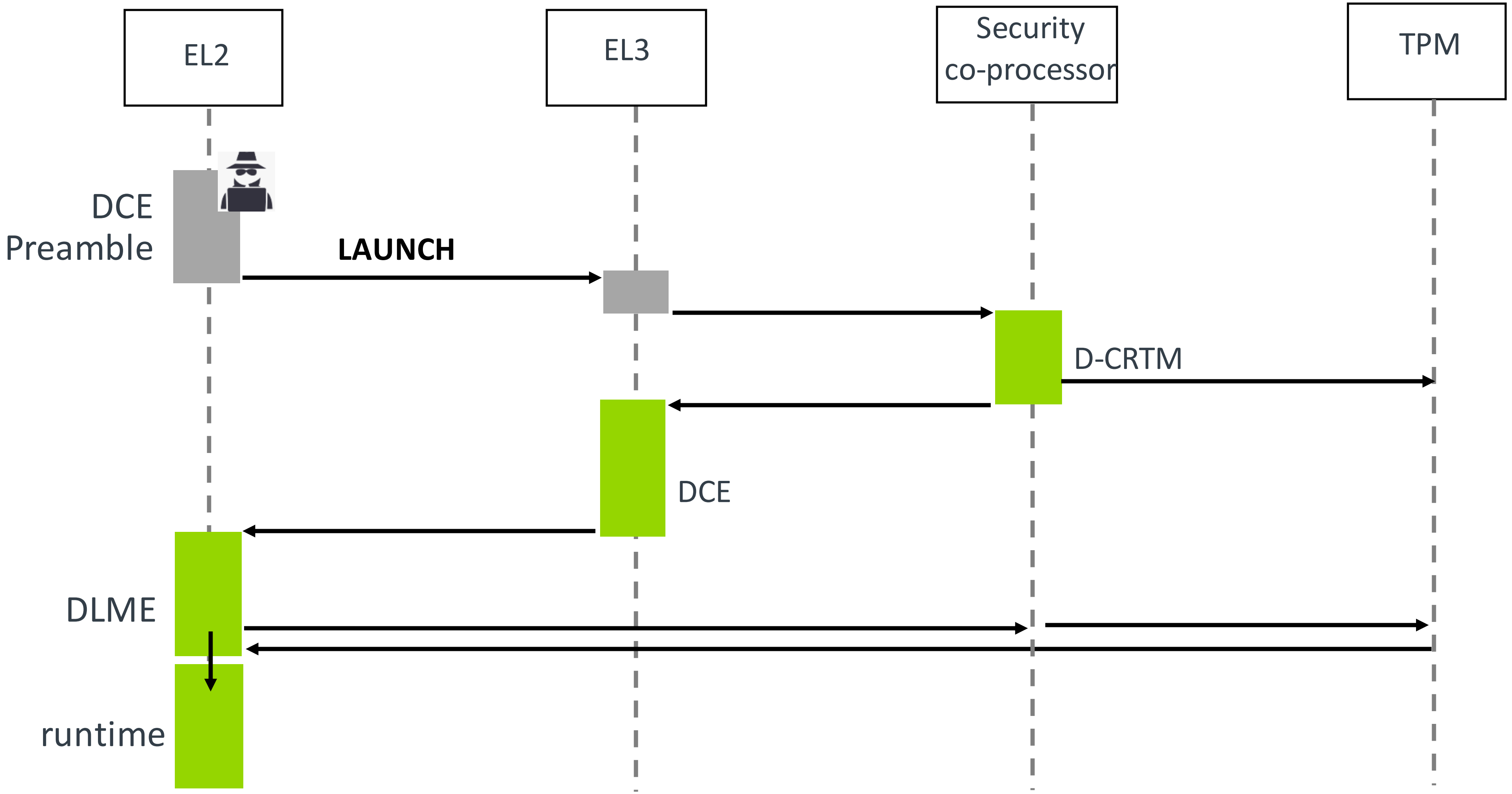
- The scope of the restarted DRTM chain-of-trust is the non-secure side of the machine

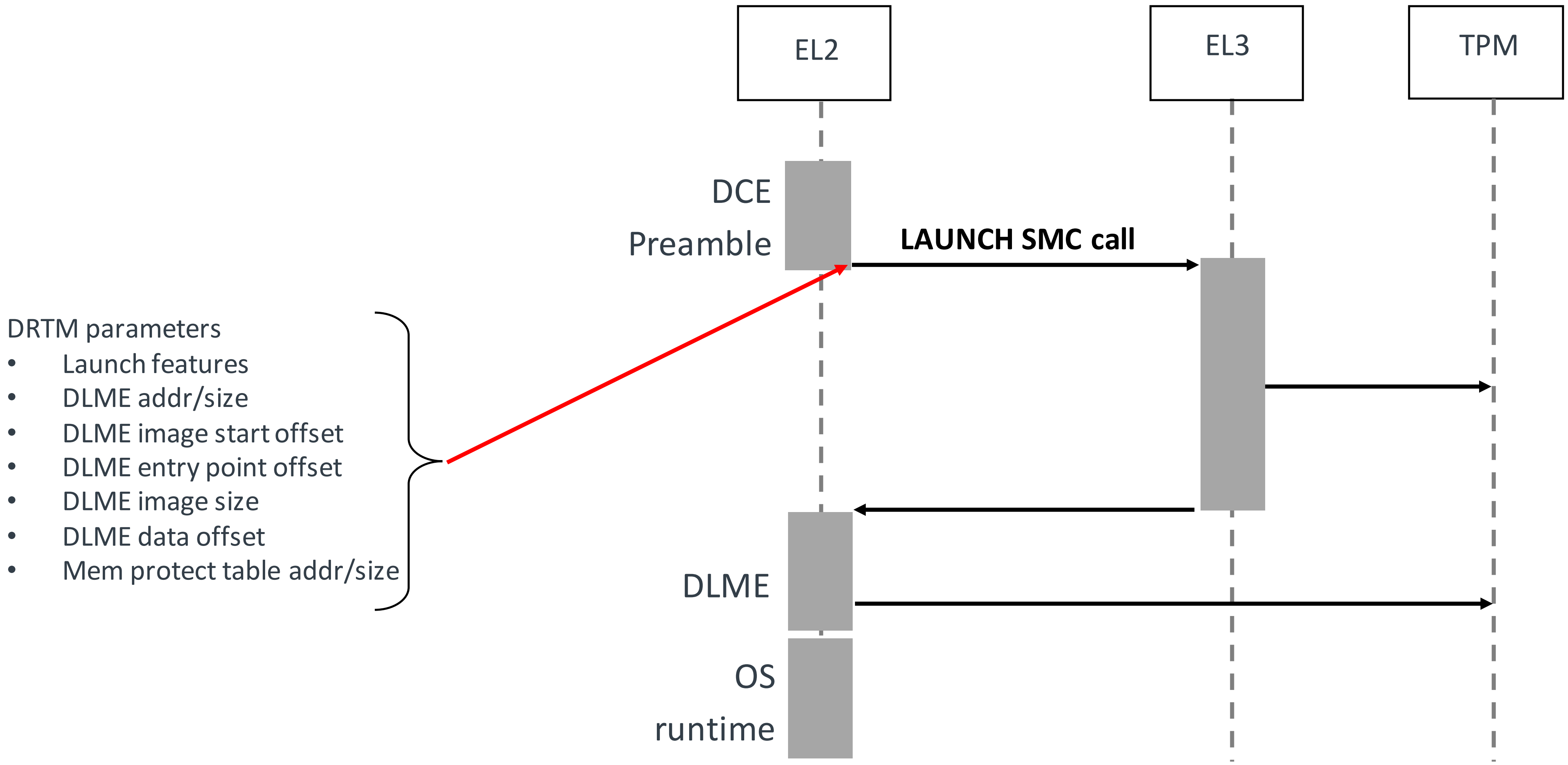


DRTM on Arm – firmware backed



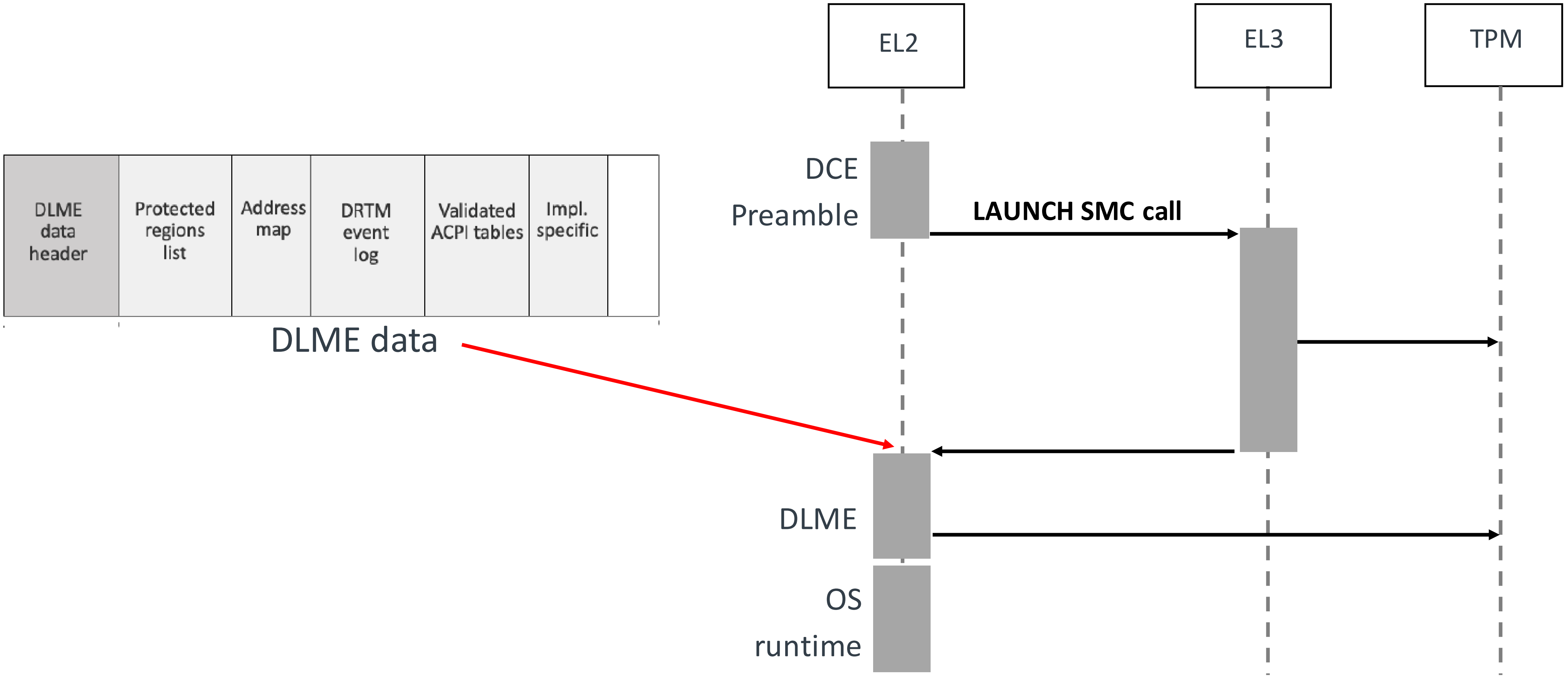
DRTM on Arm – hardware backed





DRTM parameters

- Launch features
- DLME addr/size
- DLME image start offset
- DLME entry point offset
- DLME image size
- DLME data offset
- Mem protect table addr/size



DLME data header	Protected regions list	Address map	DRTM event log	Validated ACPI tables	Impl. specific	

DLME data

DRTM support in TF-A

10 March 2022

TF-A

- DRTM PoC Branch hosted on trustedfirmware.org topics/arm-drtm-poc
- Based on v2.5 release
- Initial upstream support planned around mid of this year
  - Experimental
  - FVP platform
  - QEMU support depends on interests and support from maintainers

Implementation details

- Firmware backed implementation
- D-CRTM and DCE components are both part of EL3, DCE guarded against build macro to decouple it from EL3 in future
- EL3 makes sure pre-condition to launch DLME is met by ensuring
  - Single PE execution
  - NS Interrupts disabled
  - SMMU v3 driver to abort all NS pending transactions and disable SMMU before launching DLME to achieve complete DMA protection
- DRTM standard services(SMC details on next slide)
- DRTM co-exist with trusted boot
- DRTM parameter parsing support

Contd...

- Crypto support for hash calculation of various DRTM components
- Event Log driver support
  - To record the hash measurements of various DRTM components
  - Attach it to DLME data
- Platform hooks for
  - Retrieve the address map and attach it to DLME data
  - Retrieve base address and number of SMMU to engage DMA protection
  - To read/write DRTM errors to Non-volatile memory
- CI configuration with pre-built DRTM application (DCE preamble + DLME)

SMC Support

Function	Description	Support	Limitations
DRTM_VERSION	Version of the DRTM implementation	Yes	
DRTM_FEATURES	To determine the supported DRTM capabilities of the platform	Yes	
DRTM_DYNAMIC_LAUNCH	Initiated DRTM dynamic launch	Partial	1. Measure various image/data components (partial) 2. Engage DMA protection (partial) 3. Prepare DLME data (partial)
DRTM_UNPROTECT_MEMORY	Removes the memory protection put in place by the dynamic launch	Partial	Region based protection is not supported
DRTM_CLOSE_LOCALITY	Close a locality in the physical TPM.	No	No physical TPM supported
DRTM_GET_ERROR	Returns error code from the previous DRTM dynamic launch	Yes	
DRTM_SET_ERROR	Set the Dynamic launch error code	Yes	
DRTM_SET_TCB_HASH	Record the hashes of the TCB components	No	
DRTM_LOCK_TCB_HASH	Lock the TCB component hashes	No	

Limitations in first delivery

- Targeted only for 2 world system
- Assumptions
  - There is no secure payload running which can impact DRTM
  - No request to power on secondary cores
- Complete DMA protection, no region-based protection yet
- Separate event log driver for SRTM(measured boot) and DRTM
- Disabling SDEI events
  - It's responsibility of DCE preamble to make call to disable SDEI events (by using SDEI_PRIVATE_RESET & SDEI_SHARED_RESET)
  - Once it is done, EL3 can check that SDEI events are disabled before launching DLME

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה