Arm CCA

Developer Resources

Matteo Carlini

Publicly Available Arm CCA Resources

arm CCA

https://developer.arm.com/architectures/architecture-security-features/confidential-computing

March 2021 till now

Register XML

AC6 EAC asm/disasm support for RME (6.16)

GNU Binutils support for RME

Released TODAY!

Reference manual supplements

- RME Architecture (ARM DDI 0615A.a)
- SMMU for RME (ARM IHI 0094A.a)
- MPAM (ARM DDI 0598C.a)

RME System Architecture (DEN0129) platform design doc

Guides

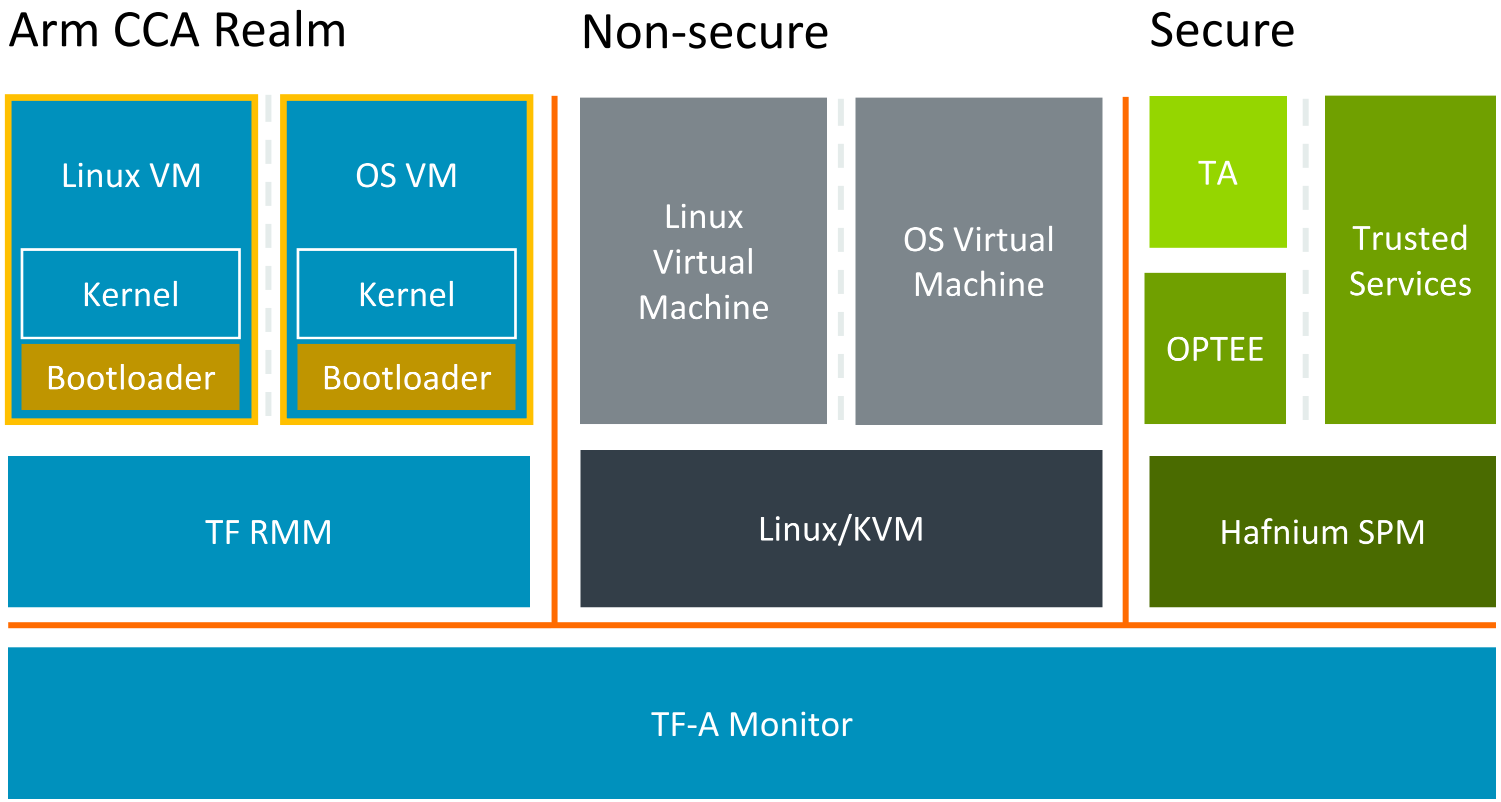
- Overview of the Arm CCA (DEN0125)
- Arm Realm Management Extension (DEN0126)
- Arm Confidential Compute Software Stack (DEN0127)

Coming Soon

AEM Base FVP with RME support will be publicly available in July (feature aligned with the released RME supplement spec)

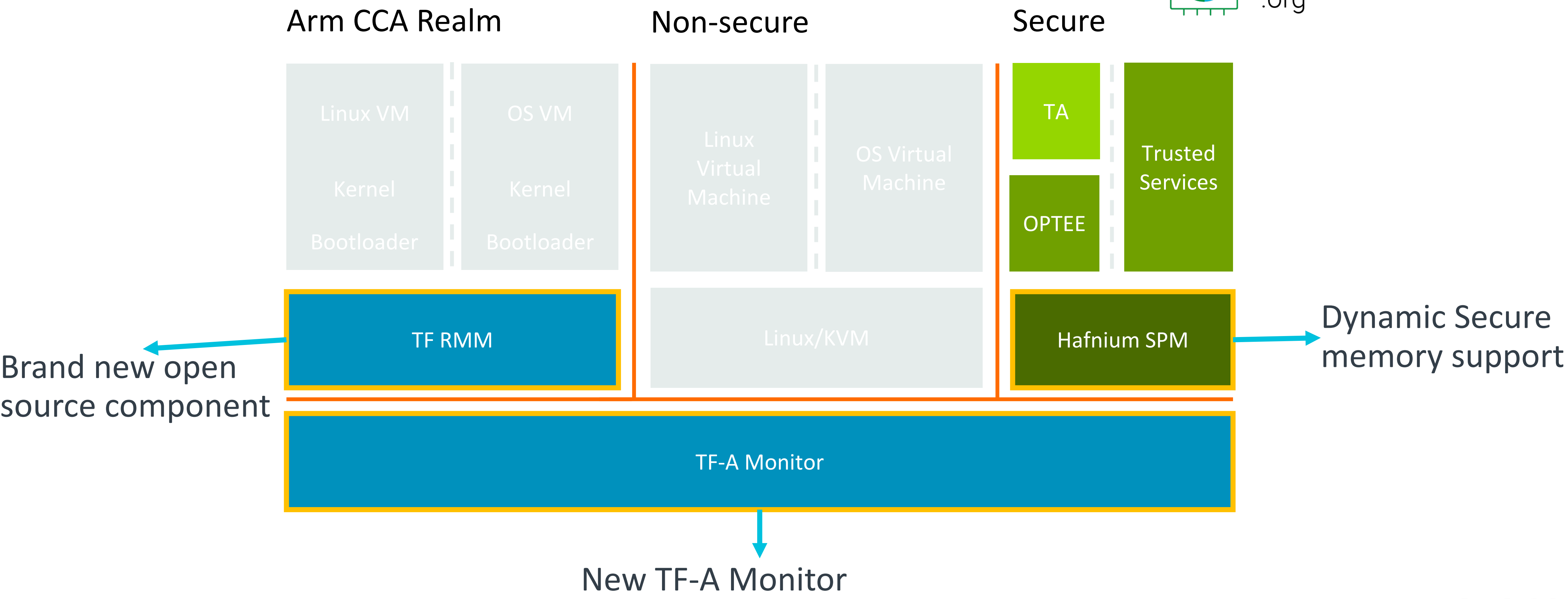
LLVM asm/disasm expected to be upstreamed by mid-July (aligned to above AEM FVP) arm CCA

Open Source Software enablement



Open Source Software enablement

TrustedFirmware.org



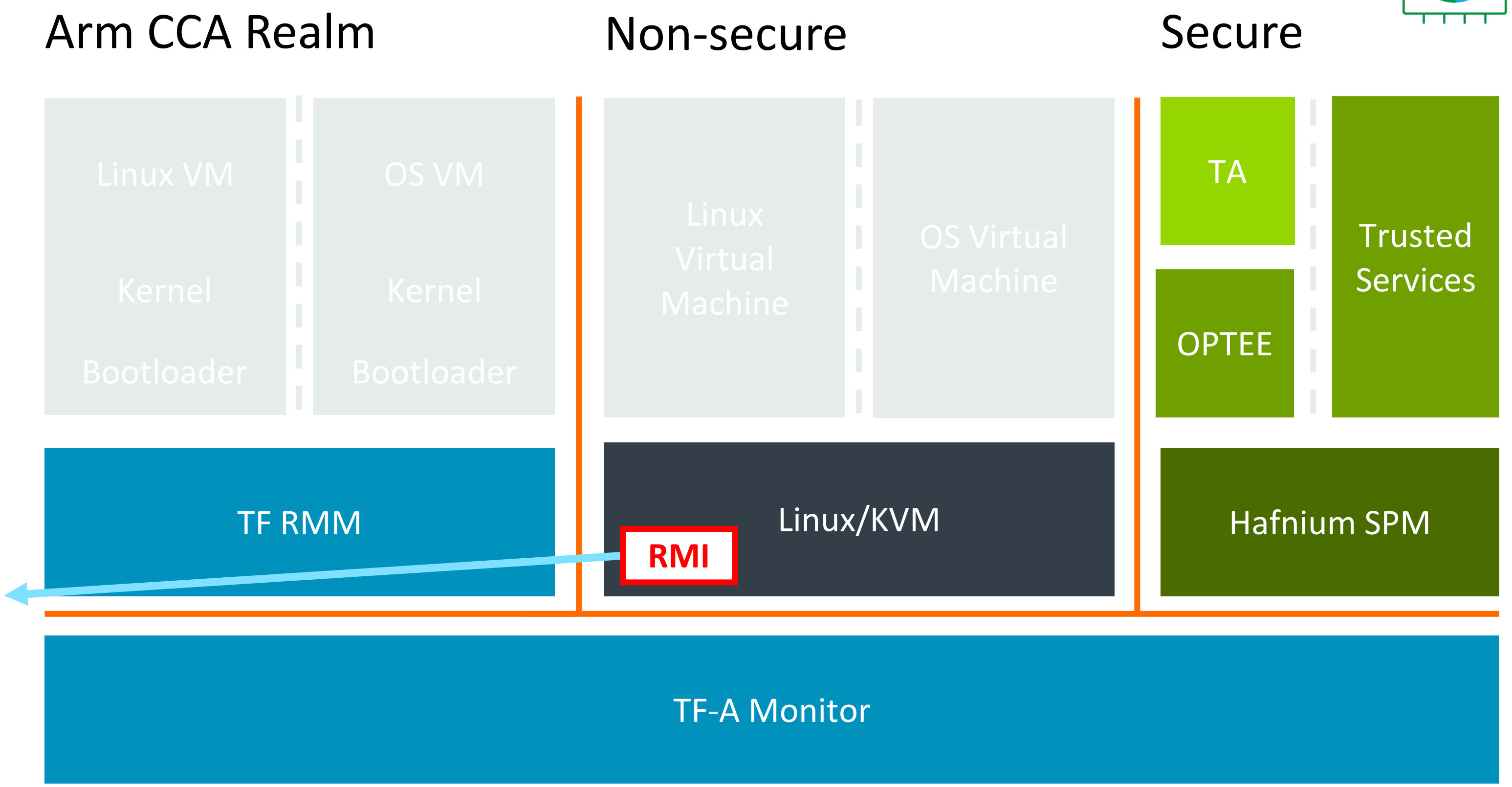
Brand new open source component

Dynamic Secure memory support

New TF-A Monitor

Open Source Software enablement

TrustedFirmware.org



Arm CCA Realm

Non-secure

Secure

Linux VM

Kernel

Bootloader

OS VM

Kernel

Bootloader

Linux Virtual Machine

OS Virtual Machine

TA

OPTEE

Trusted Services

TF RMM

Linux/KVM

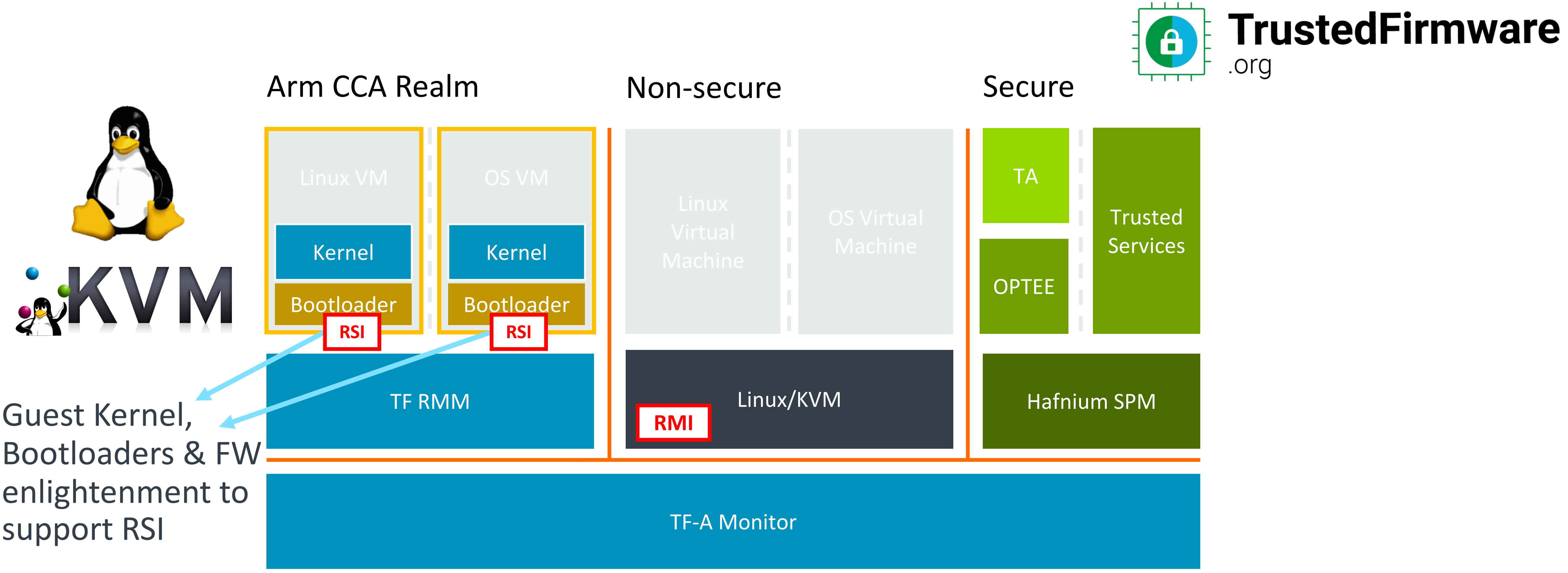
RMI

Hafnium SPM

TF-A Monitor

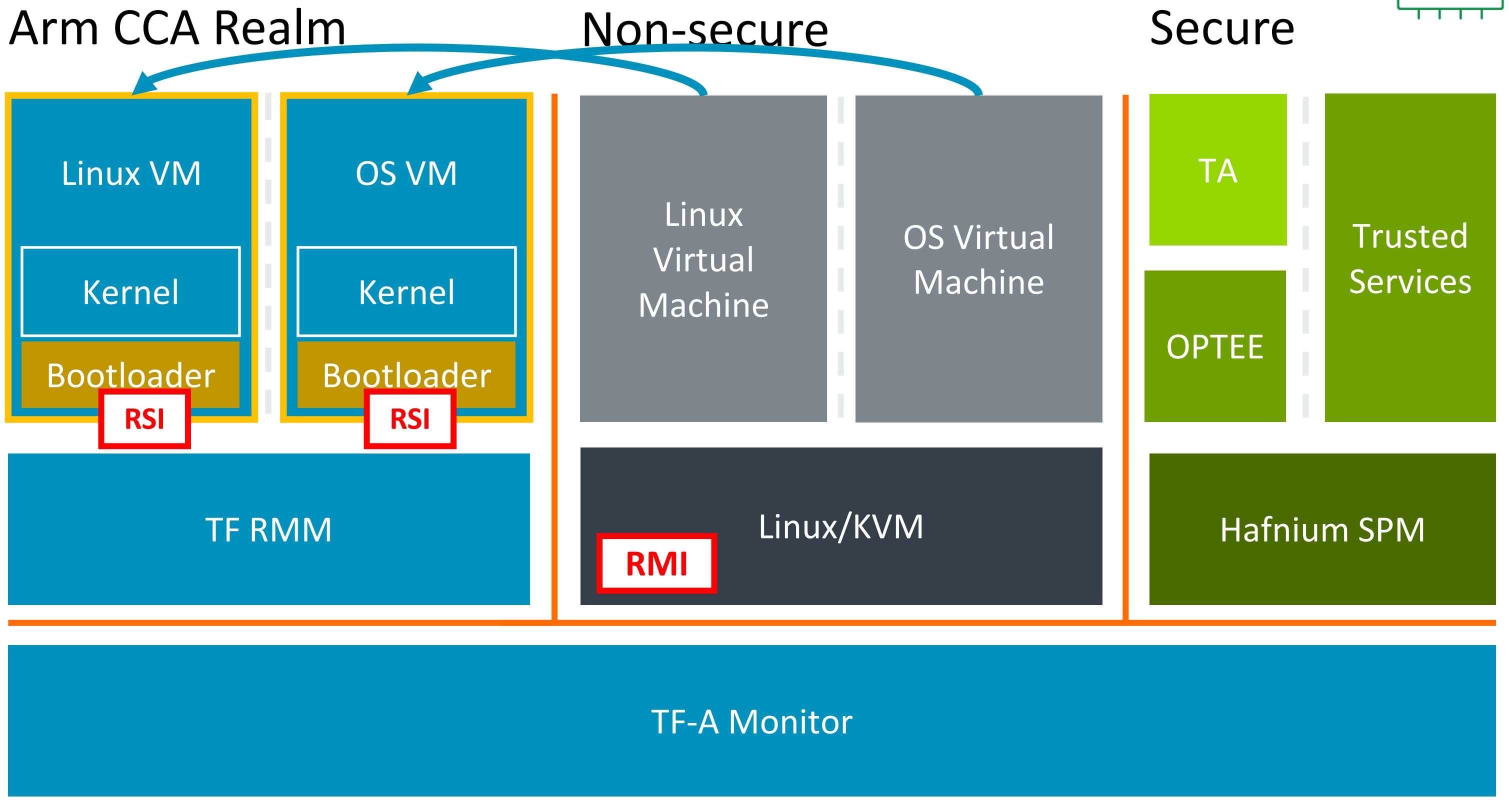
Host Kernel/KVM support for RMI

Open Source Software enablement



Guest Kernel, Bootloaders & FW enlightenment to support RSI

Open Source Software enablement



Introducing the TF-A Monitor development branch

- TF-A Monitor prototype branch published TODAY!

- Available as part of the TrustedFirmware.org Community Project.

- Demonstrating initial RME-enabled system
  - New boot flow
  - GPT support
  - Realm world & RMM dispatcher

- Listen to today's final session
  - **TF-A Monitor Firmware (deep dive)**

Open development and collaboration

- Plan to develop the Arm CCA software in the open, within respective open source communities
- Collaboration through:
  - Mailing lists
  - Public code reviews
  - Public Tech Forums
- Compilers + AEM Base FVP model + TF-A Monitor code provides starting kit for exercising the new architecture and help with the continuous development

Future Enablement plans

- RME evolution:
  - RME supplements will be incorporated by the 2021 revision of the architecture
  - AEM Base FVP update & Arm DS support added shortly after the above
  - TF-A Monitor will evolve in the open
    - TF-A Monitor alignment with upstream TF-A expected shortly after 2021 architecture revision publication

- RMM evolution:
  - RMM specification is expected to evolve throughout 2022
  - TF RMM reference & Kernel/KVM RFC patches will be posted following first publication of the spec
  - Continuous open development expected after that step, tracking spec evolution

Thank You

Danke

Gracias

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה