



BKK19-213

TF-M Services on Multi-Core System

Karl Zhang



Linaro
connect

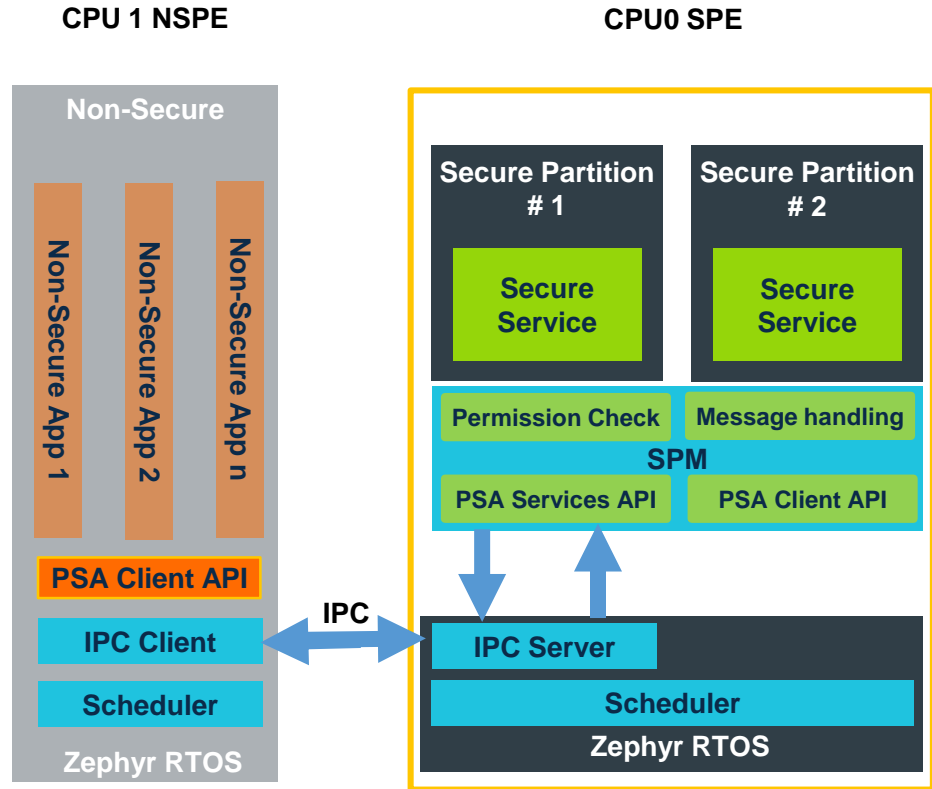
Bangkok 2019

Agenda

- Overview
- TF-M Modularization
 - Modular Services
 - SPM on RTOS
- Remote call for service
 - openAMP & eRPC
 - Accessing secure service
- Future plan
- Reference

Overview

- Multiple Core based
 - Physically isolated
 - IPM (MHU)
- RTOS adapting
 - Secure services
 - SPM implementation
- IPC
 - Asynchronous access
 - openAMP/ePRC
 - PSA compliance
 - Remote call





TF-M Modularization



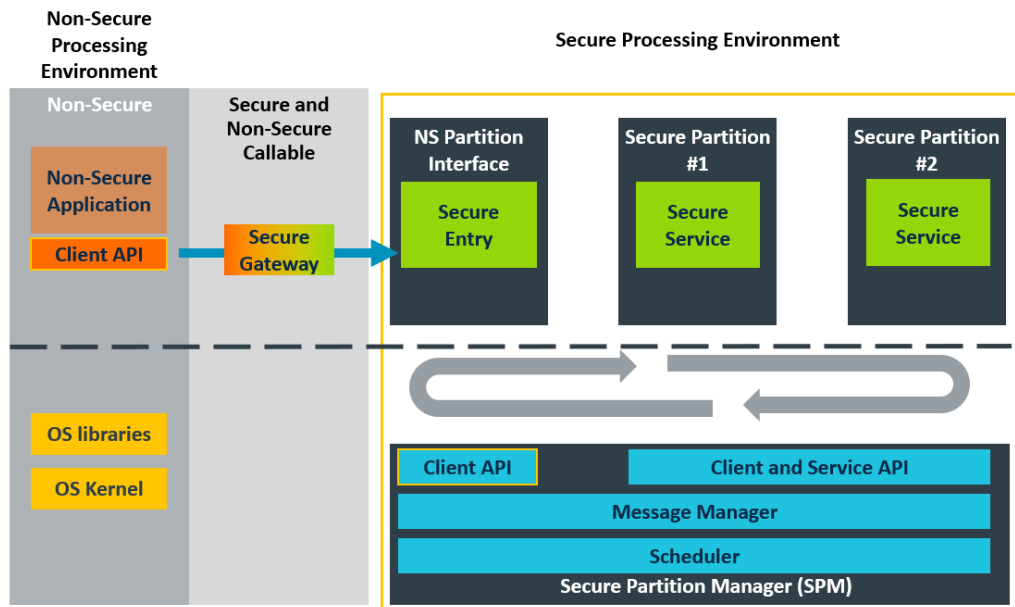
**Linaro
connect**
Bangkok 2019

Why TF-M modularization

- Reuse existing secure service in TF-M
 - Typically use TF-M as a whole
- Create your trusted OS quickly
 - PSA FF compatible is recommended

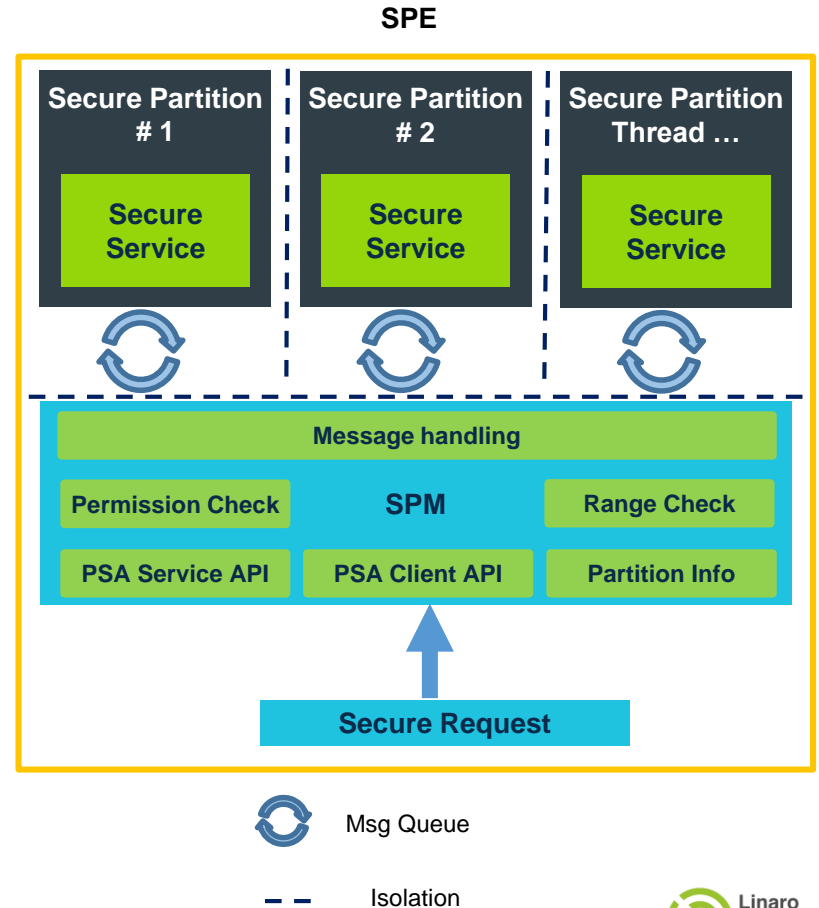
TF-M Modular scope

- Secure partition
 - Standalone lib for each partition
 - PSA APIs
- SPM
 - PSA FF Compliance
 - Manage info and states of SP (Secure Partition)
 - Handle messages to SP
 - Interfaces to IPC, OS kernel



SPM on RTOS

- PSA APIs
- Service serve one request at one time
- Range check based on isolation level
- Asynchronous access
- Ports to OS (MsgQueue/Semaphore)



A close-up photograph of a person's hands working on a green printed circuit board (PCB) in a workshop. The person is wearing a grey and white checkered shirt. The background is blurred, showing other people and warm lighting. A semi-transparent grey hexagonal shape is overlaid on the left side of the image, containing the text.

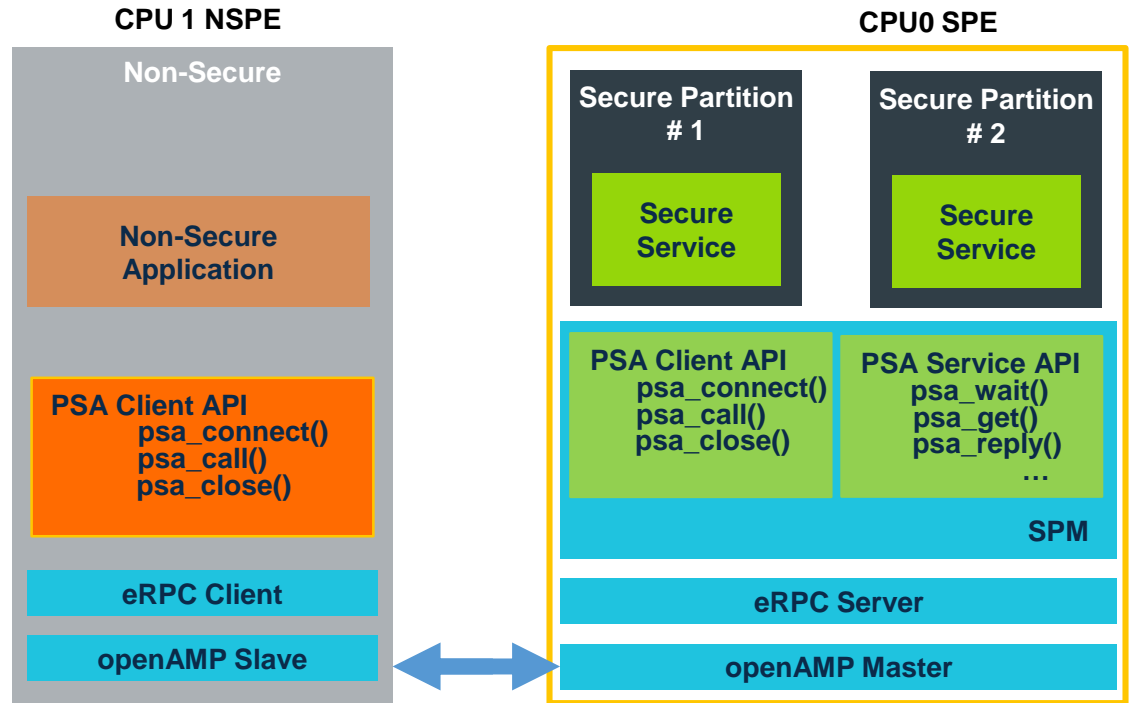
Remote call for service



**Linaro
connect**
Bangkok 2019

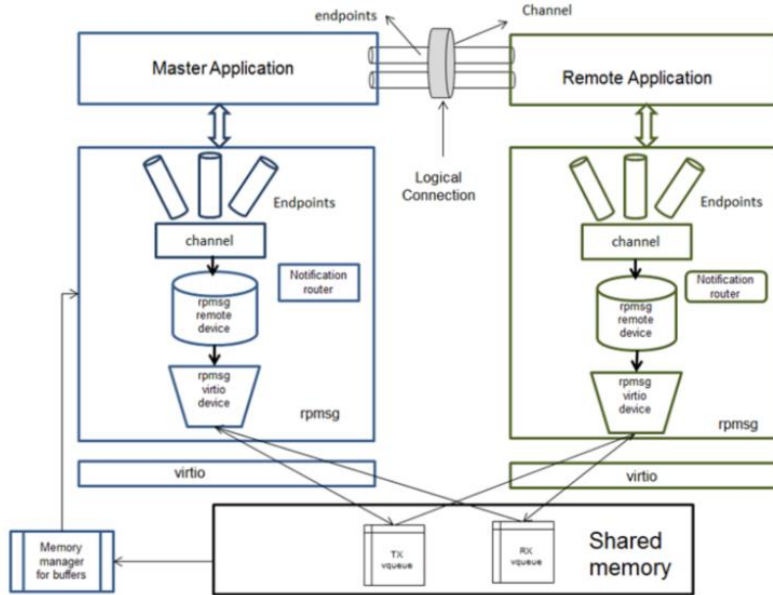
IPC - PSA FF APIs across multiple cores

- IPC based on open source project
 - openAMP
 - eRPC
- PSA compliant API
- Asynchronized

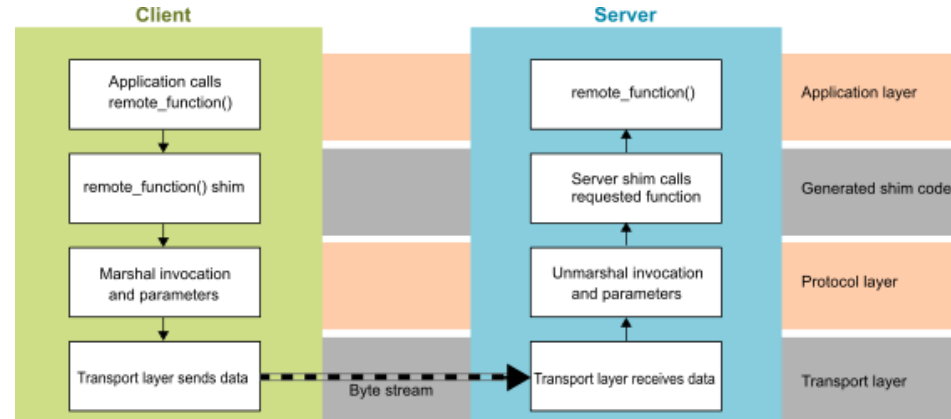


openAMP & eRPC

Figure 4-2. RPMsg Driver Components

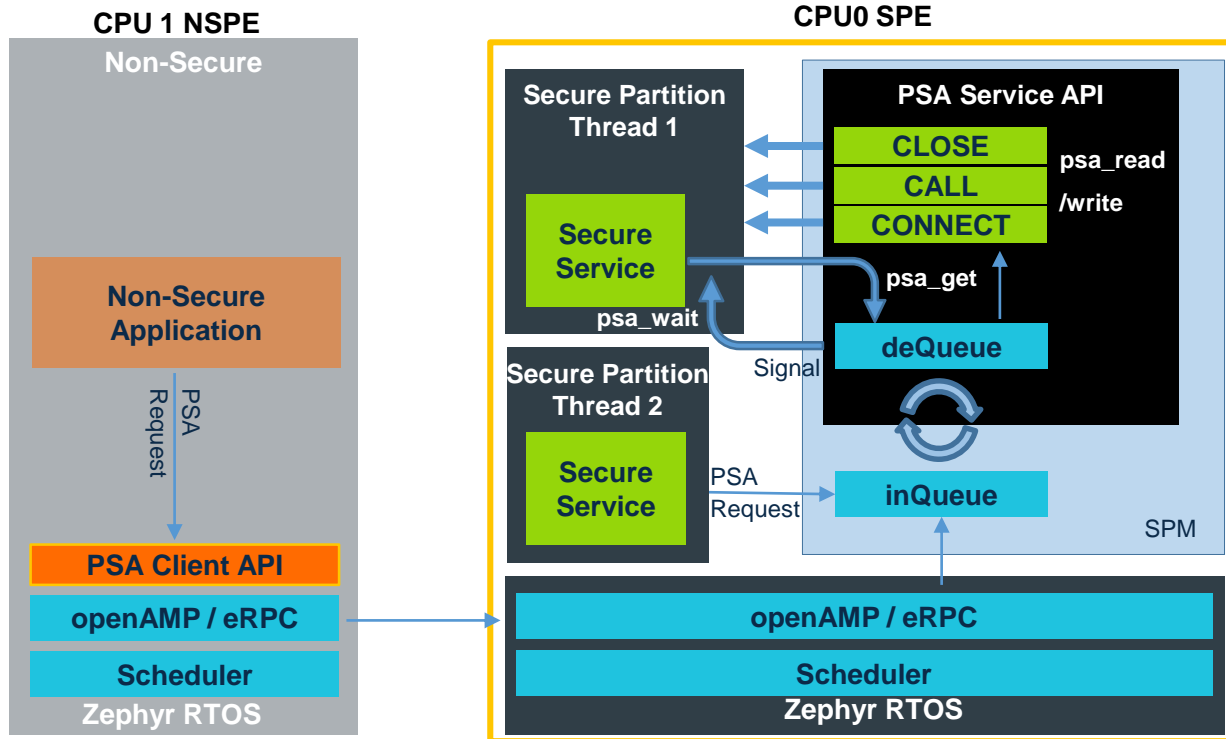


RPMsg in openAMP

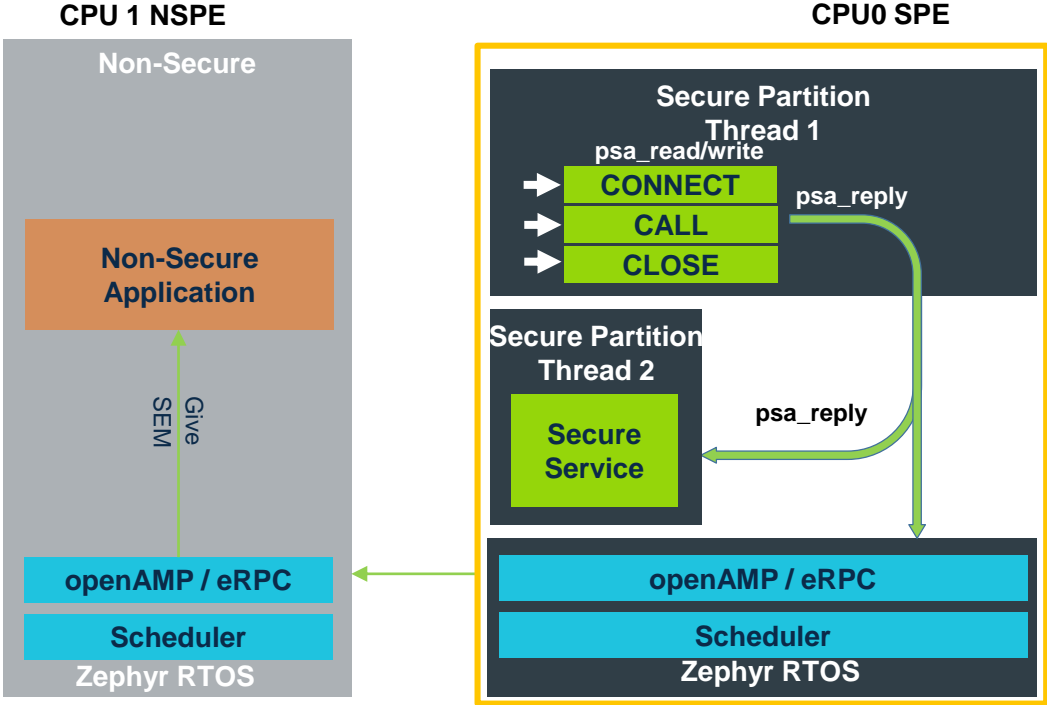


eRPC

Accessing secure service



Secure service reply



Changes in Progress

- Musca Dual-core support in Zephyr
- openAMP and eRPC on Musca
- IPC (PSA FF) design
- SPM modularization

[PR 12722](#)

Supported

Initial version

Start

Future Plan

- Multiple entry to secure call
- Isolation 2 and 3 on secure CPU

Ref

- [PSA](https://pages.arm.com/psa-resources-ff.html) <https://pages.arm.com/psa-resources-ff.html>
- TF-M <https://www.trustedfirmware.org>
- TF-M E-mail tf-m@lists.trustedfirmware.org
- OpenAMP <https://github.com/OpenAMP>
- eRPC <https://github.com/EmbeddedRPC/erpc>



TrustedFirmware
.org

Thank you

Join Linaro to accelerate deployment of your Arm-based solutions through collaboration

contactus@linaro.org



Develop & Prototype on the Arm Technology



Boards is a range of specifications with boards and peripherals offering different performance levels and features in a standard footprint.



**Linaro
connect**

Bangkok 2019