BKK19-213

TF-M Services on Multi-Core System

Karl Zhang
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
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 serves one request at one time
- Range check based on isolation level
- Asynchronous access
- Ports to OS (MsgQueue/Semaphore)
Remote call for service
IPC - PSA FF APIs across multiple cores

- IPC based on open source project
  - openAMP
  - eRPC
- PSA compliant API
- Asynchronized
openAMP & eRPC
Accessing secure service
Secure service reply

CPU 1 NSPE

Non-Secure Application

openAMP / eRPC

Scheduler

Zephyr RTOS

CPU0 SPE

Secure Partition
Thread 1

psa_read/write

CONNECT

CALL

CLOSE

Secure Service

psa_reply

Secure Partition
Thread 2

psa_reply

openAMP / eRPC

Scheduler

Zephyr RTOS
Changes in Progress

- Musca Dual-core support in Zephyr (PR 12722)
- openAMP and eRPC on Musca (Supported)
- IPC (PSA FF) design (Initial version)
- SPM modularization (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](https://www.trustedfirmware.org)
- TF-M E-mail  [tf-m@lists.trustedfirmware.org](mailto:tf-m@lists.trustedfirmware.org)
- OpenAMP  [https://github.com/OpenAMP](https://github.com/OpenAMP)
- eRPC  [https://github.com/EmbeddedRPC/erpc](https://github.com/EmbeddedRPC/erpc)
Thank you

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

contactus@linaro.org