TF-M Hybrid Platform Demo

Mate Toth-Pal

2024.04.11.

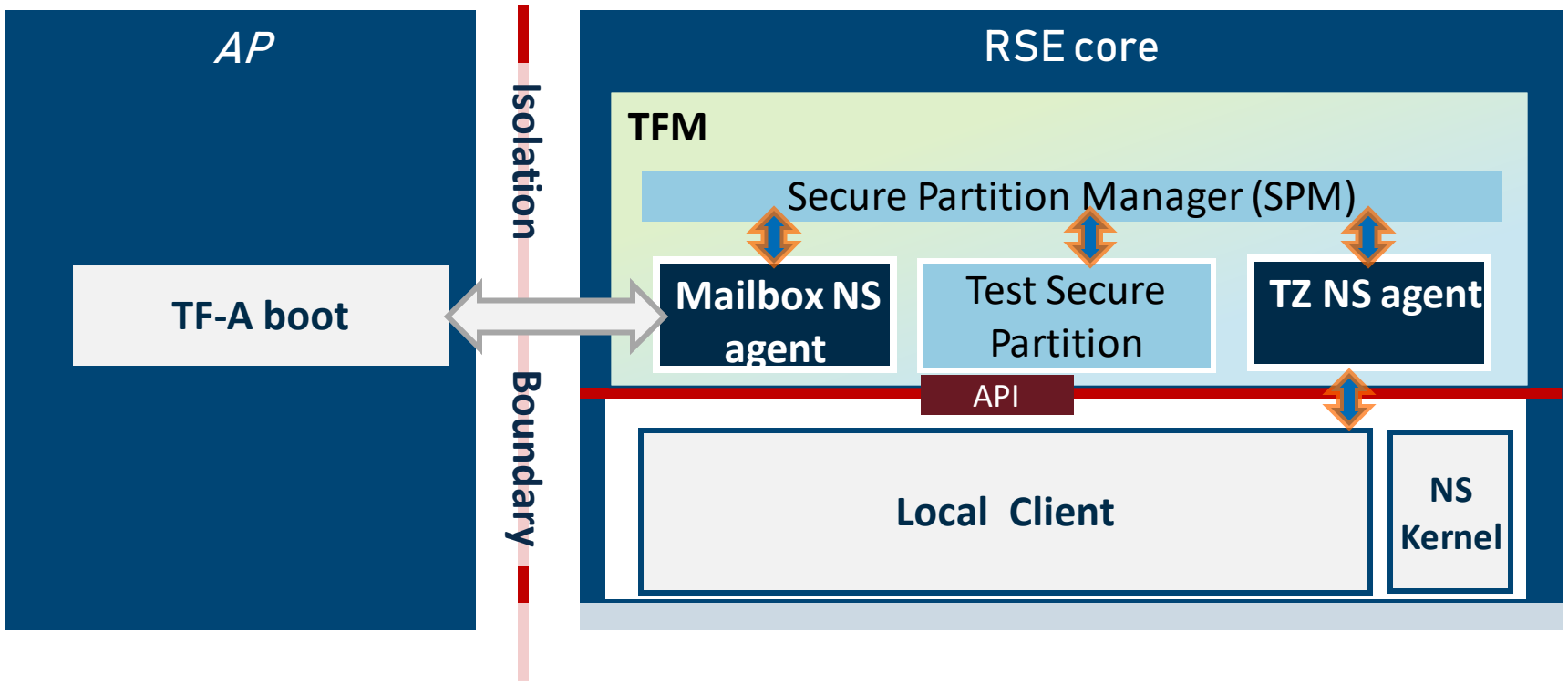
Hybrid platform

- A platform that contains a ARMv8-M core running TF-M with Non-secure clients in the NSPE and one or more additional A or M class core(s), that call secure services on the v8-M core.
- Hybrid platforms, and possible TF-M configurations for Hybrid platforms have been discussed earlier on TF-M tech forum
  - For Recording and slides see "Sept 14, 2023: Hybrid Platform Desing Update/Dev Branch Renaming" at https://www.trustedfirmware.org/meetings/tf-m-technical-forum/
  - In the presentation Ken proposes 3 possible TF-M configurations, called "solution"
  - Currently Solution 1 is available
- Demo is not aligned with any of the solutions, just demonstrates clients connecting to a TF-M secure service from a local and a remote client.

Platform

- The demo runs on the TC2 FVP (TC – Total Compute)
  - The TC2 platform has an Armv8M core that can run TF-M compiled to the arm/rse/tc platform, and an Armv8 core that can run TF-A, and is connected to the v8M core via mailbox
- For further information on the platform see
  - https://trustedfirmware-m.readthedocs.io/en/latest/platform/arm/rse/readme.html
  - https://totalcompute.docs.arm.com/en/latest/totalcompute/tc2/index.html

Demo setup



Changes made for the Demo

- The patch introducing uniform NS Client ID mapping is applied to TF-M: https://review.trustedfirmware.org/c/TF-M/trusted-firmware-m/+/26947
- The RSE platform code in TF-M is updated so that it accepts service requests coming from the AP that target the test service TFM_SECURE_CLIENT_SRV_DUMMY
- The TF-A bootflow is modified so that when the mailbox connection to the RSE is established, the service TFM_SECURE_CLIENT_SRV_DUMMY is called in an infinite loop
- The test service TFM_SECURE_CLIENT_SRV_DUMMY in tf-m-tests repo is modified so that it prints information on the service call
- The NS entry point in tf-m-tests repo is modified that instead of calling the tets framework, the service TFM_SECURE_CLIENT_SRV_DUMMY is called in an infinite loop

Demonstrated features

- TF-M can receive client calls from both local and remote clients
- Non-secure Client ID is mapped
  - The called service sees a different Client ID, even if the client in NSPE and on the AP uses Client ID –1.

arm

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు