SCMI server in TEE

Etienne Carrière - ST
Vincent Guittot - Linaro

Linaro Connect VIRTUAL 2020

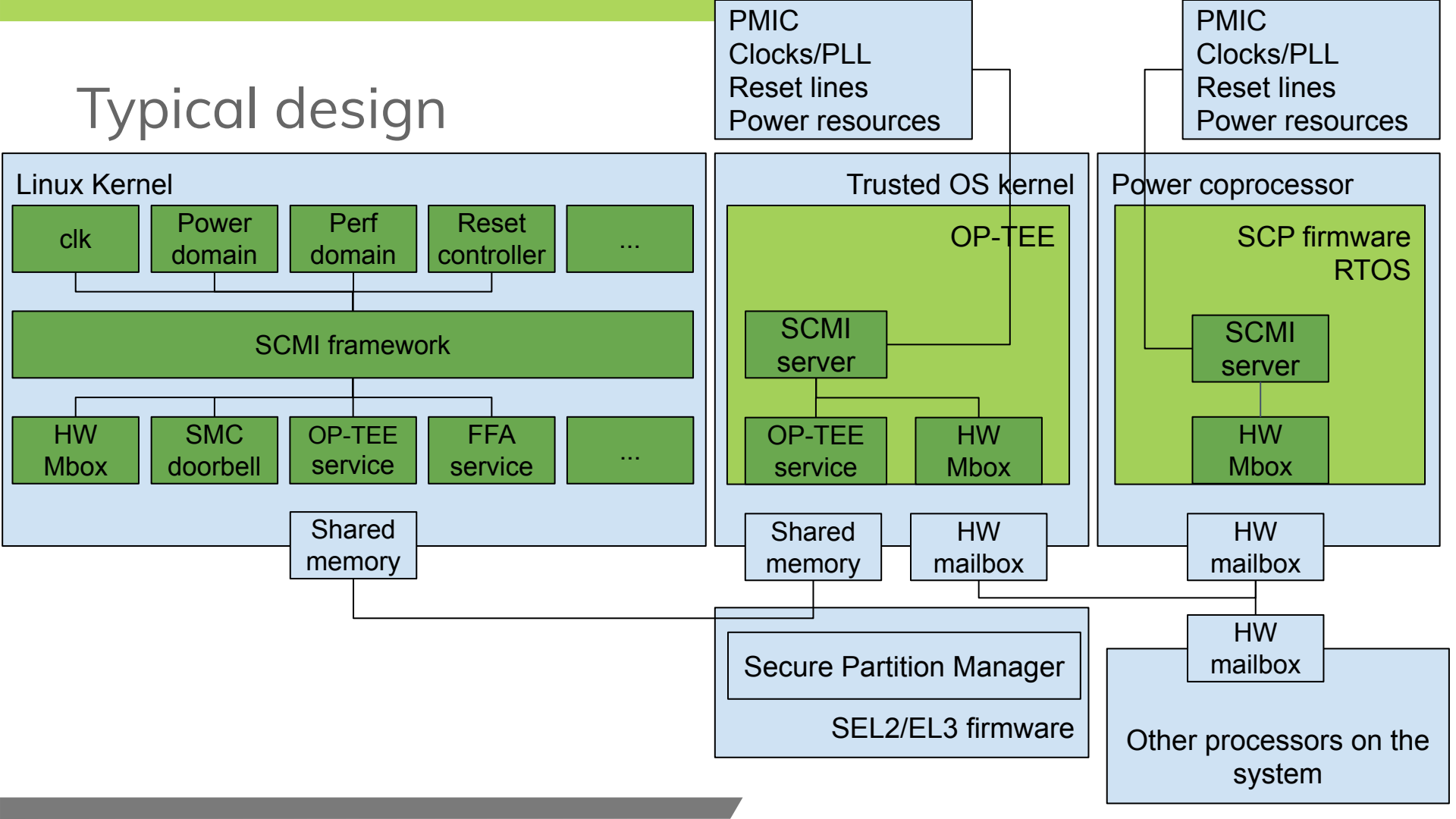
Agenda

- SCMI server in TEE
- Where to run ?
- Typical design
- SCMI server in OP-TEE
- Next steps
- Future steps

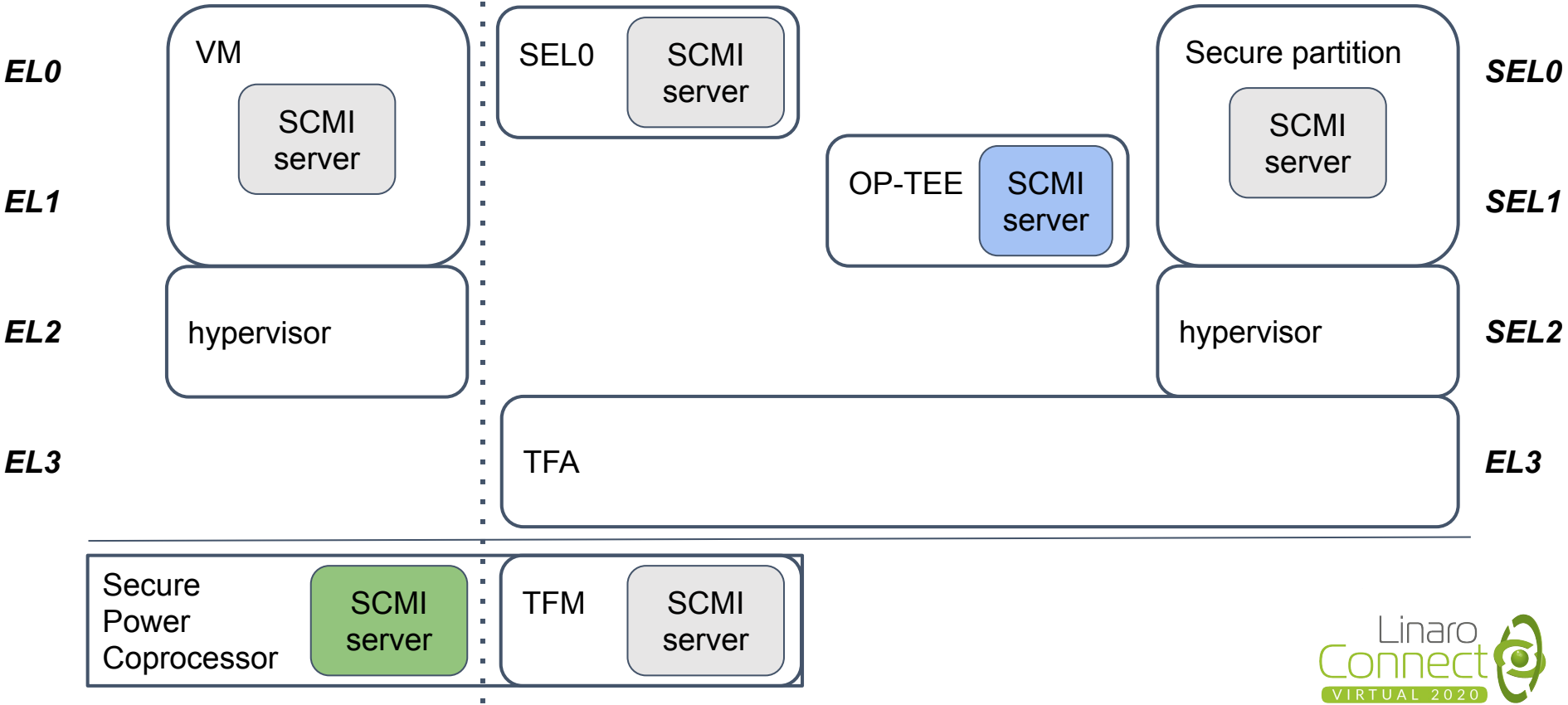
SCMI server in TEE

- Manage critical resources of a systems
  - without power co-processor
  - without enough channels
- Use SCMI server as a proxy
- Ease HW configuration
  - Server can run on different subsystems
- Use one SW for all configurations
  - Maximise SW reuse
- SCP firmware:
  - Implemented for cortex-M processor
  - SCMI server based on HW mailbox

Typical design



Where to run ?



SCMI server in OP-TEE

- Transport layer
  - OP-TEE shared memory
  - OP-TEE invoke command
- Support multiple messages per channel
  - Up to 8 pending messages for now
  - Messages are processed sequentially
- Support multiple channels
  - One OP-TEE session per transport channel
  - Enable to process multiple requests simultaneously

Next Steps

- Backport to mainline repository
  - SCP-firmware mainline support for SCMI server integration in OP-TEE
  - OP-TEE support of SCMI server pseudo TA
  - Linux OP-TEE transport layer in SCMI driver
  - U-Boot OP-TEE transport layer in SCMI driver
- Notification to Linux agent
- Supporting voltage regulator
- Device Tree support
  - Use at compile time
  - Use at boot time

Future steps

- SCMI server in secure partition cortex-A
  - SEL0 secure partition with TFA
  - Secure partition with FFA

- SCMI server in TEE for cortex-M

Thank you

Accelerating deployment in the Arm Ecosystem

Linaro Connect VIRTUAL 2020