linaro™

Arm Solutions at Lightspeed

Core Collective

Confidential Computing

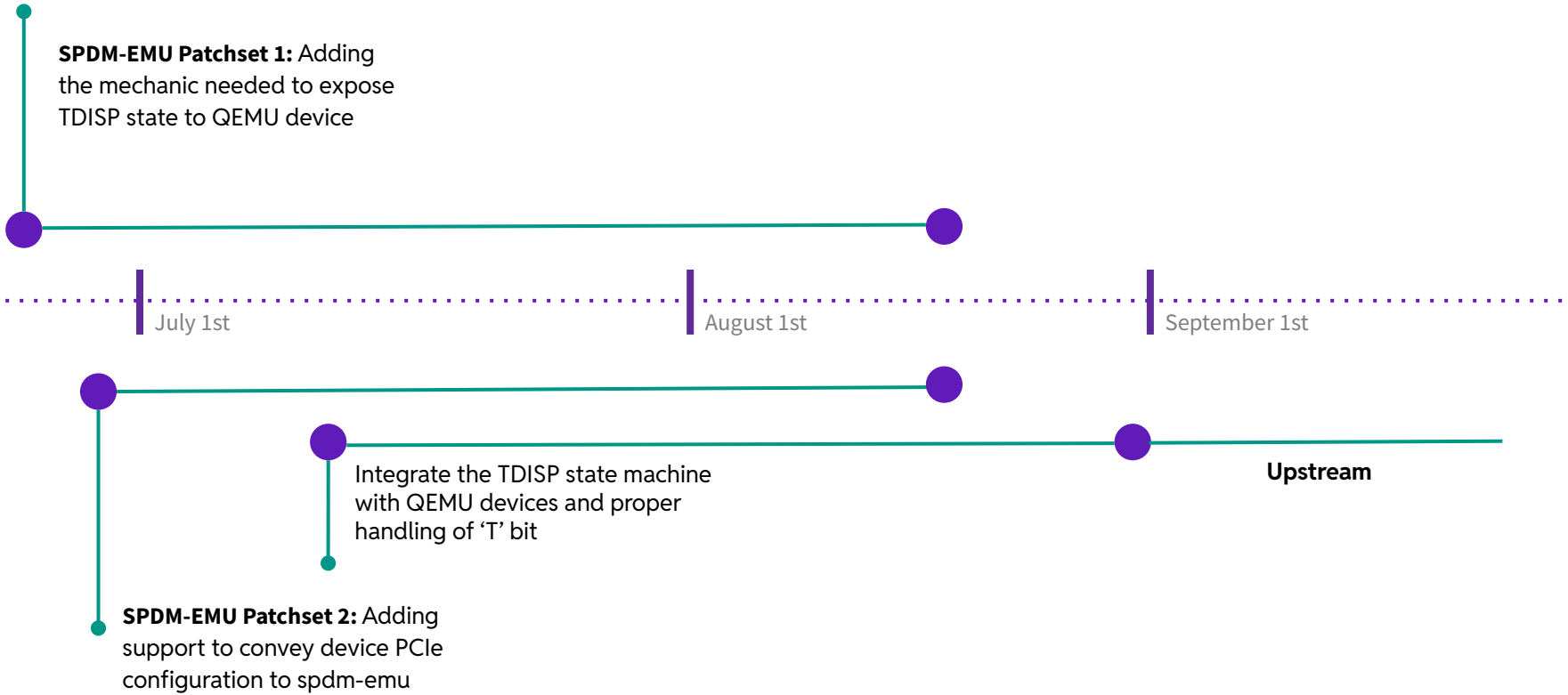
Update - June 20th

Progress Updates

- QEMU - System Emulation
  - 2 patchsets have been submitted to the spdm-emu project:
    - Goal: Properly support TDISP in QEMU
    - Patchset 1: Adding the mechanic needed to expose TDISP state to QEMU device
    - Patchset 2: Adding support to convey device PCIe configuration to spdm-emu
  - Work is now commencing to integrate the TDISP state machine with QEMU devices
    - What TDISP state is a device in?
    - Properly set the ‘T’ bit on PCIe DMA transaction when a device is in locked state

- Shrinkwrap support for QEMU
  - Work is ongoing → limited funding, limited progress

QEMU System Emulation

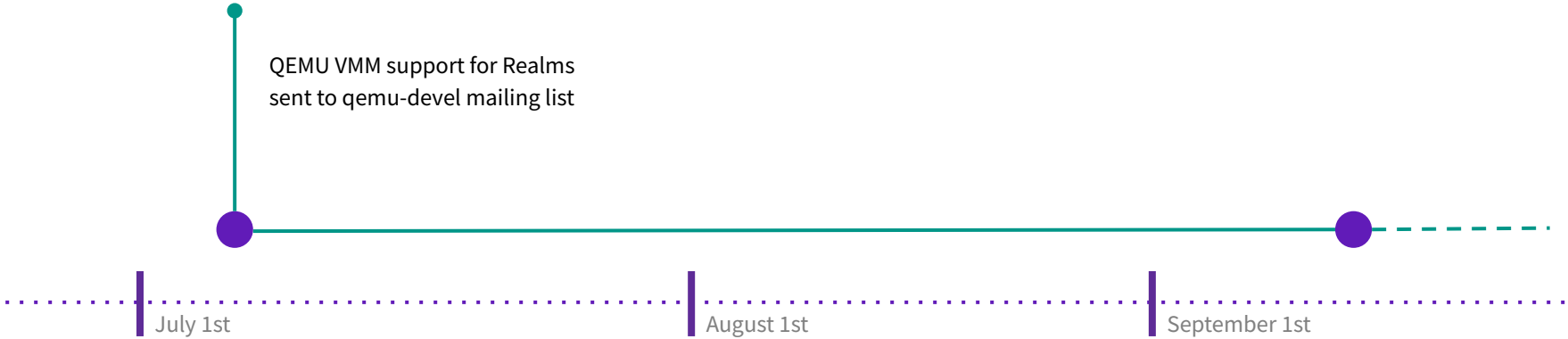


Progress Update

- QEMU - VMM
  - Foundational solution to start a Realm using the QEMU-VMM is ready for public release
  - Specifics: RMI 2.0, RSI 1.1, upstream kernel release: V13
  - Need to investigate if V14 can also be used
  - No support for Device Assignment
  - RFC sent out to some members of the Linaro QEMU team for initial review
  - Public release is imminent - this week or next week

- Ongoing Work:
  - Handling of Transparent Huge Pages (TPH) with MAP_PRIVATE memory attribute is broken on V14. Fix will be part of V15
  - In-place guest-memfd memory conversion
    - Pulled patches from here and here in a foundational branch
    - Works has started to adapt to CCA

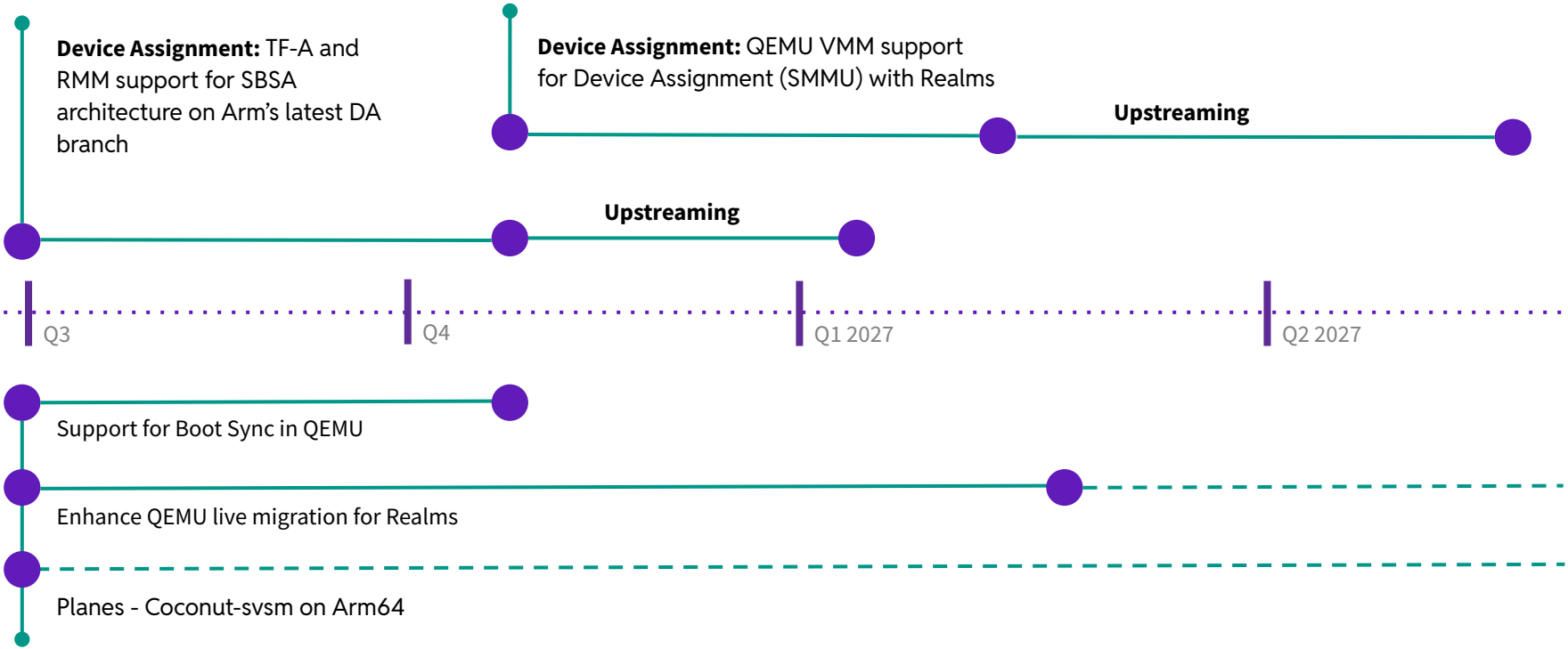
QEMU VMM Upstreaming



Backlog

- Device Assignment work
  - TF-A and RMM support for SBSA architecture with SMMU on Arm's latest DA branch
  - QEMU VMM device assignment support with Realms
  - Depends on a stable baseline (kvmtool, TF-A, RMM, kernel) from Arm
- QEMU support for Boot Sync
- Enhance QEMU Live Migration support to Realms
- Planes → coconut-svsm on Arm64
- Integration of the kernel's device security module with Veraison (3rd party authentication)
- Confidential Containers

Backlog (*HYPOTHETICAL*)




linaro
linaro
linaro