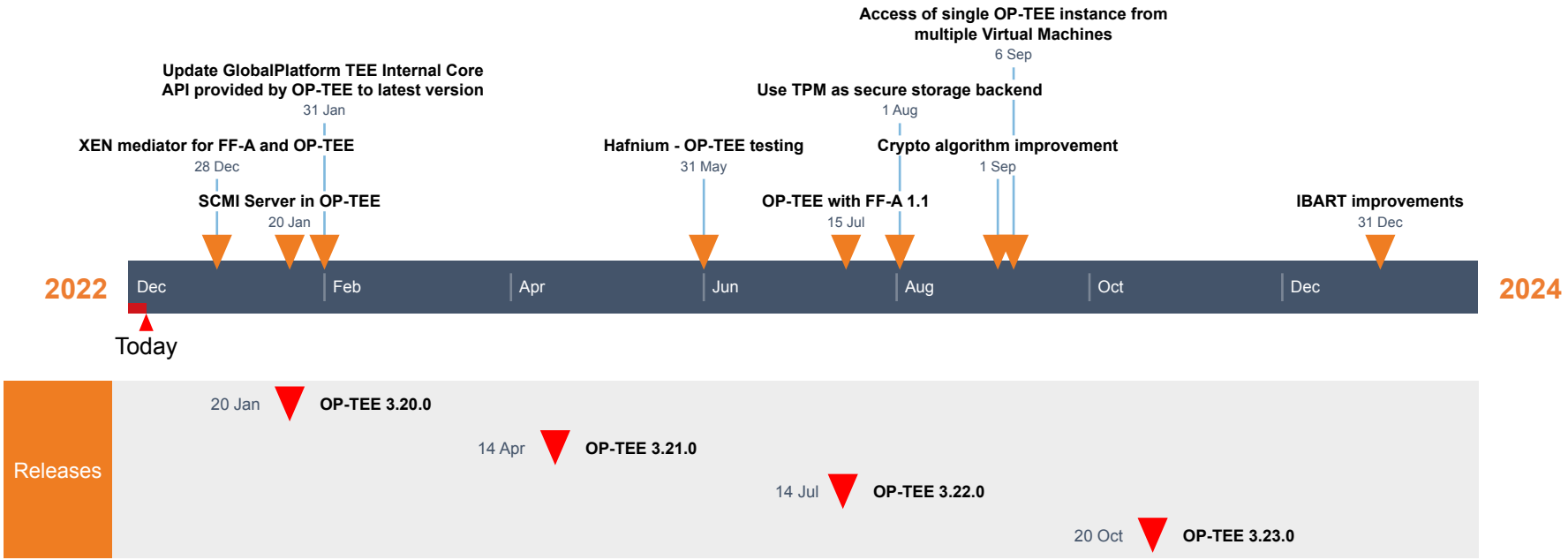
OP-TEE Updates

2023-01-19 Ilias Apalodimas & Julianus Larson

Linaro's OP-TEE contributions (OP-TEE)



OP-TEE Summary

- Delivered since last review (2022-05-13 1/2)
  - Multiple TA signers (using subkeys)
  - SCMI server support
  - SHA-512 and SM3 using ARMv8.2-A cryptographic extensions
  - Add support for compiler stack protector (Core and TAs)
  - Adds support for the SM4-XTS algorithm
  - Adds mitigations in TA loading against hardware fault injection attacks
  - Reject weak hash algorithms when verifying for instance signed TAs
  - PAC for OP-TEE Core
  - MTE support
  - RNG driver based on Arm SMCCC TRNG interface
  - Preallocate translation tables for S-EL0 contexts
    - We used to have a static amount of translation tables
    - If enough TAs were loaded, we had to wait and block if no tables were available
    - That would not work for SPs
  - TPMv2 basic support (might be removed in the future)

OP-TEE Summary

- Delivered since last review (2022-05-13 2/2)
  - Elliptic curve algorithms Ed25519, Ed25519ctx and Ed25519ph as defined in TEE Internal Core API v1.3.1, as well as PKCS#11 support
  - Updates to LibTomCrypt, MBedTLS
  - Loading SP images from the TF-A FIP
  - New platforms Arm Corstone-1000, NXP i.MX 93 EVK and TI K3 J784S4
  - Self-tests for SPMC

OP-TEE Summary

- In progress
  - TPMv2 as a secure storage backend
  - Support 1.3.1 GP APIs (will be merged after 3.20)
  - FF-A support for the XEN mediator (patches under review)
- Next
  - FF-A 1.1 updates
  - Crypto algorithm improvements and additions
    - GP 1.3.1 has a few new mandatory algorithms (e.g SHA3)
  - Hafnium and OP-TEE testing
  - IBART improvements