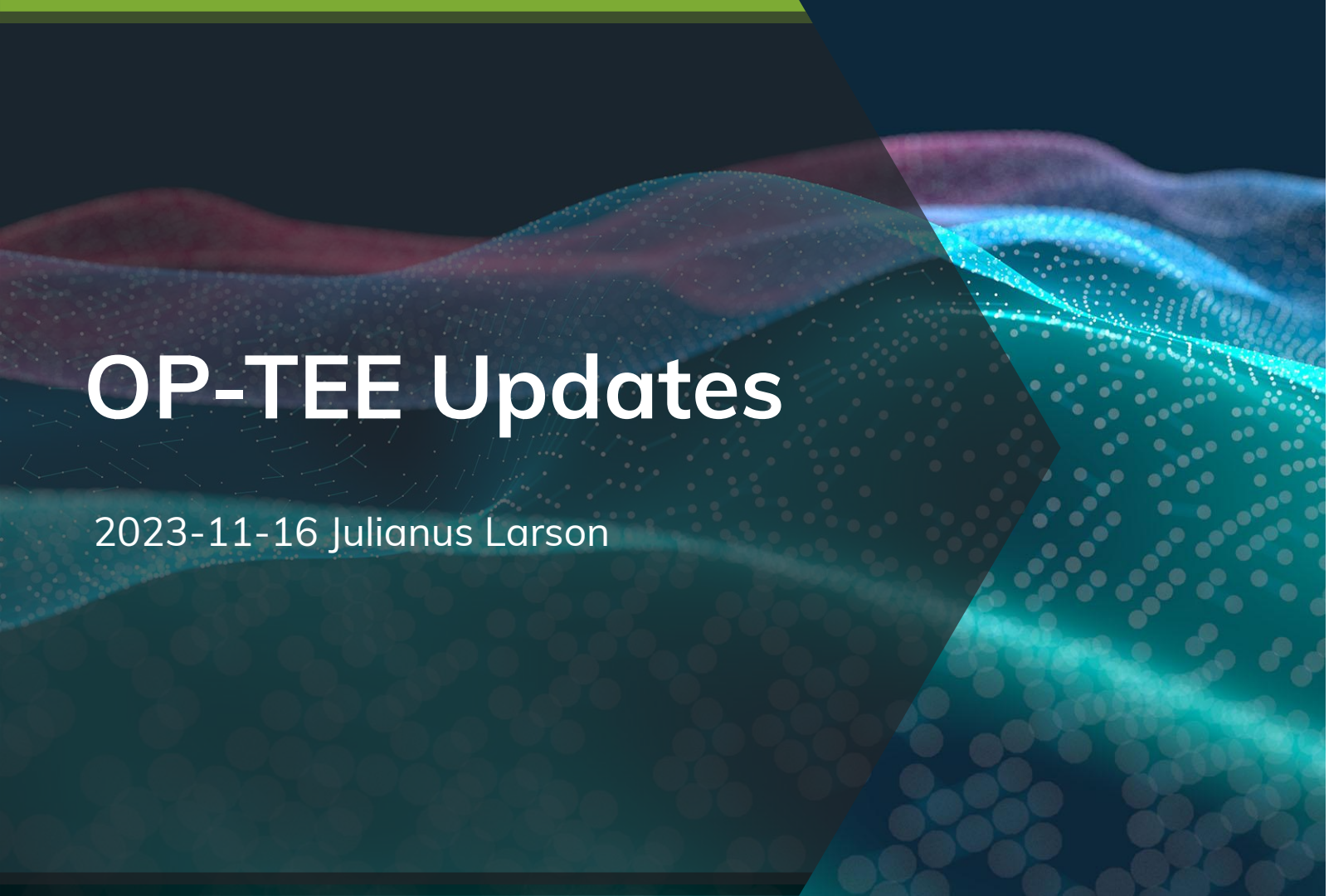
# OP-TEE Updates

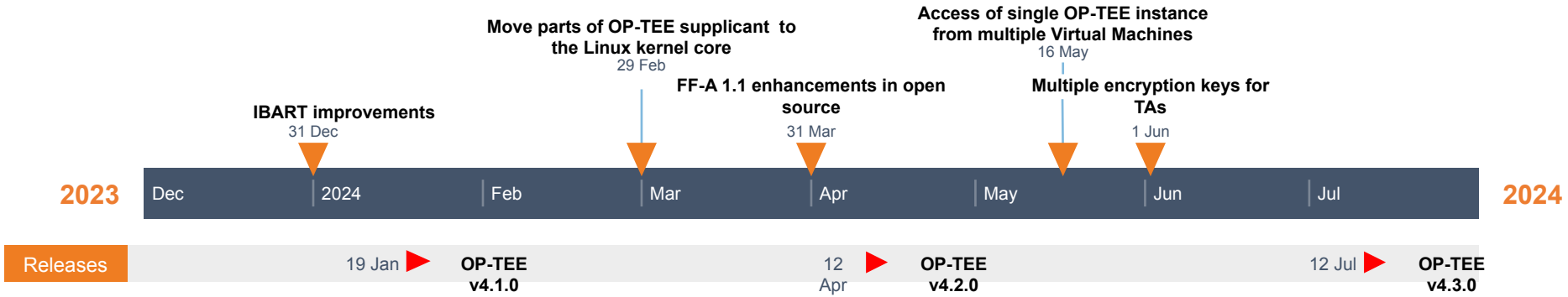
2023-11-16 Julianus Larson



# OP-TEE Summary

- Delivered since last review (2023-01-19)
  - OP-TEE 3.20.0 released 2023-01-20
    - Signing TAs using subkeys - Enabling key hierarchies
  - OP-TEE 3.21.0 released 2023-04-14
    - Miscellaneous improvements
  - OP-TEE 3.22.0 released 2023-07-07
    - Support for FF-A v1.1
  - OP-TEE 4.0.0 released 2023-10-20
    - OP-TEE follows Semantic Versioning 2.0.0 and we're making incompatible API/ABI changes
    - The changes are needed to make the code easier to maintain and to keep up with changes in third-party code
    - Backwards compatibility is not guaranteed, but will work in most cases
    - Support for PAN (Privileged Access Never)

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

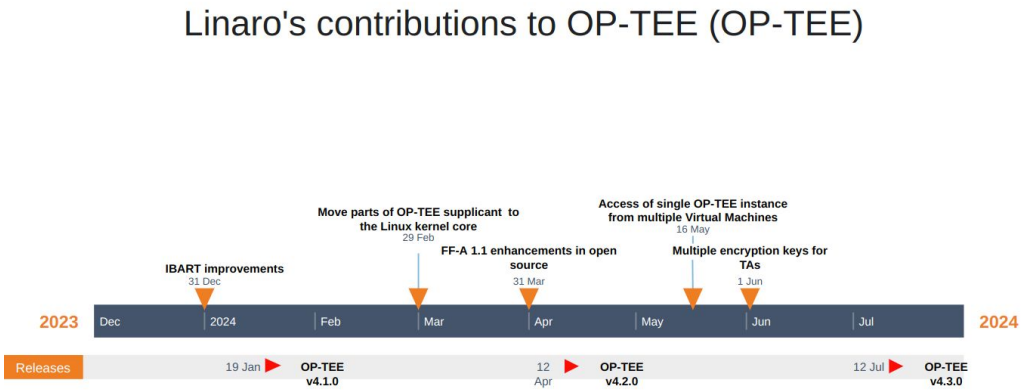


# OP-TEE Roadmap - IBART improvements

IBART is the test framework verifying every single patch going into the OP-TEE project. The way it works is that every time a pull request is sent to the OP-TEE project, a webhook is triggered and a payload is sent to the IBART instance, which in turn either starts a build or puts a job into a build queue if there are already ongoing builds.

Improvements

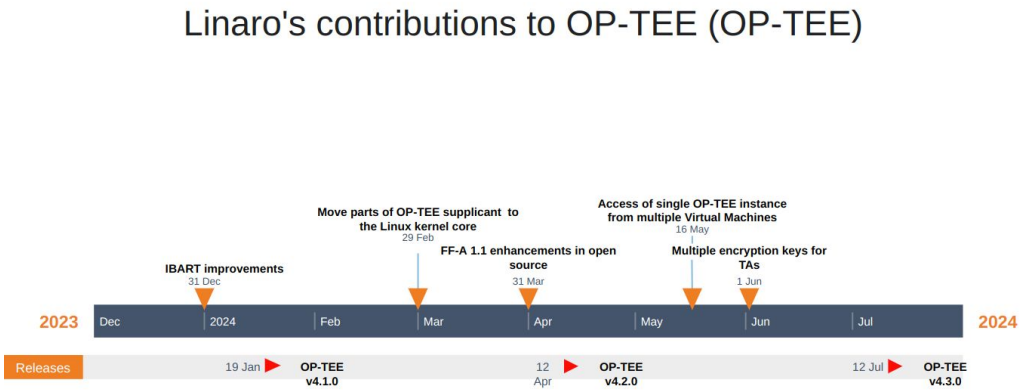
- RockPi4 hardware and software support
- Parallel builds
- Use merge branch
- Live logging
- Remove QEMU empty line
- Re-enable optee-example
- Support remote yaml (.ibart.yaml)
- Timeout improvements



# OP-TEE Roadmap - Move parts of OP-TEE supplicant  to the Linux kernel core

Right now accessing an RPMB through OP-TEE implies we will have a userspace application (the op-tee supplicant) running.

It would be beneficial to have the part of the op-tee supplicant that deals with the RPMB accesses inside the linux kernel, as it would make the entire operation more secure and at the same time allow distros to support the various features without depending on a userspace application.



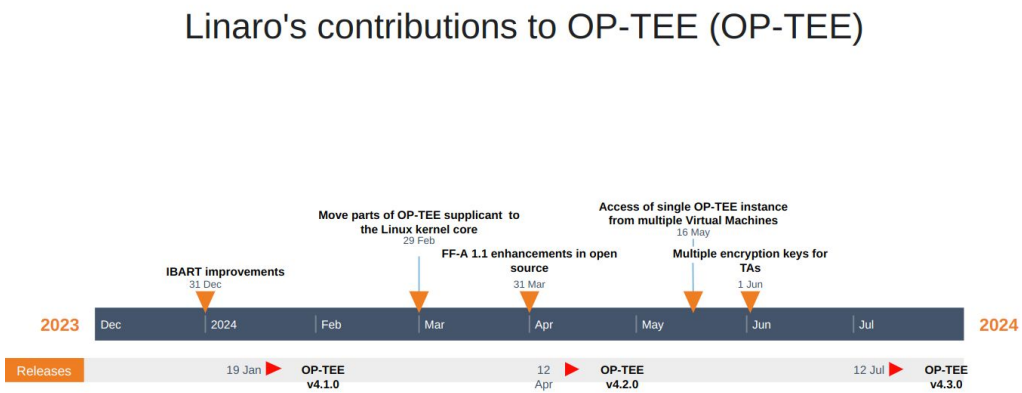
# OP-TEE Roadmap - FF-A 1.1 enhancements in open source

FF-A 1.1 support has been recently added to OP-TEE in release 3.22.0.

With the initial support in place, there are various open-source projects that need enhancements and new features to support FF-A 1.1 and take advantage of the improvements it offers.

Main focus is on Xen:

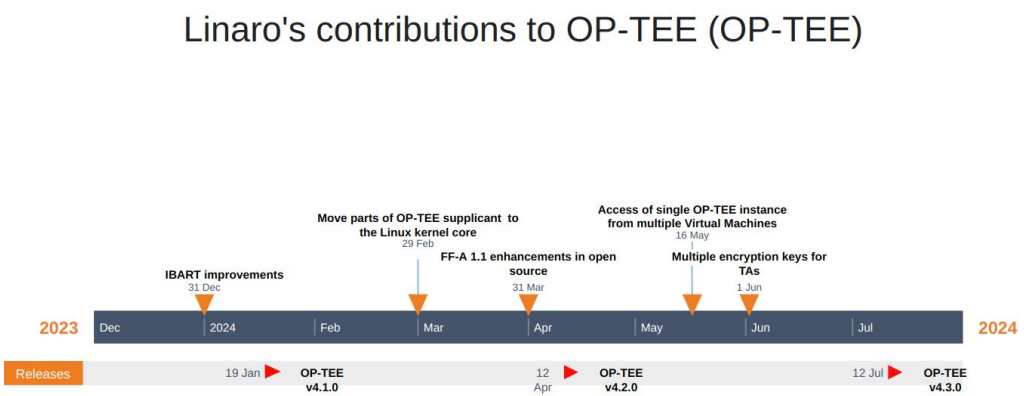
- Basic FFA-1.1 has been added to Xen and will be included in the coming Xen release.



# OP-TEE Roadmap - Access of single OP-TEE instance from multiple Virtual Machines

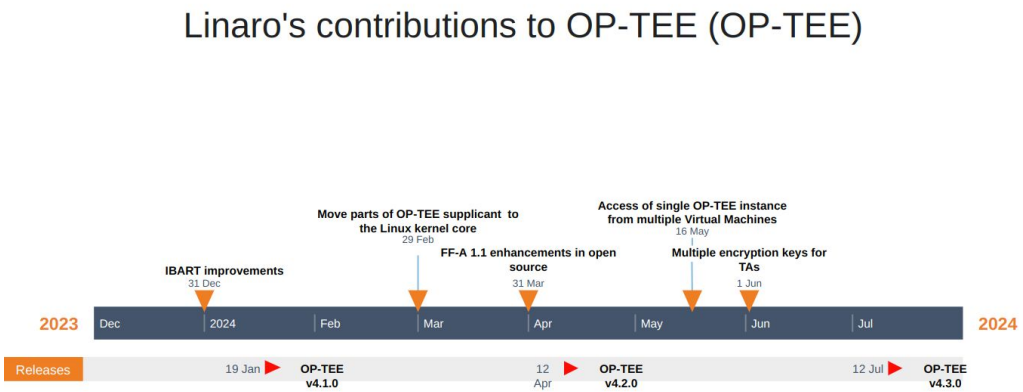
Accessing the Trusted Execution Environment (TEE) should work in the exact same way as for a native system as from a guest VM.

Need a good use case as a base for the development.



# OP-TEE Roadmap - Multiple encryption keys for TAs

In the same way as sub keys exists for signing it shall be possible to have a hierarchy of encryption keys. This way the encryption key does not need to be shared with others.



# Releases

- New versions of OP-TEE are released four times a year, i.e., quarterly releases.
- Releases are made based on what is merged into the master branch.