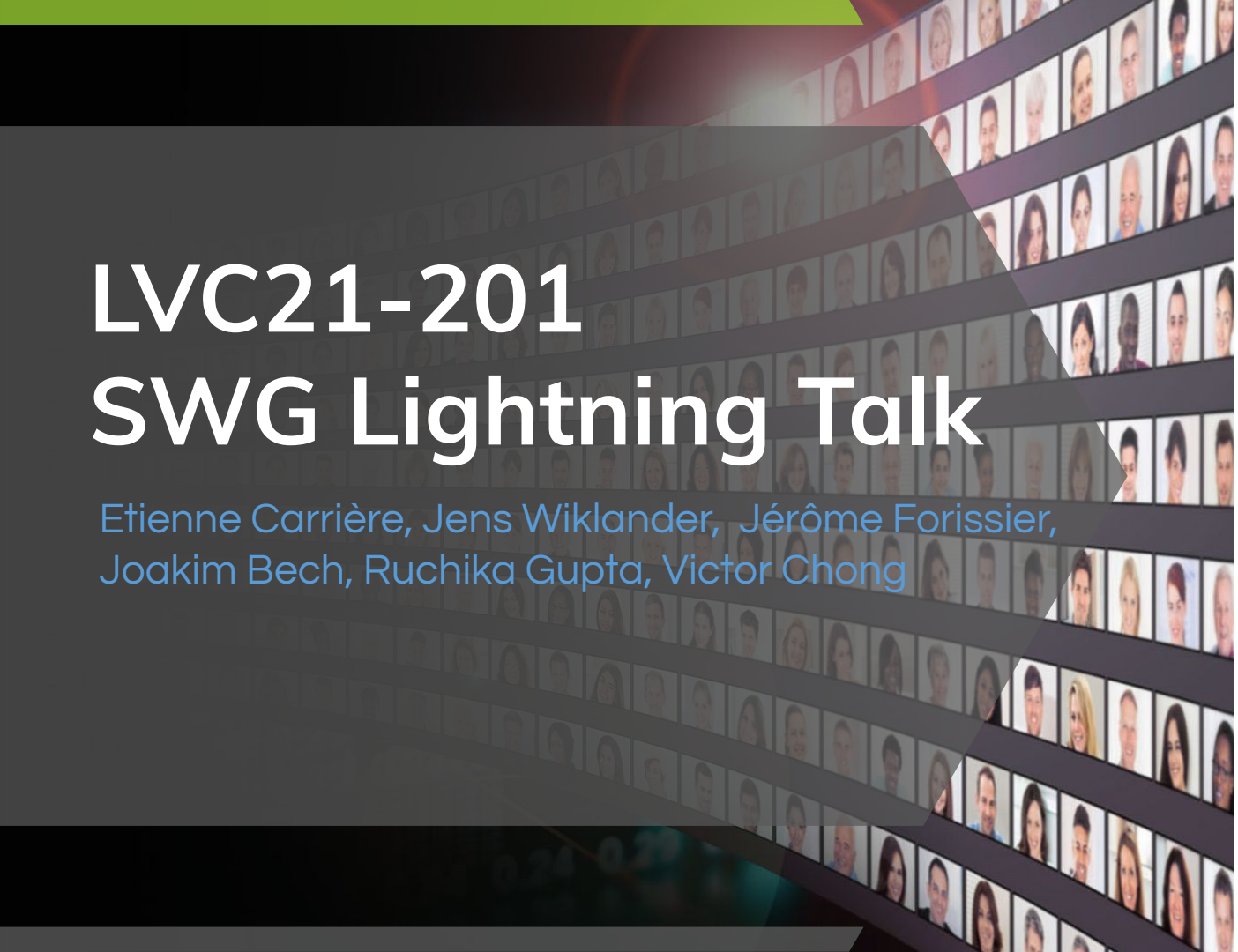


LVC21-201
SWG Lightning Talk

Etienne Carrière, Jens Wiklander, Jérôme Forissier,
Joakim Bech, Ruchika Gupta, Victor Chong

Linaro Connect
VIRTUAL • SPRING 2021

Agenda

- General OP-TEE Updates
- PKCS#11
- GP-TEE Compliance - GP test v2.0.0.2
- Standalone MM with OP-TEE
- FF-A and Secure Partition Updates
- SCMI Message Drivers
- AOSP and Keymaster
- DRM - OEMCrypto library (Widevine DRM)
- OP-TEE Security issues

General OP-TEE Updates

- OP-TEE v3.12.0 release in January
- Active community on github contributing to OP-TEE.
  - ~30 different SoC's, ~50 different platforms from ARM, Amlogic, Atmel, Broadcom, HiSilicon, Marvell, MediaTek, NXP, Renesas, Rockchip, Socionext, STMicroelectronics, TI, Xilinx
  - Crypto framework extended to add hardware accelerators by Clement (NXP)
  - SE050 driver by Jorge Ramirez-Ortiz (Foundries.io)
  - tee-supplicant Plugin Framework by Aleksandr Anisimov (Omprussia)
  - OP-TEE based hwrng driver, Trusted TEE Keys Framework (Sumit Garg , Linaro)
- Monthly Meeting for LOC (Linaro OP-TEE Contributions).
  - Details of the meeting available at [1].
  - Previous meeting notes and recordings available at [2].
  - Project Page at [3].

[1] - https://www.trustedfirmware.org/meetings/ [2] - http://bit.ly/loc-notes
[3] - https://www.linaro.org/projects/#LOC

PKCS#11

- OP-TEE/PKCS#11 was presented at HKG18 [1] as a initiative and work was done on private branches. Details available here [1]
- This work is being reviewed, matured and integrated in OP-TEE as PKCS#11 TA.
  - Object management, session management, few flavors of AES, HMAC, Key Generation, Derivation for symmetric keys, random number generation.
  - Testing - Tests being added in xtests as more API's are added. We are also using SoftHSM Tests and pkcs11-test from Google wherever possible.
- Next steps
  - Wrap/Unwrap Keys, RSA & EC support, symmetric ciphers
  - Add Documentation in optee docs.
- Thanks to the contributors for fixes and improvements (Gabor, Rouven, Vesa Jääskeläinen)
  - Vesa added support for TEE based authentication [2] and has been actively helping in reviewing and upstreaming functionality
- LVC21 session dedicated to this: LVC21-215 PKCS#11 in OP-TEE, Wed 24th, 11h30 UTC

[1] - https://github.com/OP-TEE/optee_os/issues/4283

[2] - https://github.com/OP-TEE/optee_os/pull/4222

GP-TEE Compliance (GP Test v2.0.0.2)

- Starting from OP-TEE v3.11.0, OP-TEE was updated to support the TEE_Initial_Configuration-Test_Suite_v2_0_0_2-2017_06_09.7z version from the GlobalPlatform Compliance Test suite.
- These tests are included in our current CI (IBART), so it'll no longer just run the publicly available xtest, but also run the GlobalPlatform test suite when people are sending patches upstream to the OP-TEE project.
- xtest can be extended/patched to include the GlobalPlatform Compliance Test suite. This can be done by downloading the GlobalPlatform Compliance Test suite (a *.7z file) and add an additional compiler flag (GP_PACKAGE) to the make invocation line, example:

```
$ make GP_PACKAGE=/tmp/TEE_Initial_Configuration-Test_Suite_v2_0_0_2-2017_06_09.7z
```

Note - The GlobalPlatform test suite is not free and therefore the OP-TEE project cannot upstream GlobalPlatform tests directly to the project itself. The package is free for GP members and can be purchased by non-members.

StMM with OP-TEE

- Standalone Management Mode PI is an EDK2 application used to store EFI variables in OP-TEE

- Due to limitations on the current platforms where it is only possible to run a single payload on the secure side (S-EL1), a decision had to be made and as a stepping stone to future architectures, Linaro in collaboration with Arm ended up adding support in OP-TEE such that was possible to use StMM more or less unmodified.

- Changes made in OP-TEE
  - Support available in OP-TEE for creating a secure partition - A Secure Partition is an unprivileged software sandbox environment running in the Secure World, under the control of privileged software. (OP-TEE)
  - PTA in OP-TEE for encapsulating/decapsulating MM message
  - Patches in OP-TEE - StandaloneMM together with OP-TEE

FF-A and Secure Partition Updates

- FF-A S-EL1 SPMC Prototype

- Secure Partition at S-EL0 groundwork with the pull requests
  - Add Secure partitions to OP-TEE image
  - Rename stmm
  - core: ldelf: implement separate syscalls for ldelf
  - Separate ldelf from user TAs

- OP-TEE as SP at S-EL1 is progressing
  - Based on [PATCH v4 0/7] firmware: Add initial support for Arm FF-A
  - With Hafnium at S-EL2 as SPMC

SCMI Message Drivers [scmi-msg/]

- Helper drivers for minimalistic SCMI server implementation
  - Clock & reset controllers (since 3.9.0), voltage controllers (since 3.11.0)
  - SCMI message drivers are also merged in TF-A (since v2.4)
  - Compliant with SCMI client drivers in Linux kernel (v5.9+) and U-Boot (v2021.01+), SCMI transport drivers (mailbox or SMCCC v1.0)
  - Next steps: DFVS? power domains?
  - Not designed for complex SCMI event scenario (async. events, notifications, etc...)

- Scheme: drivers get an SCMI message payload from some IPC memory, identify the content, call necessary platform handler functions, forge and write back the SCMI response message.

- Linaro is also porting a full fledged of SCMI server in OP-TEE and other hosts environments [1] based on SCP-firmware repository for more complex scenario
  [1] https://www.linaro.org/projects/#SCMI, SAN19-207, LVC20-118.

AOSP and Keymaster

Current State

- Hikey960 AOSP master (Nov 2020) dev build with v3.9.0 based OP-TEE
  - Some regressions in xtest and VtsHalKeymasterV3_0TargetTest
- Hikey960 AOSP Pie (v9 r30) stable build with v3.12.0 based OP-TEE
  - No regressions
- Hikey620 EOL - support removed from upstream AOSP
- Keymaster v3 HAL, Gatekeeper v1 HAL
  - Security advisories: https://github.com/linaro-swg/kmgk/security/advisories
- FBE support requires platform specific changes
  - https://connect.linaro.org/resources/san19/san19-226
  - some info outdated but overall concept still hold

AOSP and Keymaster

Testing Strategy

- xtest
- VtsHalKeymasterV3_0TargetTest, VtsHalGatekeeperV1_0TargetTest
- KMGK_gtest (min secs between ops or max uses per boot per key generated)
- Linaro CI and testing

Wish List

- Update stable build to use master
- GKI support for OP-TEE driver
- Community support and patches welcome

DRM - OEMCrypto Library (Widevine DRM)

- Studios and content creators want to protect their content and that is typically achieved by using a DRM solution. Google created Widevine which consists of a specification and library defining and implementing a DRM solution. This also goes under the name OEMCrypto.
- We have implemented an OEMCrypto Trusted Application and supporting libraries to be able to run Widevine with OP-TEE for OEMCrypto v15.2.
- The solution has been deployed on member devices and in addition to that it's possible to run the solution in QEMU (Armv7-A as well as Armv8-A), which
  - Enables a good and efficient development environment.
  - Development and testing turnaround time is short and debuggers like GDB are very stable.
- Widevine comes with the Widevine License Agreement (WLA), which disallows open sourcing the components.

OP-TEE security issues

- Security advisories page at optee.org
  - https://www.op-tee.org/security-advisories
  - We request CVE's when appropriate

- Vulnerability Reporting Process
  - The OP-TEE project as part of the TrustedFirmware.org organization is using the security incident process as described at the TrustedFirmware.org security incident page.

- How to report security issues?
  - To report an issue, please follow the process as specified here. The email address to use can be found at the Mailing Aliases page.

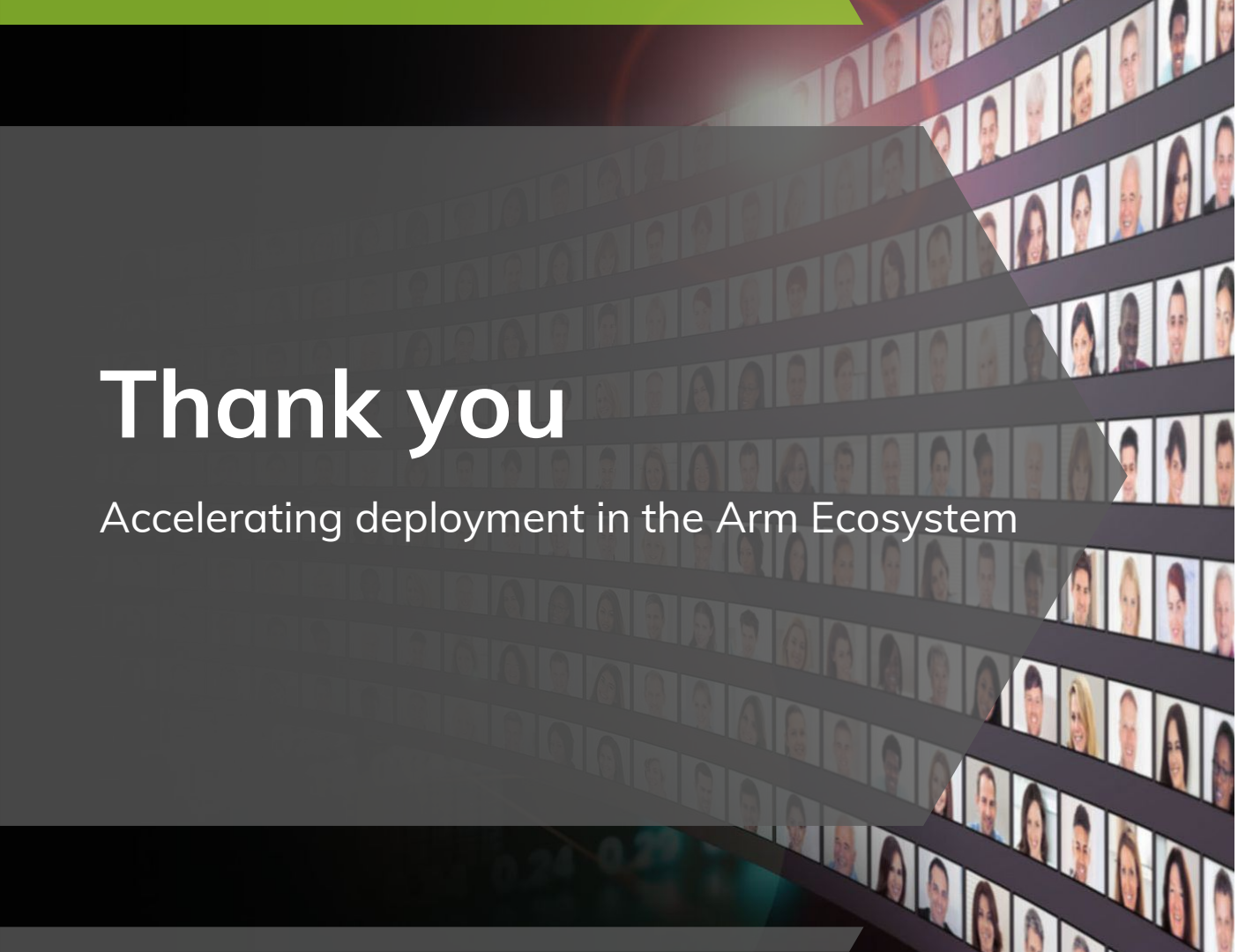
What’s next ?

- OP-TEE and Virtualization
  - Getting the experimental support available in CI on QEMU
  - FF-A mediator in Xen instead of TEE specific mediator
  - Sharing of HW resources (RPMB for storage)
  - Further work with FF-A
- Asynchronous notification to the non-secure world (pre v8.4)
- OP-TEE and Functional Safety Compliance

Contributions and ideas are welcome!

Other Security Sessions

- LVC21-118 ASLR in OP-TEE
  Tues 23/3, 7:00pm UTC
- LVC21-215 PKCS#11 in OP-TEE
  Wed 24/3, 11:30am UTC
- LVC21-305 OP-TEE as a Secure Partition running on SPM using ARMv8.4-A SEL2 feature
  Thurs 25/3, 12:45pm UTC
- LVC21-307 PSA-FF-A compliant Secure User Mode partition support for Arm platforms
  Thurs 25/3, 1:15pm UTC
- LVC21-312 Secure Partition Management in OP-TEE (pre 8.4 Cortex-A devices)
  Thurs 25/3, 1:45pm UTC



Thank you

Accelerating deployment in the Arm Ecosystem

Linaro Connect
VIRTUAL • SPRING 2021