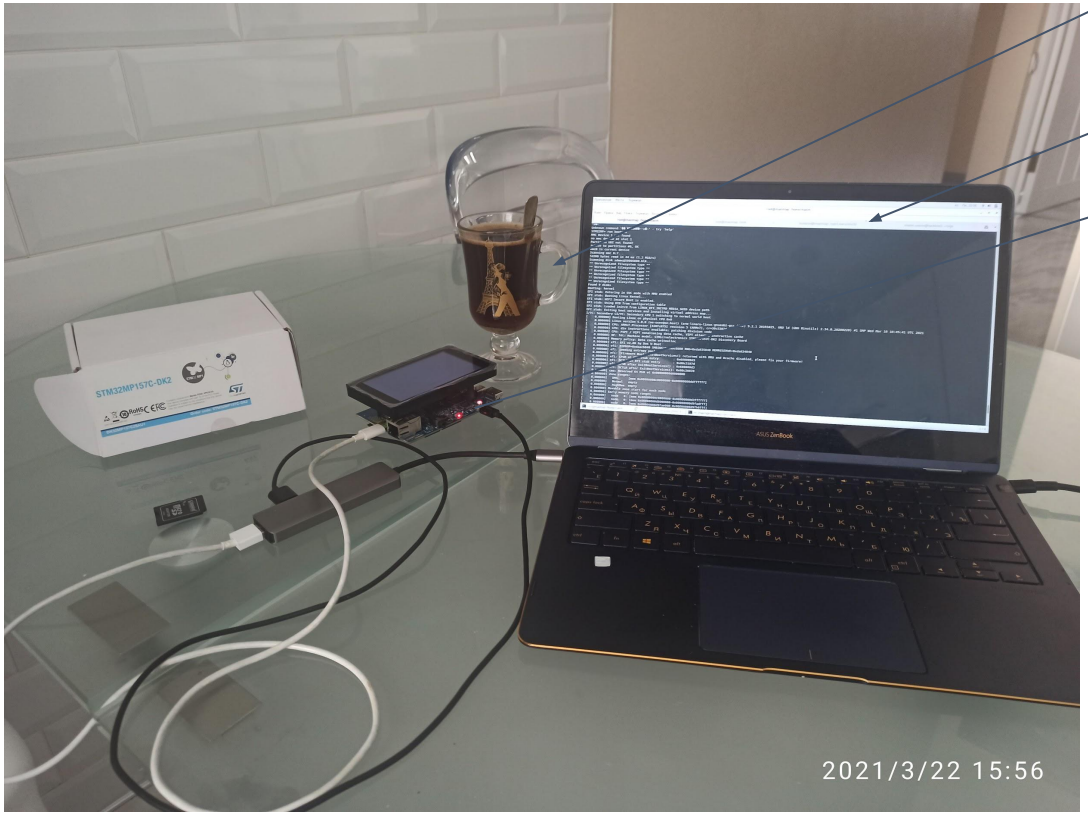
LVC21-216: UEFI Secure Boot of LEDGE RP on STM32MP1, KEK provisioning and direct booting of Linux

Maxim Uvarov <maxim.uvarov@linaro.org>

Linaro Connect
VIRTUAL • SPRING 2021

STM32MP1 and LEDGE RP



Coffee

Console

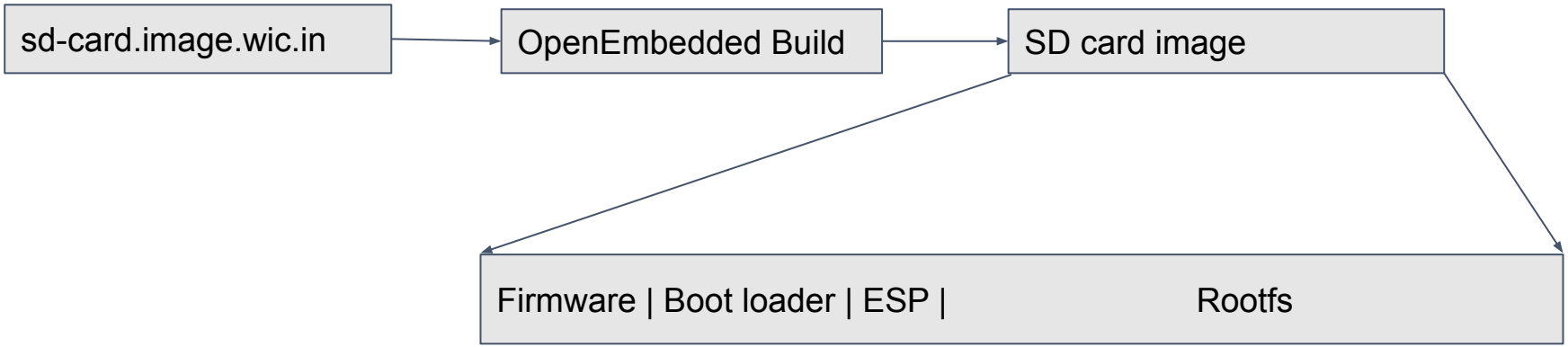
STM32MP157DC-DK2

Dual Arm® Cortex®-A7 core running up to 800 MHz and Cortex®-M4 at 209 MHz combined with a dedicated 3D graphics processing unit (GPU) and MIPI-DSI display interface and a CAN FD interface.

STM32MP1 and LEDGE RP (Continued …)

LEDGE RP - Linaro's LEDGE Reference Platform is considered to be a reference platform supporting industry standards for Linux operating system. Primary purpose is to build an operating system for IoT and EDGE devices observing specifications like UEFI, Secure Boot, EBBR, ACPI and etc.

OpenEmbedded WIC images



WIC Image

Ledge-stm32mp157c-dk2-optee.wks.in :

```
# short-description: Create SD card image with a boot partition
# long-description: Creates a partitioned SD card image
#
#  - ----- -------- ------------- ----------------------------------------------------
# | | TFA | u-boot  | teeh | teed | teex |    bootfs   |    rootfs                  |
#  - ----- -------- ------------- ----------------------------------------------------
# ^ ^    ^       ^     ^     ^     ^          ^                          ^
# | |    |       |     |     |     |          |                          |
# 0 17kB 529kB    2.5MB   2.8MB  3MB    3.3MB       67.3MiB
#
# Warning: the first stage of boot (here fsbl1, fsbl2, ssbl) MUST be on GPT partition to
be detected.
#
```

WIC Image continue..

bootloader --ptable gpt

part fsbl1 --source rawcopy --fstype=ext4 --fsoptions "noauto" --part-name=fsbl1 --sourceparams="file=${DEPLOY_DIR_IMAGE}/arm-trusted-firmware/tf-a-stm32mp157c-dk2.stm32" --ondisk mmcblk --part-type 0x8301 --fixed-size 256K --align 17

part fsbl2 --source rawcopy --fstype=ext4 --fsoptions "noauto" --part-name=fsbl2 --sourceparams="file=${DEPLOY_DIR_IMAGE}/arm-trusted-firmware/tf-a-stm32mp157c-dk2.stm32" --ondisk mmcblk --part-type 0x8301 --fixed-size 256K

part ssbl --source rawcopy --fstype=ext4 --fsoptions "noauto" --part-name=ssbl --sourceparams="file=${DEPLOY_DIR_IMAGE}/u-boot-trusted.stm32" --ondisk mmcblk --part-type 0x8301 --fixed-size 2048K

part teeh --source rawcopy --fstype=ext4 --fsoptions "noauto" --part-name=teeh --sourceparams="file=${DEPLOY_DIR_IMAGE}/optee/tee-header_v2.stm32" --ondisk mmcblk --part-type 0x8301 --fixed-size 256K

part teed --source rawcopy --fstype=ext4 --fsoptions "noauto" --part-name=teed --sourceparams="file=${DEPLOY_DIR_IMAGE}/optee/tee-pageable_v2.stm32" --ondisk mmcblk --part-type 0x8301 --fixed-size 256K

WIC Image continue..

part teex --source rawcopy --fstype=ext4 --fsoptions "noauto" --part-name=teex --sourceparams="file=${DEPLOY_DIR_IMAGE}/optee/tee-pager_v2.stm32" --ondisk mmcblk --part-type 0x8301 --fixed-size 256K

part /boot --source bootimg-efi --sourceparams="loader=kernel" --fstype=vfat --part-type 0xef00 --label bootfs --align 4 --use-uuid --include-path "${DEPLOY_DIR_IMAGE}/dtb ${DEPLOY_DIR_IMAGE}/ledge-initramfs.rootfs.cpio.gz" --fixed-size 64M

part / --source rootfs --fstype=ext4 --label rootfs --align 4 --fsuuid 6091b3a4-ce08-3020-93a6-f755a22ef03b --exclude-path boot/

Get image and flash

wget
http://snapshots.linaro.org/components/ledge/oe/ledge-stm32mp157c-dk2/901/rpb/ledge-iot-ledge-stm32mp157c-dk2-20210321230908.rootfs.wic.bin.gz

zcat ledge-iot-*.rootfs.wic.bin.gz > /dev/sda (sda is an SD card).

wget
http://snapshots.linaro.org/components/ledge/oe/ledge-stm32mp157c-dk2/901/rpb/ledge-kernel-uefi-certs.ext4.img

Put: KEK.auth kernel.auth PK.auth to ESP partition (sda7 for above WIC image)

Poweron and set up SecureBoot

```
load mmc 0:7 ${kernel_addr_r} kernel.auth
setenv -e -nv -bs -rt -at -i ${kernel_addr_r}:$filesize db

load mmc 0:7 ${kernel_addr_r} KEK.auth
setenv -e -nv -bs -rt -at -i ${kernel_addr_r}:$filesize KEK

load mmc 0:7 ${kernel_addr_r} PK.auth
setenv -e -nv -bs -rt -at -i ${kernel_addr_r}:$filesize PK

efidebug boot add 0000 'kernel' mmc 0:7 /efi/boot/bootarm.efi
efidebug boot order 0000
bootefi bootmgr
```

Output from the board

```
STM32MP> load mmc 0:7 ${kernel_addr_r} kernel.auth
1294 bytes read in 35 ms (35.2 KiB/s)
STM32MP> setenv -e -nv -bs -rt -at -i ${kernel_addr_r}:$filesize db
STM32MP> load mmc 0:7 ${kernel_addr_r} KEK.auth
2299 bytes read in 35 ms (63.5 KiB/s)
STM32MP> setenv -e -nv -bs -rt -at -i ${kernel_addr_r}:$filesize KEK
STM32MP> load mmc 0:7 ${kernel_addr_r} PK.auth
2299 bytes read in 35 ms (63.5 KiB/s)
STM32MP> setenv -e -nv -bs -rt -at -i ${kernel_addr_r}:$filesize PK
STM32MP> efidebug boot add 0000 'kernel' mmc 0:7 /efi/boot/bootarm.efi
STM32MP> efidebug boot order 0000
STM32MP> bootefi bootmgr
```

Output from the board (Continued...)

STM32MP> bootefi bootmgr

ETZPC: 0x5a003000 node disabled, decprot 10=0

Booting: kernel

EFI stub: Entering in SVC mode with MMU enabled

EFI stub: Booting Linux Kernel...

EFI stub: UEFI Secure Boot is enabled.

EFI stub: Using DTB from configuration table

EFI stub: Loaded initrd from LINUX_EFI_INITRD_MEDIA_GUID device path

EFI stub: Exiting boot services and installing virtual address map...

I/TC: Secondary CI/TC: Secondary CPU 1 switching to normal world boot

[0.000000] Booting Linux on physical CPU 0x0

[0.000000] Linux version 5.8.0 (oe-user@oe-host) (arm-linaro-linux-gnueabi-gcc (GCC) 9.2.1 20191025, GNU ld (GNU Binutils) 2.34.0.20200220) #1 SMP Wed Mar 10 10:45:41 UTC 2021

[0.000000] CPU: ARMv7 Processor [410fc075] revision 5 (ARMv7), cr=30c5387d

Check in userland

ledge-stm32mp157c-dk2:~$ efivar -l

8be4df61-93ca-11d2-aa0d-00e098032b8c-BootCurrent

8be4df61-93ca-11d2-aa0d-00e098032b8c-SignatureSupport

8be4df61-93ca-11d2-aa0d-00e098032b8c-OsIndicationsSupported

8be4df61-93ca-11d2-aa0d-00e098032b8c-PlatformLangCodes

8be4df61-93ca-11d2-aa0d-00e098032b8c-VendorKeys

8be4df61-93ca-11d2-aa0d-00e098032b8c-DeployedMode

8be4df61-93ca-11d2-aa0d-00e098032b8c-AuditMode

8be4df61-93ca-11d2-aa0d-00e098032b8c-SetupMode

8be4df61-93ca-11d2-aa0d-00e098032b8c-**SecureBoot**

8be4df61-93ca-11d2-aa0d-00e098032b8c-BootOrder

8be4df61-93ca-11d2-aa0d-00e098032b8c-Boot0000

8be4df61-93ca-11d2-aa0d-00e098032b8c-PK

8be4df61-93ca-11d2-aa0d-00e098032b8c-KEK

d719b2cb-3d3a-4596-a3bc-dad00e67656f-db

8be4df61-93ca-11d2-aa0d-00e098032b8c-PlatformLang

Check in userland (Continued …)

ledge-stm32mp157c-dk2:~$ efivar -p -n 8be4df61-93ca-11d2-aa0d-00e098032b8c-SecureBoot

GUID: 8be4df61-93ca-11d2-aa0d-00e098032b8c

Name: "SecureBoot"

Attributes:

Boot Service Access

Runtime Service Access

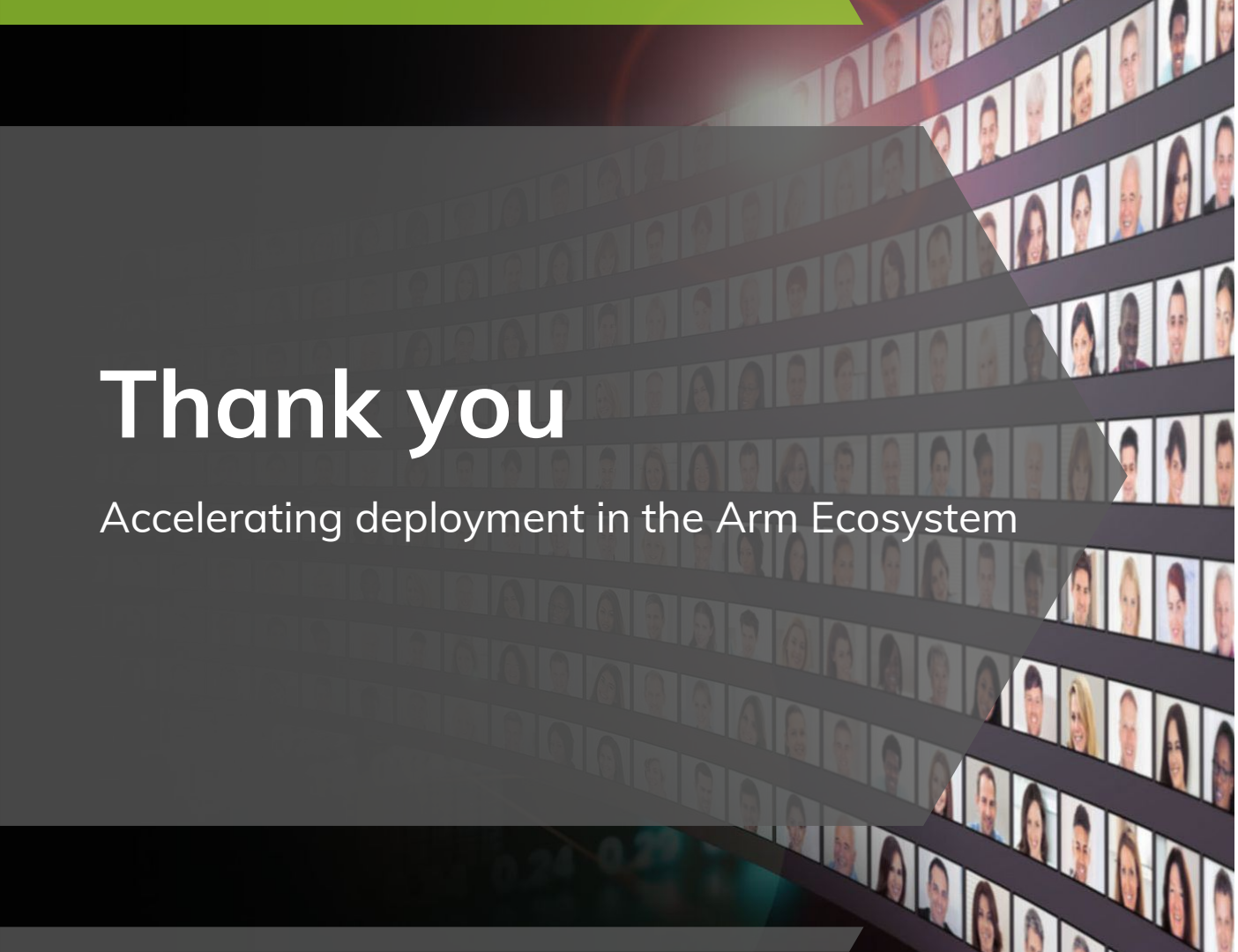
Value:

00000000 **01**

What if kernel is not signed?

....
Scanning disk sdmmc@58005000.blk...
Found 9 disks
Image not authenticated
Loading Boot0000 'kernel' failed
EFI boot manager: Cannot load any image
Found EFI removable media binary efi/boot/bootarm.efi
11612672 bytes read in 526 ms (21.1 MiB/s)
Booting /efi\boot\bootarm.efi
Image not authenticated
Loading image failed
EFI LOAD FAILED: continuing...

Screen Share and live demo!



Thank you

Accelerating deployment in the Arm Ecosystem

Linaro Connect
VIRTUAL • SPRING 2021