Manuel Traut
manuel.traut@mt.com
@manut@mountains.social

Booting an Embedded System Like a PC

All Systems Go!, Berlin, DE, September 25-26 2024

METTLER TOLEDO

ALL SYSTEMS GO!

Embedded Linux Developer, METTLER TOLEDO

- Concept of our Debian based Embedded Linux distribution
- GitLab CI Pipelines
- Member of our Open Source Focus Group

Laboratory Weighing

Laboratory Balances, Analytical, Precision and Micro & Ultra Micro Balances, Powder & Liquid Dosing, Moisture Analyzers, Test Weights

Industrial Weighing Scales and Systems

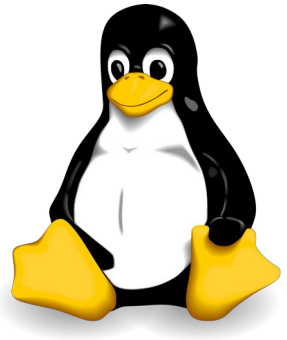
Bench Scales, Portable Scales, Floor Scales, Counting and Mixing Scales, Terminals, Weigh Modules, Load Cells, SQC, Software

Debian User and Contributor

- User since 2006, contributor since 2022
- Package maintainer of libusbgx
  This library is used in some of our scales
- Package maintainer of cozy (audiobook player)
  Using it on my PinePhone running Mobian
- Toradex Colibri i.MX6DL Evalboard support in u-boot
  It is used for our demos and for integrationtests
- Speaker at Debconf22
  Build Debian based Embedded Images in the Cloud

Linux Kernel

- User since ~2000
- Sporadic contributor since 2019
- Mainlained PineTab2 Devicetree in 6.9
- Some oneliners



Agenda

1	Motivation
2	System Architecture
3	Firmware
4	Operating System
5	Conclusion
6	
7	
8	
9	

Further Improve Security of our Debian based Embedded Linux Platform

- **Protect** our intellectual property
- Only allow **trusted devices** to access cloud services
- Install trusted software **upgrades** (avoid downgrades)
- Allow users to exchange / add software on an **unlocked device**

Similar Requirements are True and Solved for PCs

- ~~Protect our intellectual property~~ Protect users private data

LUKS
Linux Unified Key Setup

- Only allow trusted ~~**devices**~~ **users** to access cloud services

OpenSSL TPM-2 backend, PCR sealing

- Install trusted software upgrades ~~(avoid downgrades)~~

[● ◀] **systemd** - sysupdate from signed source, dm-verity

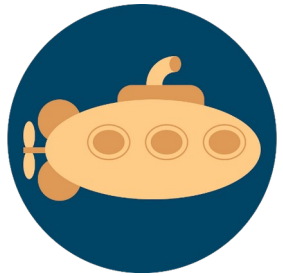
- Allow users to exchange / add software on an unlocked device

SecureBoot (TM)

Most Relevant Differences

...Booting!

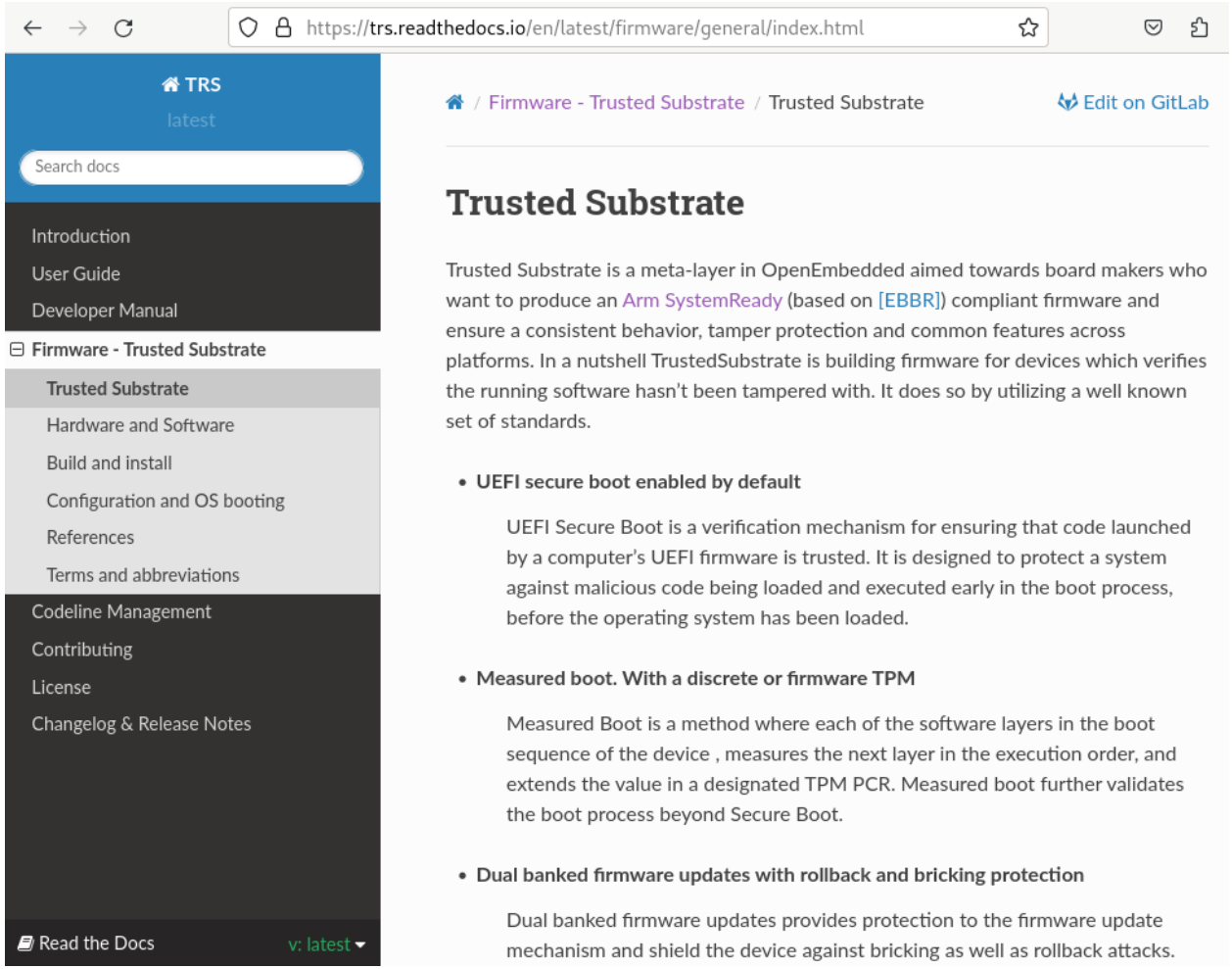
- Our devices boot with “Das U-Boot” / distroboot



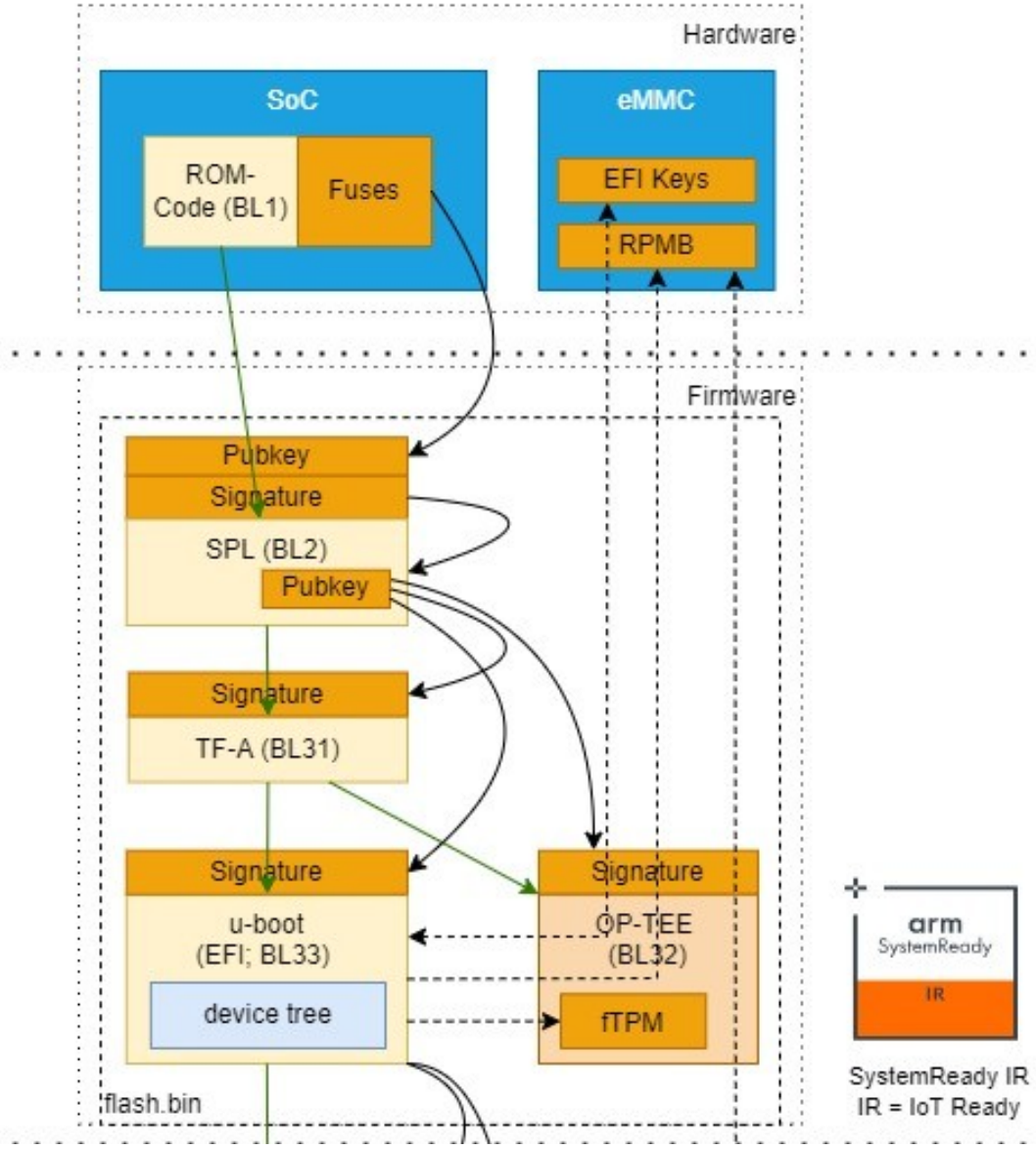
- A PC boots with UEFI and includes a TPM 2.0

System Architecture

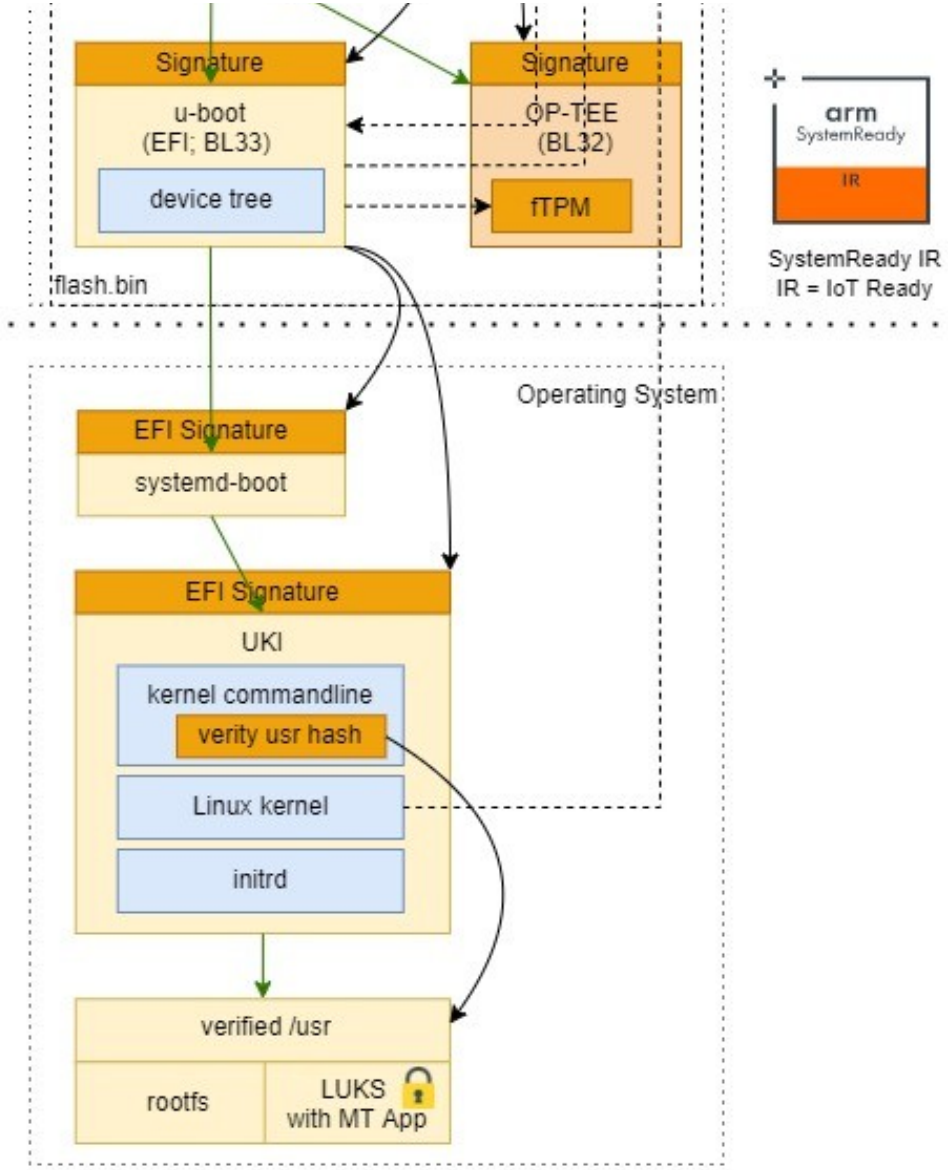
- All needed components to implement UEFI Boot with a TPM2.0 in firmware are available e.g.for Freescale i.MX8MM SoC
- It is “just” an **integration task**
- “**arm SystemReady IR**” is a specification that describes booting via EFI with TPM support
- **Linaro Trusted Substrate Firmware**
  Implements this for different platforms
  - Documentation is available here: https://trs.readthedocs.io/



System Architecture

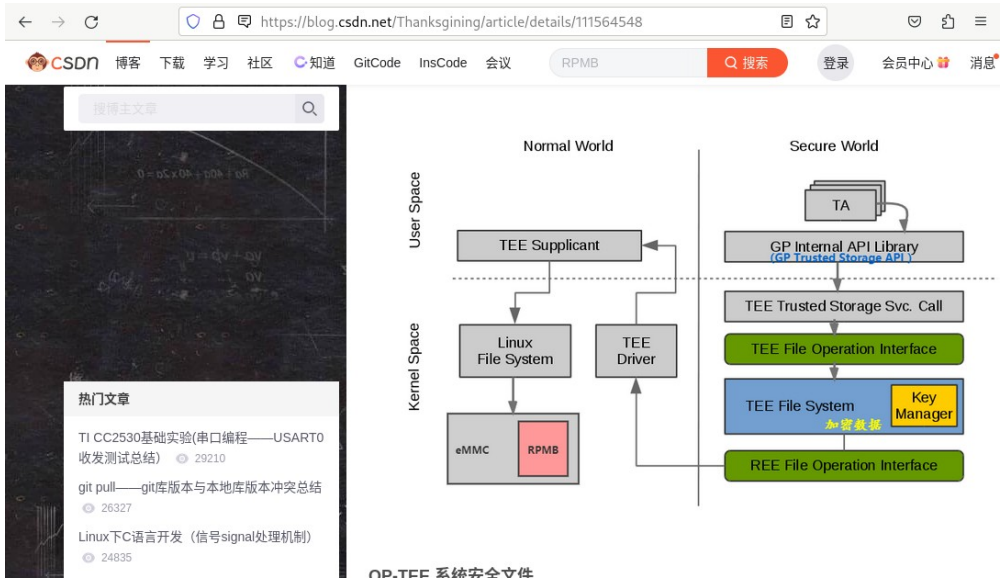


System Architecture



OP-TEE

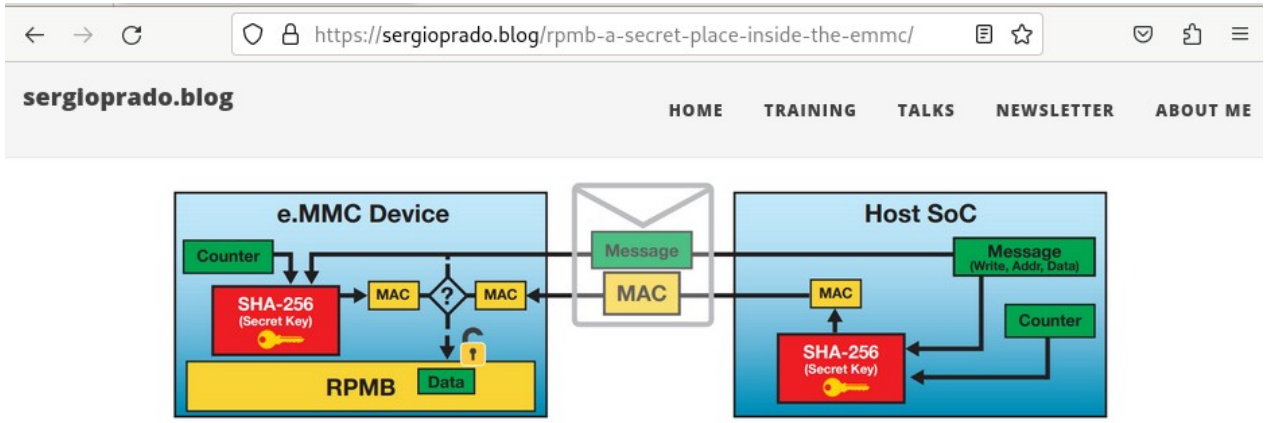
- **fTPM** sample application as OP-TEE Early TA (compiled-in)
  - fTPM **driver** is in **mainline** U-Boot and mainline Linux
  - From a user perspective no difference to a hardware TPM
  - OP-TEE OS, PR for fTPM as TA from Jens Wiklander
    https://github.com/OP-TEE/optee_os/pull/7054



- Non-volatile Storage for fTPM is the **RPMB** block of the **eMMC**
  - eMMC is not available in ARM TrustZone
  - OP-TEE calls non-secure world to handle RPMB requests
  - U-Boot includes code to handle this RPMB requests
  - Linux will have an RPMB subsystem (merged for 6.12):
    https://lore.kernel.org/lkml/20240814153558.708365-1-jens.wiklander@linaro.org/
  - Currently tee-supplicant needs to do this in userspace

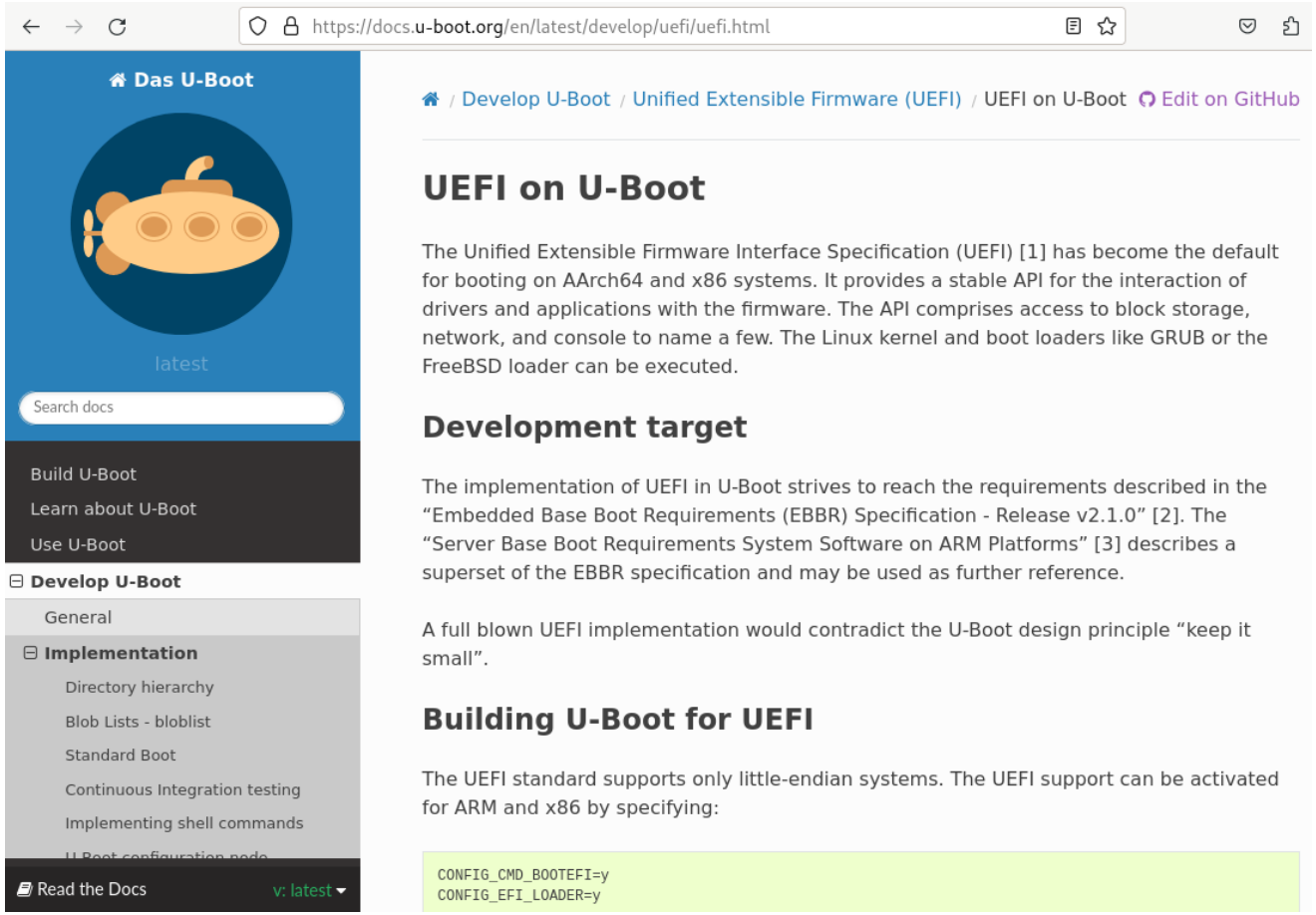
RPMB Key

- RPMB Key is a **Symmetric Key**
  that is needed to write to the eMMC RPMB block
- RPMB Key can be configured/written to the eMMC only once
- **Key shall not be compiled into software**
  to avoid extracting/reverse engineering it
- On i.MX8 the RPMB Key can be **derived**
  from an i.MX **Uniq-Device-Id** that is only readable in TrustZone



Das U-Boot

- **EFI** support is mainline
- **SecureBoot** support is mainline
  - EFI variables are stored in OP-TEE
  - EDK II StandAloneMM is linked to OP-TEE
- EFI **Capsule Upgrade** support is mainline
- **Documentation** is excellent
  https://docs.u-boot.org/en/latest/develop/uefi/uefi.html



Use systemd and mkosi

- Use TPM 2.0 PCR measurements to verify system integrity
  systemd-pcrlock
- Deploy LUKS Key to TPM
  systemd-cryptenroll, systemd-cryptsetup
- Manage credentials used by services
  systemd-creds
- Build and sign OS images with dm-verity and UKIs
  mkosi
- Applying A/B OS upgrades generated by mkosi
  systemd-sysupdate, systemd-boot, bootctl
- Creating / resizing partitions by deploying an OS update
  systemd-repart

Review of Requirements

We are able to...

- ✔ **Protect IP**
  Stored in LUKS volumes backed by TPM
  LUKS key sealed to PCR of SecureBootMode
- ✔ **Protect certificates** used for authentication
  stored in TPM, sealed to PCR of SecureBootMode
- ✔ Deploy **OS upgrades**
  File based verification before deployment is missing
- ✔ **Boot latest OS**
  Bootcounting/fallback is missing
- ✔ Boot **verified operating systems** only
  with EFI SecureBoot enabled
- ✔ **Unlock devices**
  by deploying new EFI Keys

And there are Even More Benefits...

- ✔ The same OS Image boots on **many devices**
- ✔ Install **any Linux distribution**

systemd-sysupgrade

```
root@iris:~# /lib/systemd/systemd-sysupdate list
Automatically discovered root block device '/dev/mmcblk1'.
Automatically discovered root block device '/dev/mmcblk1'.
Discovering installed instances…
Discovering available instances…
Determining installed update sets…
Determining available update sets…
  VERSION INSTALLED AVAILABLE
ASSESSMENT
● 1.1          ✓
current
root@iris:~# /lib/systemd/systemd-sysupdate check-new
```

Demo

Fedora Installer

```
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
Verdin iMX8MM #
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.8 | VT102 | Offline | ttyUSB4
```

Open Topics & Next Steps

- File based signature verification in systemd-sysupdate *or* systemd-boot bootcount logic implementation in RAUC
- Implement FAT “move” in U-Boot (needed by systemd-boot bootcounter)
- Learn from **Enterprise Linux admins**
  How to
  - Provision new systems?
  - Deploy, update/revoke keys and certificates?
- How to **maintain** the firmware components?
  - SBOM
  - Security Tracking
  - Updates
- Try EFI Capsule Upgrade
- Use efifb for bootlogo, plymouth

Contributions

- **RPMB Kernel Patches** “Tested-by”
  - RPMB data was not page-aligned
    (Problems with SDHCI controller, DMA, ..)
- **systemd-sysupdate**
  - Report MatchPattern assumption to user
- **mkosi** bugreport
  - ‘login’ is no longer essential in Debian

    This needed to be mentioned in documentation

Backlog

- **USB Gadget** support in **u-boot/SPL** for CI UDC Controller
- Minor patches here and there...

Conclusion

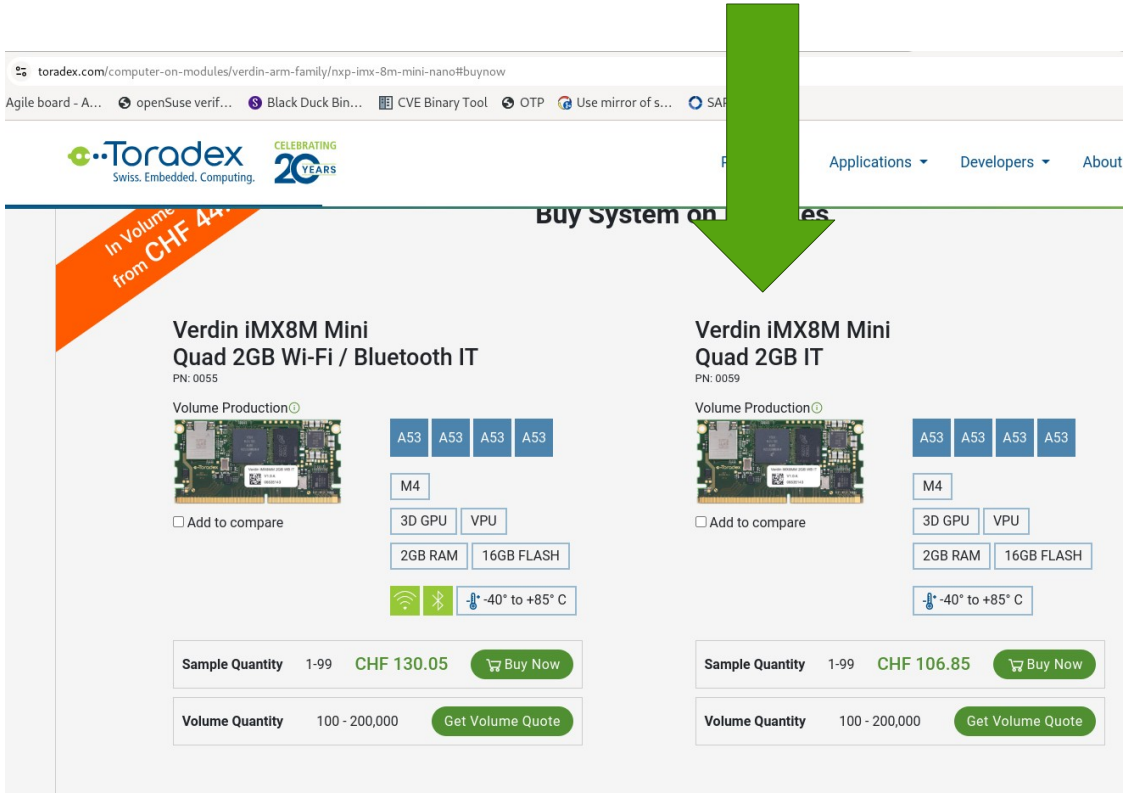
- **All needed software components are available**
- **Integration is not an easy task**
  - If something does not work,
    the complete stack needs to be understood
- Well established **tooling** can be used
- Well **specified and established interface** between firmware and operating system
  - The **operating system** and upgrade implementation is **not device specific**

To Rebuild the Demos

- **Hardware**
  - https://www.toradex.com/products/carrier-board/verdin-development-board-kit
  - https://www.toradex.com/computer-on-modules/verdin-arm-family/nxp-imx-8m-mini-nano#buynow

- **Software**
  - **Build the firmware**
    https://github.com/mt-at-mt/build-efi-firmware

    '`./build.sh`' clones all needed repos and builds the firmware
  - **Fedora Installer** (dd'ed to an SDCard)
    https://dl.fedoraproject.org/pub/archive/fedora/linux/releases/38/Server/aarch64/iso/Fedora-Server-netinst-aarch64-38-1.6.iso
  - **OS Image for the systemd-sysupgrade Demo**
    https://github.com/mt-at-mt/os-image



Thanks

- **All Systems Go!** For organizing this event and for the invitation
- **So many people, projects and communities made this a success**, especially:
  - **systemd, mkosi**
    I do not want to think about implementing all these things in shell scripts
  - **OP-TEE**
    Jens Wiklander, Developed and integrated the RPMB subsystem into Linux
  - **Debian**
    Providing stable and secure binary packages we rely on
  - David and Richard of **sigma star GmbH**
    Concept Review, help with the CAAM
- **METTLER TOLEDO**
  - For sponsoring my visit of this years All Systems Go! conference
  - Burak Gerz for the systemd-sysupdate evaluation and testing
  - Tobias Graemer for documentation and graphics

We are Hiring

Current Open Positions

- **Embedded Software Engineer – Linux**, Zürich / Switzerland
  Debian, systemd, u-boot, Kernel, PREEMPT_RT, ...
- **Senior DevSecOps Engineer**, Karnataka, Tamil Nadu / India
  On prem k8s, Linux, Windows, maven, Gradle, MsBuild, NuGet

Join us now: https://careers.mt.com/

One Team
Many Passions