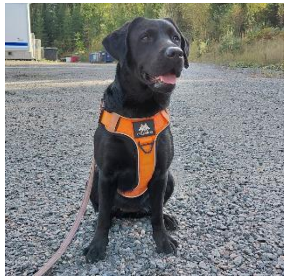
Introduction to Trusted Systems

Ian Oliver

13 November 2025

Introduction

Trust and Attestation of me….



Professor of Practice @ Oulu,
Lead Scientist @ Nokia Standards
Startup founder (medical stuff)
Works with dogs, horses and occasionally humans too

25+ years telecoms and critical system experience
200+ papers & other publications
100+ patents
1 book (some more in progress)
10th or 11th CRIM … lost count, can't remember

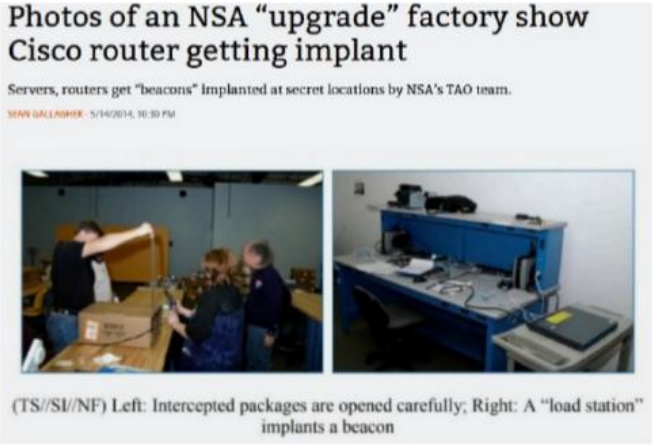
Best Seller

How the World ends

How the World ends...

Examples

Bloomberg Businessweek
The Big Hack
How China used a tiny chip to infiltrate America's top companies


Photos of an NSA “upgrade” factory show Cisco router getting implant

Servers, routers get "beacons" implanted at secret locations by NSA's TAO team.

SEAN GALLAGHER - 5/14/2014, 10:30 PM

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

Philosophy

Trust

How do we trust systems?

a) how to ensure they are WHO they claim to be?
b) how to ensure they are WHAT the claim to be?

Trust is a POSITIVE EXPECTATION regarding the BEHAVIOUR of a system

A bit of philosophy...

The trust relationship between things:

2-place trust: A trusts B
3-place trust: A trusts B to do X

Doxastic: *trust* = *believes*, A trusts B to do X => A believes B will/can/does do X
Non-doxastic: trust = A is optimistic that B will do X

Modality: deontic (obligation,permission), epistemic (knowledge)
O(A trusts B to do X) => not K(A trusts B to do X)

Proof: for A trusts B to be valid, B must prove their trust to A

A bit of philosophy...

Trustworthy systems:

- A system is trustworthy if it can provide evidence that it can be trusted.

Question: what does “trustworthy AI” mean?

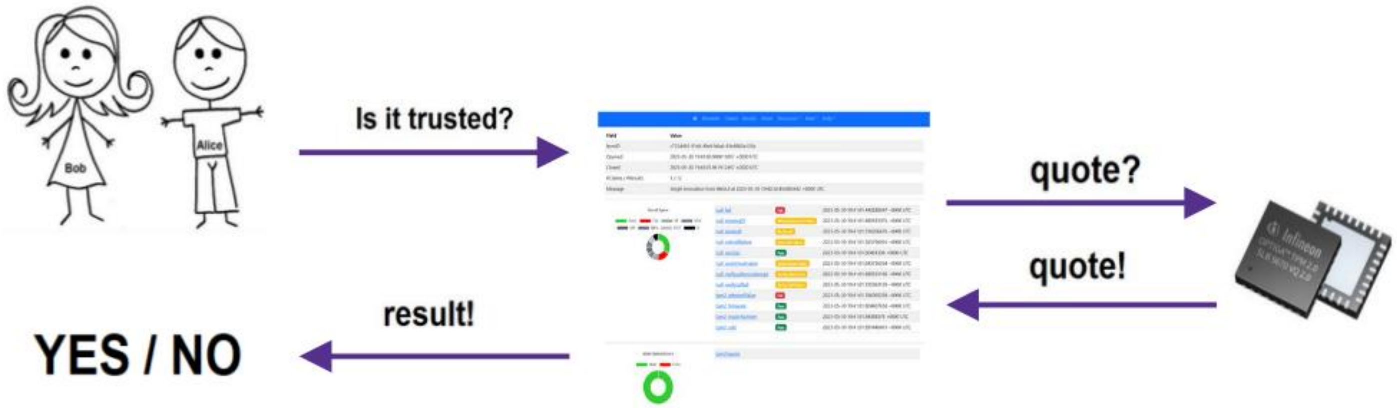
- What are the criteria for trust?

Trust $\propto$ Risk^{-1}

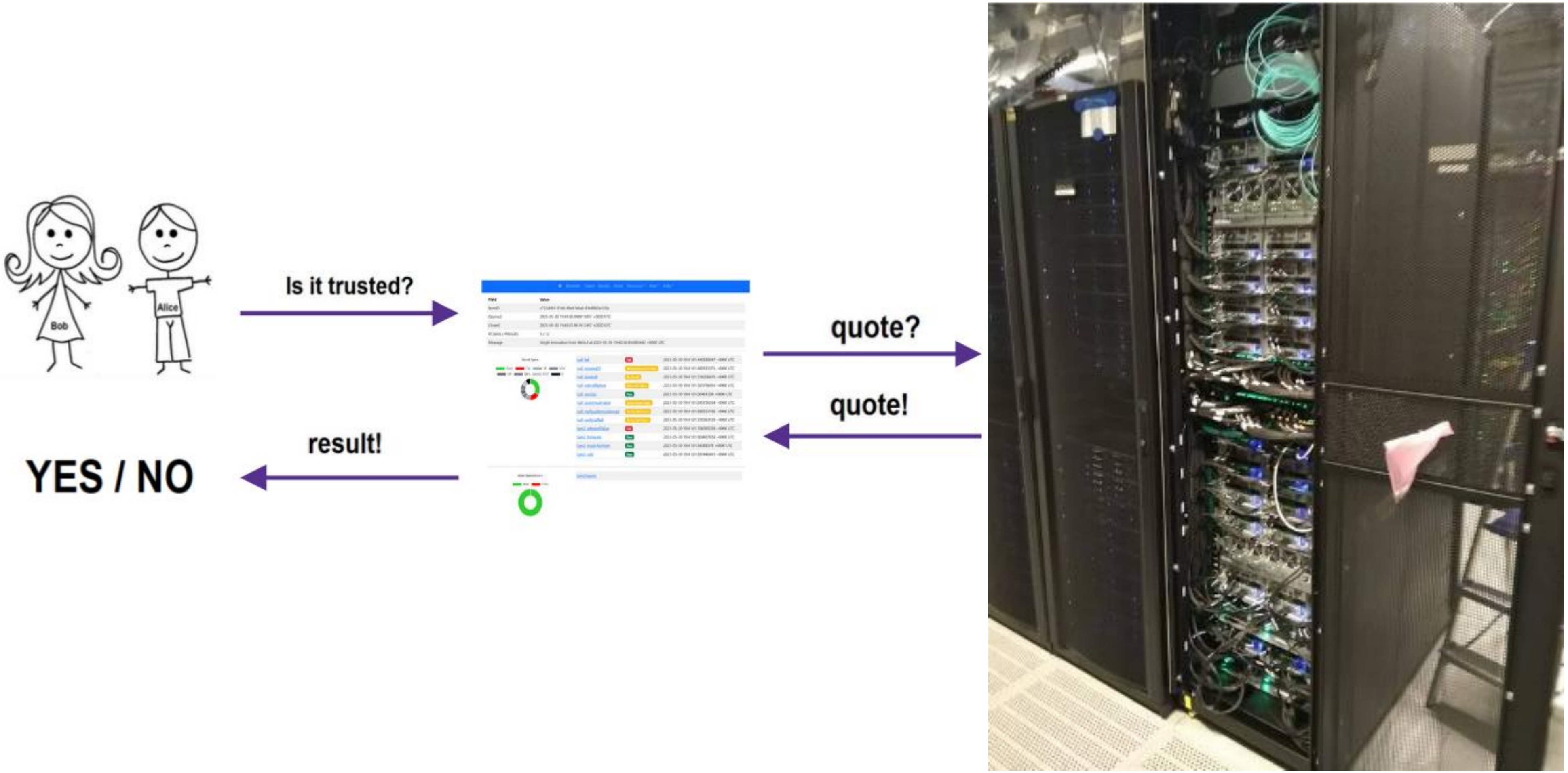
- Who takes the risk?

Establishing Trust

Attestation



Attestation



Is it trusted?

quote?

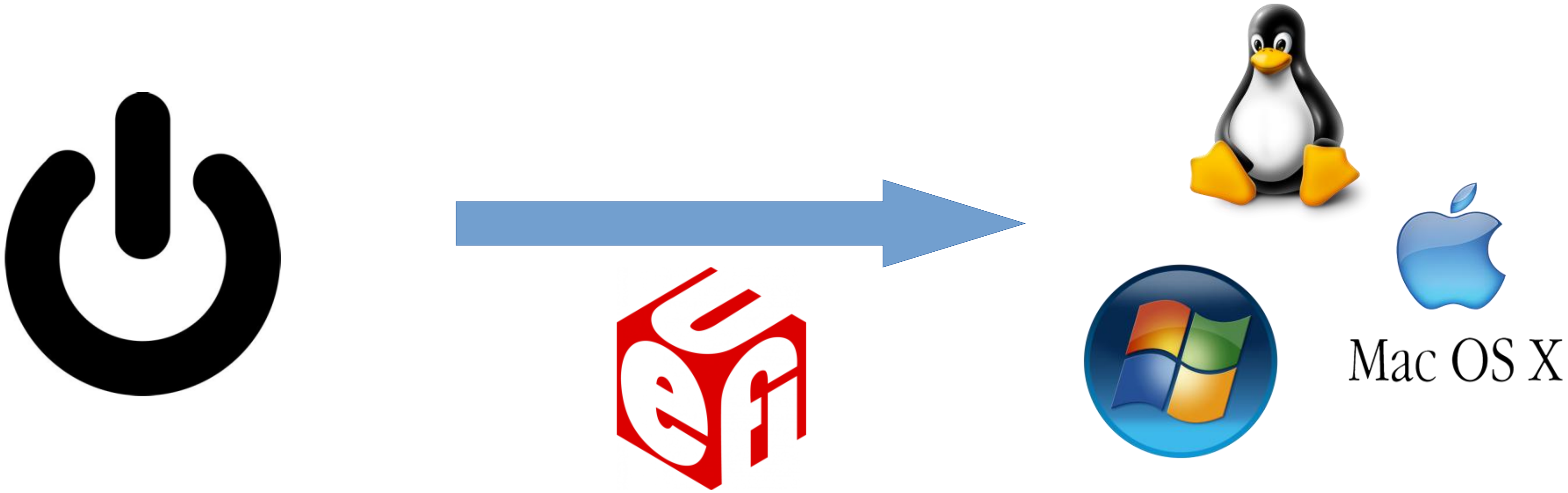
quote!

result!

YES / NO

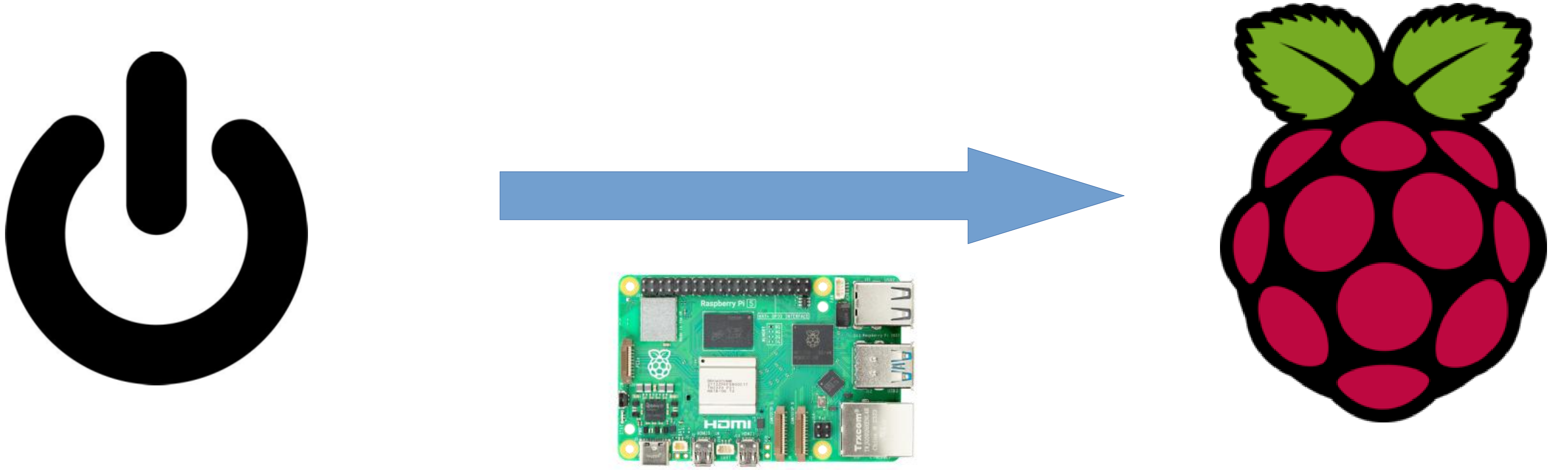
Power On

x86 -Power On



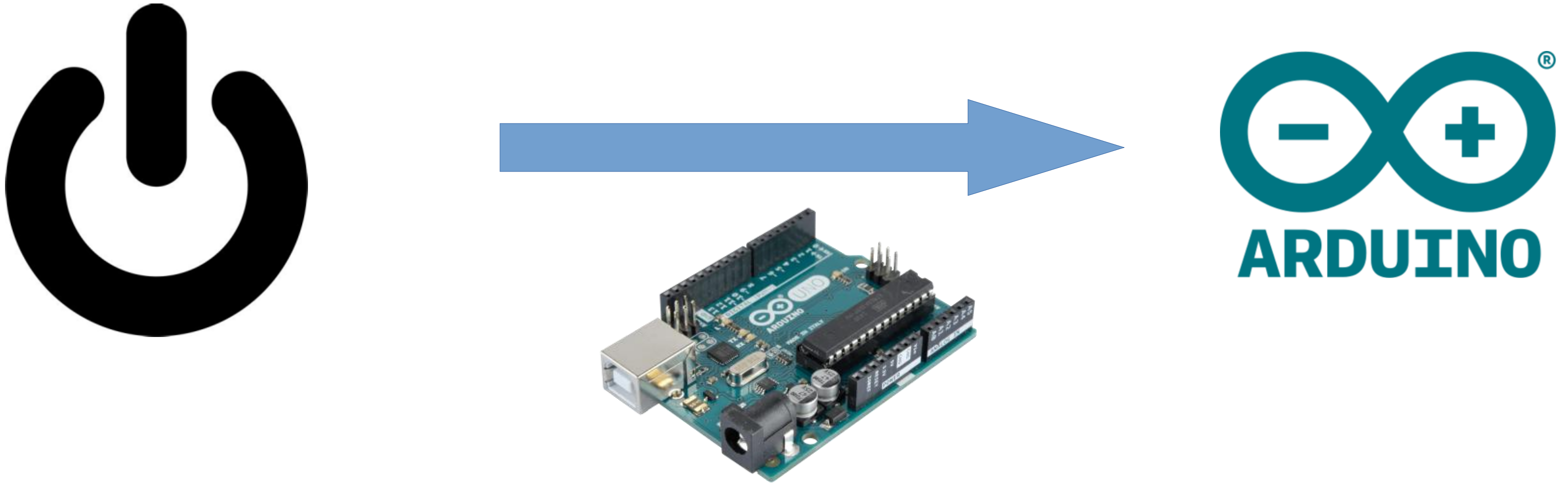
Secure Boot
Trusted Boot
Measured Boot

arm/pi - Power On



Secure Boot?
Trusted Boot?
Measured Boot?

arduino - Power On

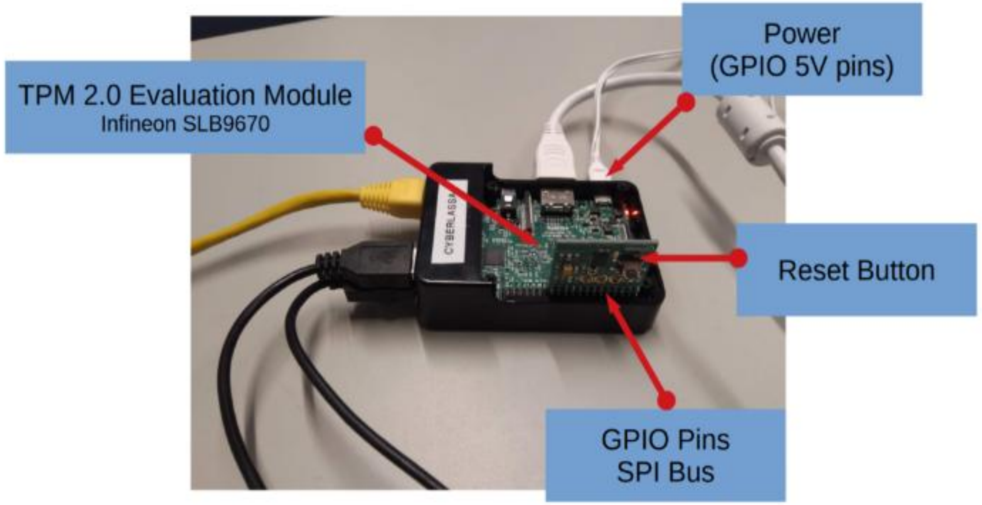


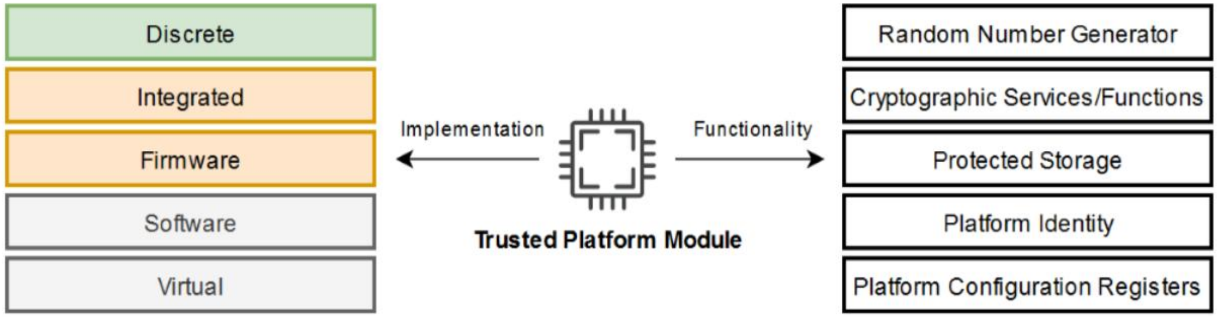
Secure Boot?
Trusted Boot?
Measured Boot?

Trusted Platform Module

THEY'RE PUTTING CHIPS IN US!
NSA
FBI
NSA/FBI/CIA MONITORING YOUR THOUGHTS!
TRUSTED PLATFORM MODULE
MIND CONTROL VIA 5G!
5G
5G

TPM

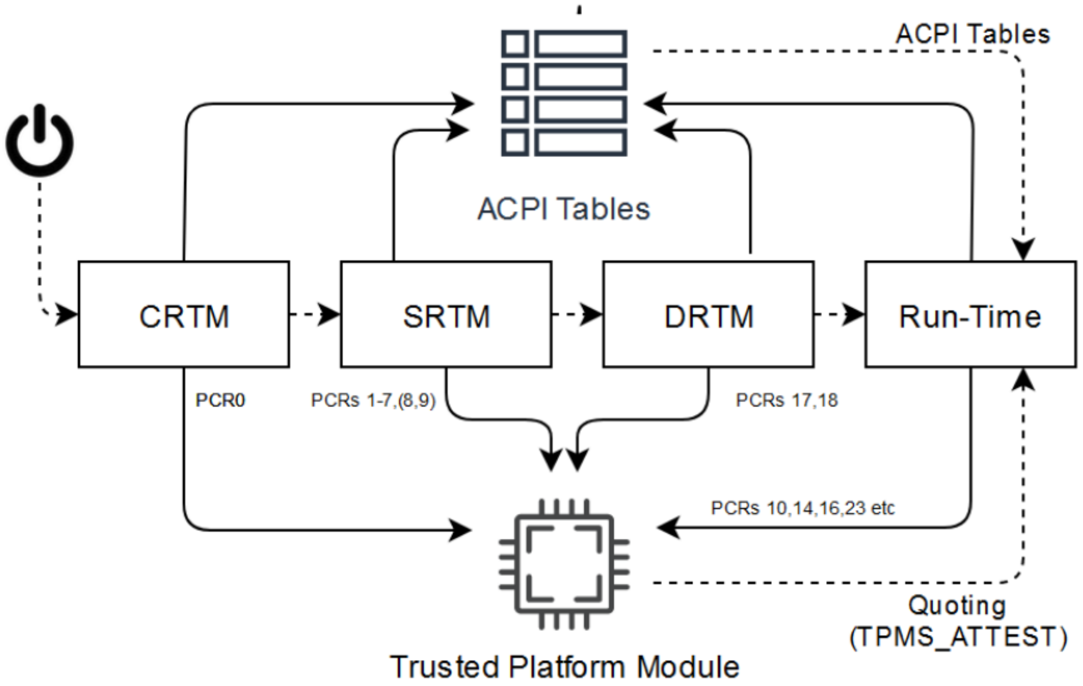




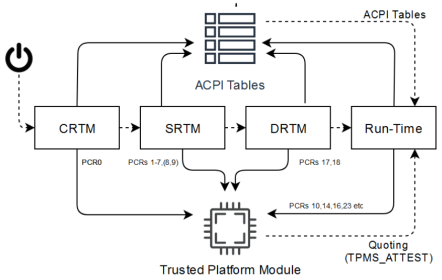
https://www.youtube.com/watch?v=S6HWK8PF5MU

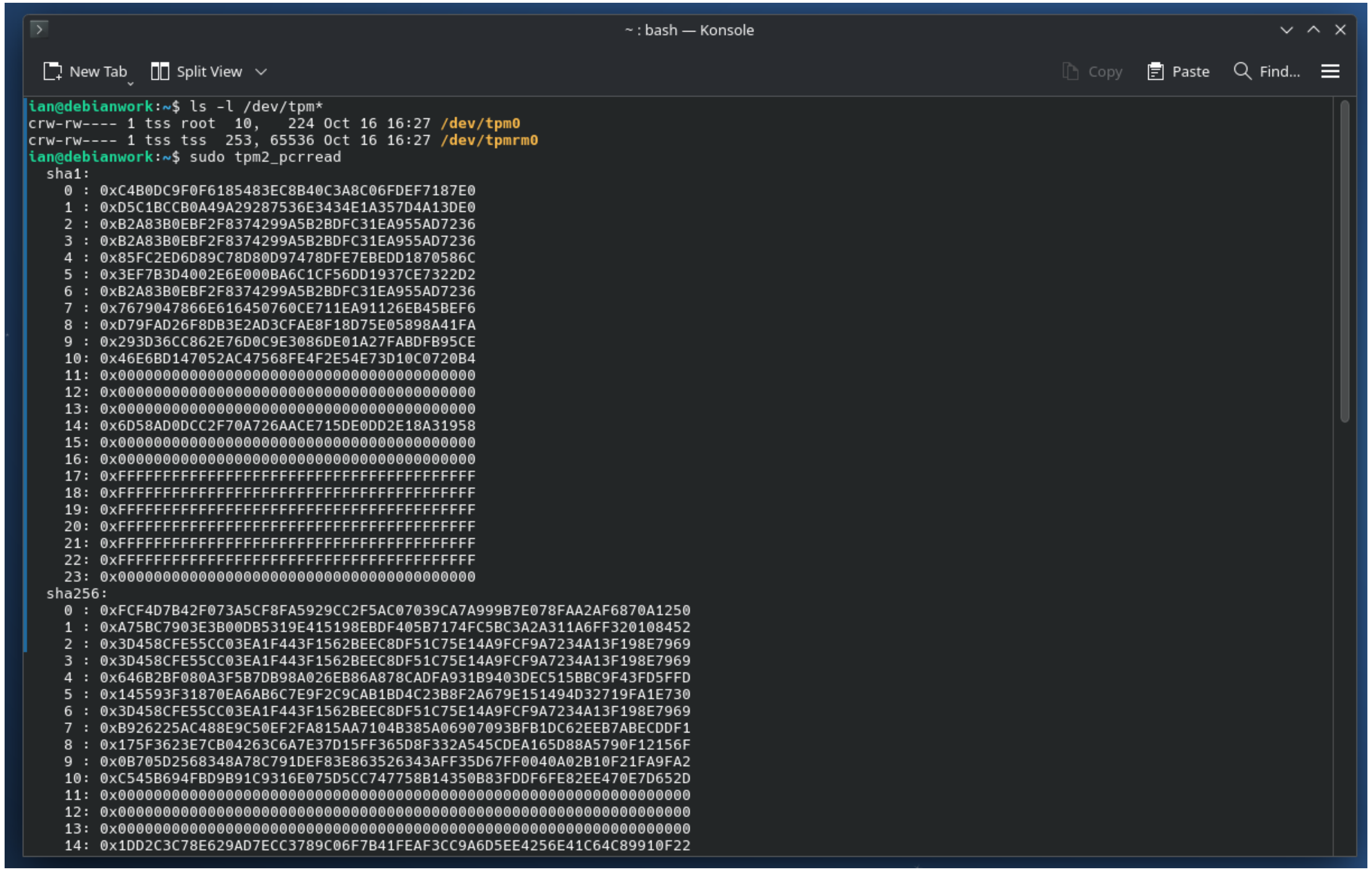
Ian Oliver, **Trusting your Raspberry Pi** – Code::Dive 2019

TPM – PC Boot Sequence



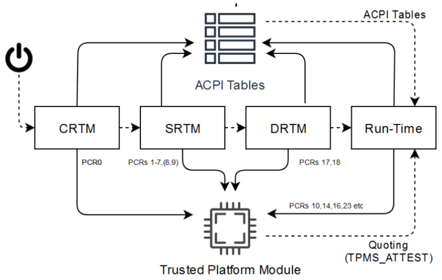
TPM - PCRs

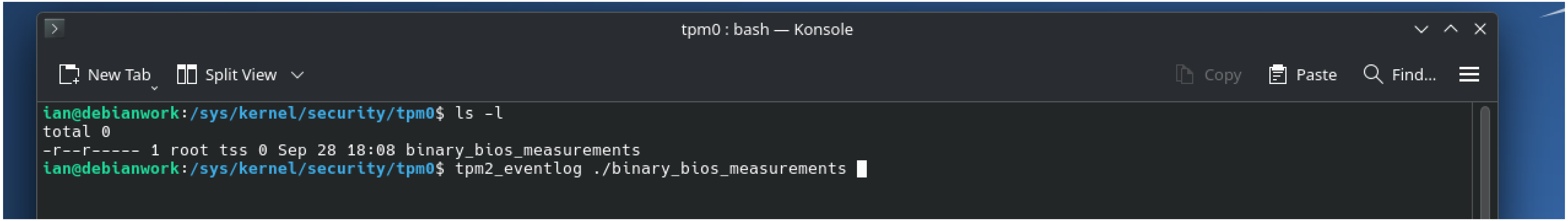




```
ian@debianwork:~$ ls -l /dev/tpm*
crw-rw---- 1 tss root  10,   224 Oct 16 16:27 /dev/tpm0
crw-rw---- 1 tss tss  253, 65536 Oct 16 16:27 /dev/tpmrm0
ian@debianwork:~$ sudo tpm2_pcrread
  sha1:
    0 : 0xC4B0DC9F0F6185483EC8B40C3A8C06FDEF7187E0
    1 : 0xD5C1BCCB0A49A29287536E3434E1A357D4A13DE0
    2 : 0xB2A83B0EBF2F8374299A5B2BDFC31EA955AD7236
    3 : 0xB2A83B0EBF2F8374299A5B2BDFC31EA955AD7236
    4 : 0x85FC2ED6D89C78D80D97478DFE7EBEDD1870586C
    5 : 0x3EF7B3D4002E6E000BA6C1CF56DD1937CE7322D2
    6 : 0xB2A83B0EBF2F8374299A5B2BDFC31EA955AD7236
    7 : 0x7679047866E616450760CE711EA91126EB45BEF6
    8 : 0xD79FAD26F8DB3E2AD3CFAE8F18D75E05898A41FA
    9 : 0x293D36CC862E76D0C9E3086DE01A27FABDFB95CE
    10: 0x46E6BD147052AC47568FE4F2E54E73D10C0720B4
    11: 0x0000000000000000000000000000000000000000
    12: 0x0000000000000000000000000000000000000000
    13: 0x0000000000000000000000000000000000000000
    14: 0x6D58AD0DCC2F70A726AACE715DE0DD2E18A31958
    15: 0x0000000000000000000000000000000000000000
    16: 0x0000000000000000000000000000000000000000
    17: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
    18: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
    19: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
    20: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
    21: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
    22: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
    23: 0x0000000000000000000000000000000000000000
  sha256:
    0 : 0xFCF4D7B42F073A5CF8FA5929CC2F5AC07039CA7A999B7E078FAA2AF6870A1250
    1 : 0xA75BC7903E3B00DB5319E415198EBDF405B7174FC5BC3A2A311A6FF320108452
    2 : 0x3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
    3 : 0x3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
    4 : 0x646B2BF080A3F5B7DB98A026EB86A878CADFA931B9403DEC515BBC9F43FD5FFD
    5 : 0x145593F31870EA6AB6C7E9F2C9CAB1BD4C23B8F2A679E151494D32719FA1E730
    6 : 0x3D458CFE55CC03EA1F443F1562BEEC8DF51C75E14A9FCF9A7234A13F198E7969
    7 : 0xB926225AC488E9C50EF2FA815AA7104B385A06907093BFB1DC62EEB7ABECDDF1
    8 : 0x175F3623E7CB04263C6A7E37D15FF365D8F332A545CDEA165D88A5790F12156F
    9 : 0x0B705D2568348A78C791DEF83E863526343AFF35D67FF0040A02B10F21FA9FA2
    10: 0xC545B694FBD9B91C9316E075D5CC747758B14350B83FDDF6FE82EE470E7D652D
    11: 0x0000000000000000000000000000000000000000000000000000000000000000
    12: 0x0000000000000000000000000000000000000000000000000000000000000000
    13: 0x0000000000000000000000000000000000000000000000000000000000000000
    14: 0x1DD2C3C78E629AD7ECC3789C06F7B41FEAF3CC9A6D5EE4256E41C64C89910F22
```

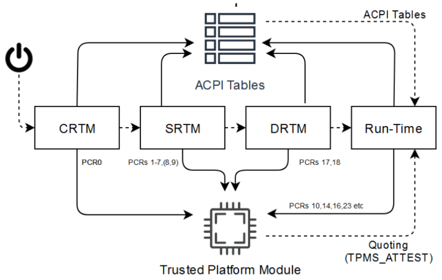
UEFI Eventlog (location)

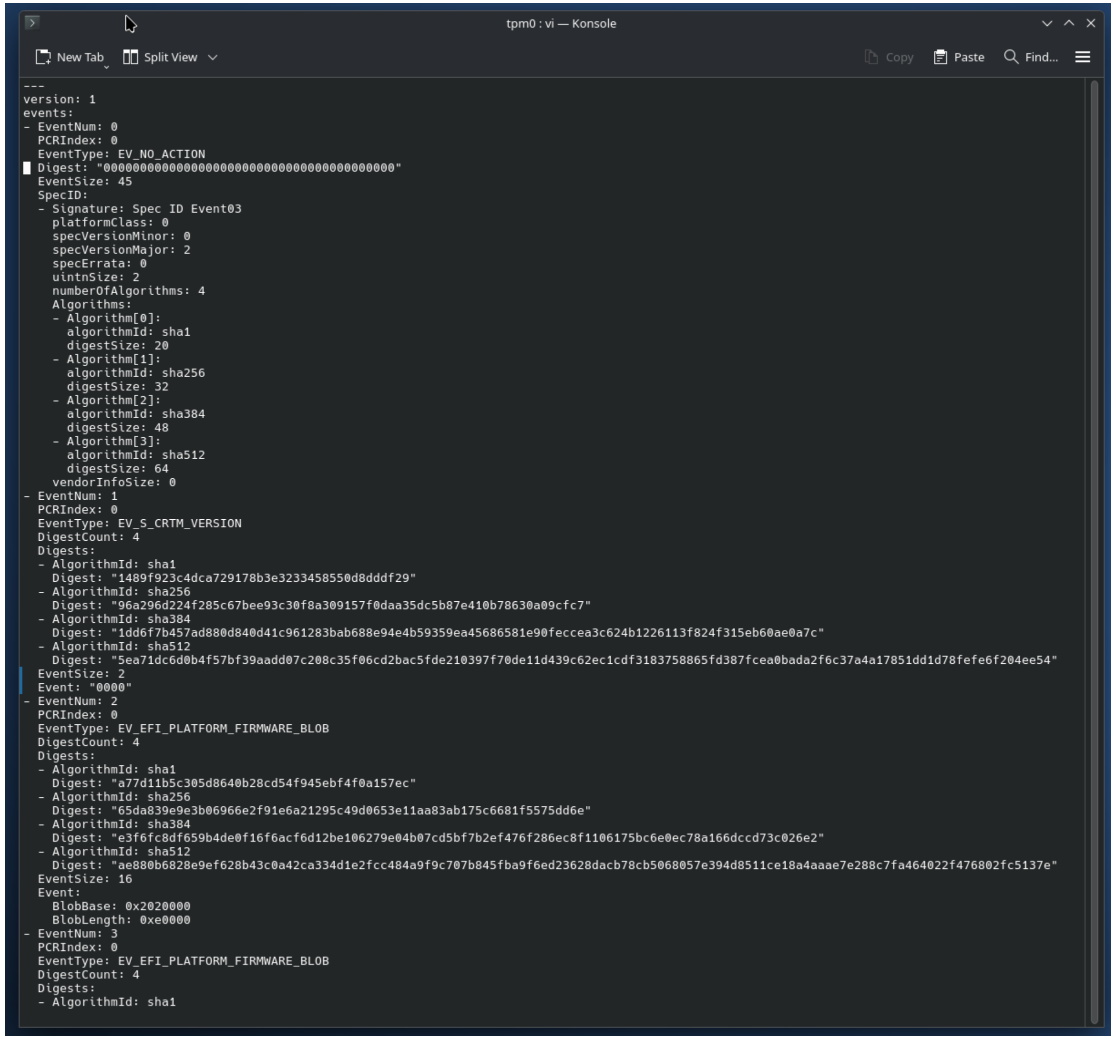




```
ian@debianwork:/sys/kernel/security/tpm0$ ls -l
total 0
-r--r----- 1 root tss 0 Sep 28 18:08 binary_bios_measurements
ian@debianwork:/sys/kernel/security/tpm0$ tpm2_eventlog ./binary_bios_measurements
```

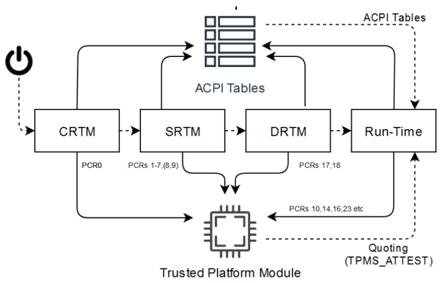
UEFI Eventlog (contents)

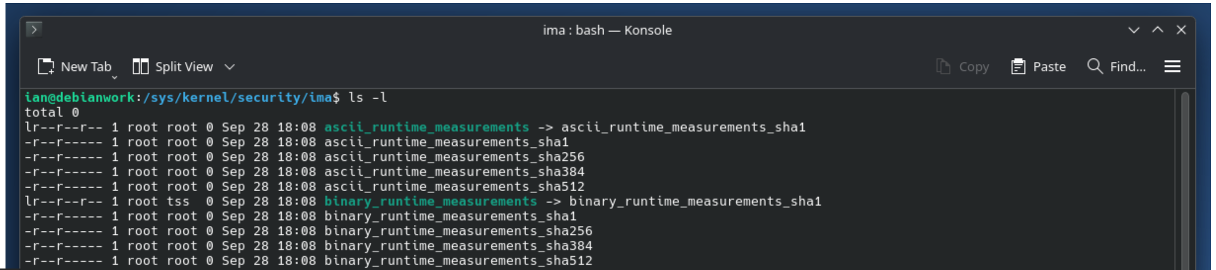




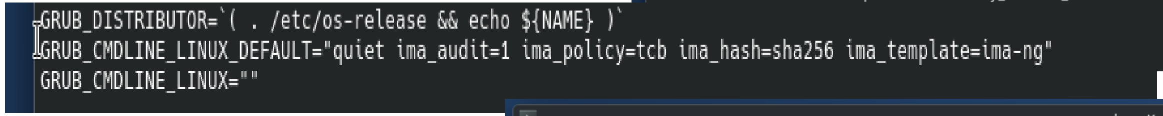
```
---
version: 1
events:
- EventNum: 0
  PCRIndex: 0
  EventType: EV_NO_ACTION
█ Digest: "0000000000000000000000000000000000000000"
  EventSize: 45
  SpecID:
  - Signature: Spec ID Event03
    platformClass: 0
    specVersionMinor: 0
    specVersionMajor: 2
    specErrata: 0
    uintnSize: 2
    numberOfAlgorithms: 4
    Algorithms:
    - Algorithm[0]:
      algorithmId: sha1
      digestSize: 20
    - Algorithm[1]:
      algorithmId: sha256
      digestSize: 32
    - Algorithm[2]:
      algorithmId: sha384
      digestSize: 48
    - Algorithm[3]:
      algorithmId: sha512
      digestSize: 64
    vendorInfoSize: 0
- EventNum: 1
  PCRIndex: 0
  EventType: EV_S_CRTM_VERSION
  DigestCount: 4
  Digests:
  - AlgorithmId: sha1
    Digest: "1489f923c4dca729178b3e3233458550d8dddf29"
  - AlgorithmId: sha256
    Digest: "96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7"
  - AlgorithmId: sha384
    Digest: "1dd6f7b457ad880d840d41c961283bab688e94e4b59359ea45686581e90feccea3c624b1226113f824f315eb60ae0a7c"
  - AlgorithmId: sha512
    Digest: "5ea71dc6d0b4f57bf39aadd07c208c35f06cd2bac5fde210397f70de11d439c62ec1cdf3183758865fd387fcea0bada2f6c37a4a17851dd1d78fefe6f204ee54"
  EventSize: 2
  Event: "0000"
- EventNum: 2
  PCRIndex: 0
  EventType: EV_EFI_PLATFORM_FIRMWARE_BLOB
  DigestCount: 4
  Digests:
  - AlgorithmId: sha1
    Digest: "a77d11b5c305d8640b28cd54f945ebf4f0a157ec"
  - AlgorithmId: sha256
    Digest: "65da839e9e3b06966e2f91e6a21295c49d0653e11aa83ab175c6681f5575dd6e"
  - AlgorithmId: sha384
    Digest: "e3f6fc8df659b4de0f16f6acf6d12be106279e04b07cd5bf7b2ef476f286ec8f1106175bc6e0ec78a166dccd73c026e2"
  - AlgorithmId: sha512
    Digest: "ae880b6828e9ef628b43c0a42ca334d1e2fcc484a9f9c707b845fba9f6ed23628dacb78cb5068057e394d8511ce18a4aaae7e288c7fa464022f476802fc5137e"
  EventSize: 16
  Event:
    BlobBase: 0x2020000
    BlobLength: 0xe0000
- EventNum: 3
  PCRIndex: 0
  EventType: EV_EFI_PLATFORM_FIRMWARE_BLOB
  DigestCount: 4
  Digests:
  - AlgorithmId: sha1
```

Linux IMA

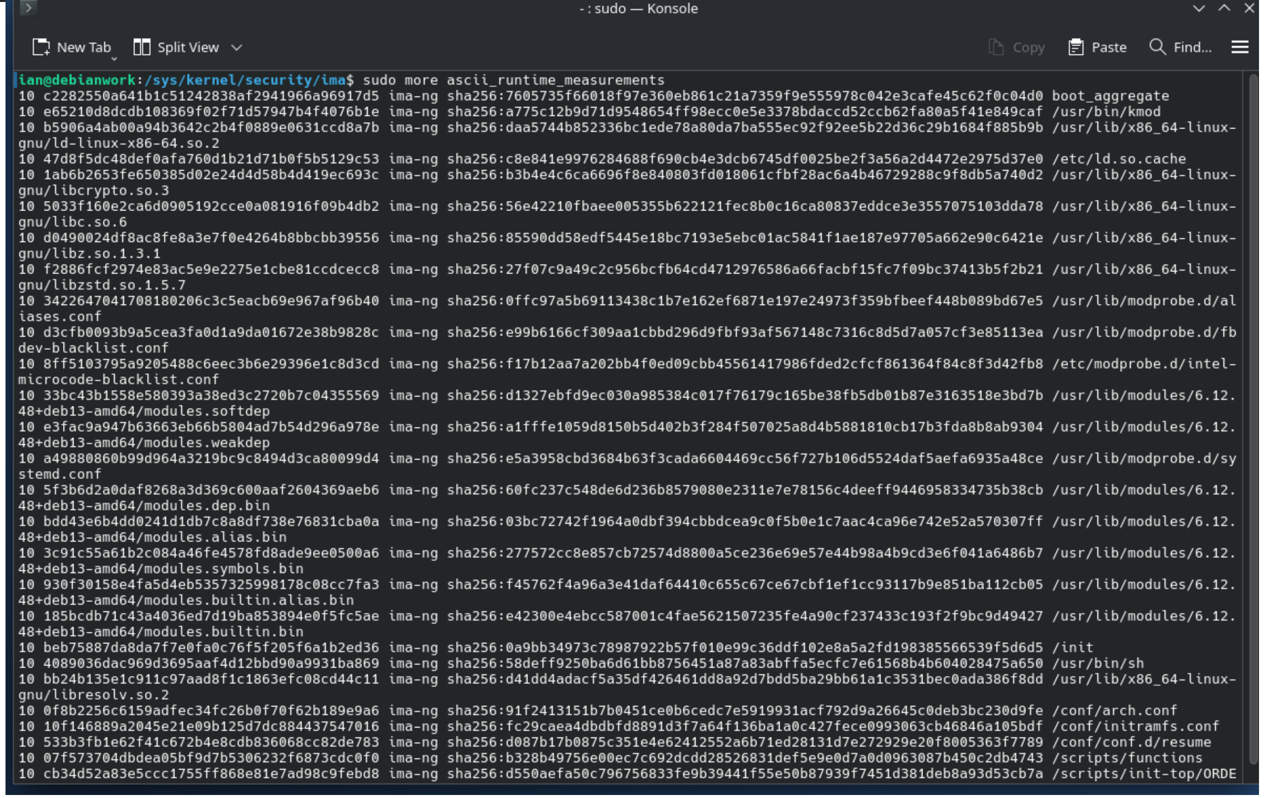




```
ian@debianwork:/sys/kernel/security/ima$ ls -l
total 0
lr--r--r-- 1 root root 0 Sep 28 18:08 ascii_runtime_measurements -> ascii_runtime_measurements_sha1
-r--r----- 1 root root 0 Sep 28 18:08 ascii_runtime_measurements_sha1
-r--r----- 1 root root 0 Sep 28 18:08 ascii_runtime_measurements_sha256
-r--r----- 1 root root 0 Sep 28 18:08 ascii_runtime_measurements_sha384
-r--r----- 1 root root 0 Sep 28 18:08 ascii_runtime_measurements_sha512
lr--r--r-- 1 root tss  0 Sep 28 18:08 binary_runtime_measurements -> binary_runtime_measurements_sha1
-r--r----- 1 root root 0 Sep 28 18:08 binary_runtime_measurements_sha1
-r--r----- 1 root root 0 Sep 28 18:08 binary_runtime_measurements_sha256
-r--r----- 1 root root 0 Sep 28 18:08 binary_runtime_measurements_sha384
-r--r----- 1 root root 0 Sep 28 18:08 binary_runtime_measurements_sha512
```

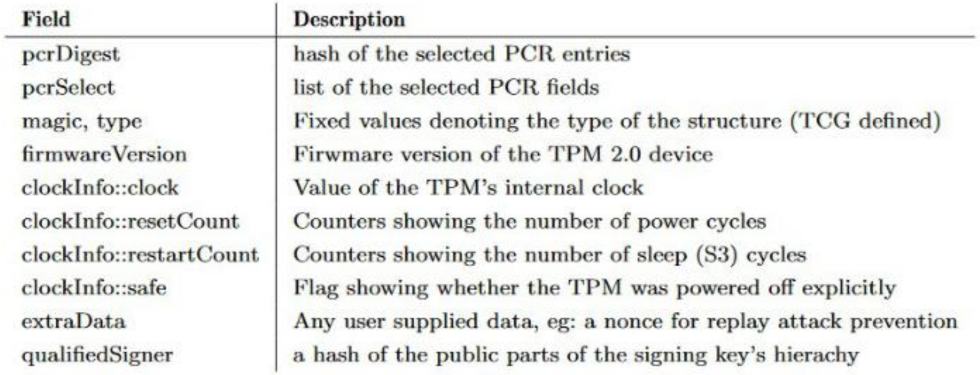


```
GRUB_DISTRIBUTOR=`( . /etc/os-release && echo ${NAME} )`
GRUB_CMDLINE_LINUX_DEFAULT="quiet ima_audit=1 ima_policy=tcb ima_hash=sha256 ima_template=ima-ng"
GRUB_CMDLINE_LINUX=""
```



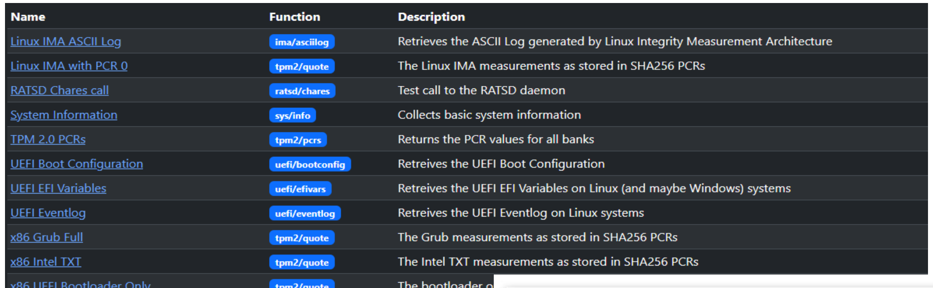
```
ian@debianwork:/sys/kernel/security/ima$ sudo more ascii_runtime_measurements
10 c2282550a641b1c51242838af2941966a96917d5 ima-ng sha256:7605735f66018f97e360eb861c21a7359f9e555978c042e3cafe45c62f0c04d0 boot_aggregate
10 e65210d8dcdb108369f02f71d57947b4f4076b1e ima-ng sha256:a775c12b9d71d9548654ff98ecc0e5e3378bdaccd52ccb62fa80a5f41e849caf /usr/bin/kmod
10 b5906a4ab00a94b3642c2b4f0889e0631ccd8a7b ima-ng sha256:daa5744b852336bc1ede78a80da7ba555ec92f92ee5b22d36c29b1684f885b9b /usr/lib/x86_64-linux-
gnu/ld-linux-x86-64.so.2
10 47d8f5dc48def0afa760d1b21d71b0f5b5129c53 ima-ng sha256:c8e841e9976284688f690cb4e3dcb6745df0025be2f3a56a2d4472e2975d37e0 /etc/ld.so.cache
10 1ab6b2653fe650385d02e24d4d58b4d419ec693c ima-ng sha256:b3b4e4c6ca6696f8e840803fd018061cfbf28ac6a4b46729288c9f8db5a740d2 /usr/lib/x86_64-linux-
gnu/libcrypto.so.3
10 5033f160e2ca6d0905192cce0a081916f09b4db2 ima-ng sha256:56e42210fbaee005355b622121fec8b0c16ca80837eddce3e3557075103dda78 /usr/lib/x86_64-linux-
gnu/libc.so.6
10 d0490024df8ac8fe8a3e7f0e4264b8bbcbb39556 ima-ng sha256:85590dd58edf5445e18bc7193e5ebc01ac5841f1ae187e97705a662e90c6421e /usr/lib/x86_64-linux-
gnu/libz.so.1.3.1
10 f2886fcf2974e83ac5e9e2275e1cbe81ccdcecc8 ima-ng sha256:27f07c9a49c2c956bcfb64cd4712976586a66facbf15fc7f09bc37413b5f2b21 /usr/lib/x86_64-linux-
gnu/libzstd.so.1.5.7
10 3422647041708180206c3c5eacb69e967af96b40 ima-ng sha256:0ffc97a5b69113438c1b7e162ef6871e197e24973f359bfbeef448b089bd67e5 /usr/lib/modprobe.d/al
iases.conf
10 d3cfb0093b9a5cea3fa0d1a9da01672e38b9828c ima-ng sha256:e99b6166cf309aa1cbbd296d9fbf93af567148c7316c8d5d7a057cf3e85113ea /usr/lib/modprobe.d/fb
dev-blacklist.conf
10 8ff5103795a9205488c6eec3b6e29396e1c8d3cd ima-ng sha256:f17b12aa7a202bb4f0ed09cbb45561417986fded2cfcf861364f84c8f3d42fb8 /etc/modprobe.d/intel-
microcode-blacklist.conf
10 33bc43b1558e580393a38ed3c2720b7c04355569 ima-ng sha256:d1327ebfd9ec030a985384c017f76179c165be38fb5db01b87e3163518e3bd7b /usr/lib/modules/6.12.
48+deb13-amd64/modules.softdep
10 e3fac9a947b63663eb66b5804ad7b54d296a978e ima-ng sha256:a1fffe1059d8150b5d402b3f284f507025a8d4b5881810cb17b3fda8b8ab9304 /usr/lib/modules/6.12.
48+deb13-amd64/modules.weakdep
10 a49880860b99d964a3219bc9c8494d3ca80099d4 ima-ng sha256:e5a3958cbd3684b63f3cada6604469cc56f727b106d5524daf5aefa6935a48ce /usr/lib/modprobe.d/sy
stemd.conf
10 5f3b6d2a0daf8268a3d369c600aaf2604369aeb6 ima-ng sha256:60fc237c548de6d236b8579080e2311e7e78156c4deeff9446958334735b38cb /usr/lib/modules/6.12.
48+deb13-amd64/modules.dep.bin
10 bdd43e6b4dd0241d1db7c8a8df738e76831cba0a ima-ng sha256:03bc72742f1964a0dbf394cbbdcea9c0f5b0e1c7aac4ca96e742e52a570307ff /usr/lib/modules/6.12.
48+deb13-amd64/modules.alias.bin
10 3c91c55a61b2c084a46fe4578fd8ade9ee0500a6 ima-ng sha256:277572cc8e857cb72574d8800a5ce236e69e57e44b98a4b9cd3e6f041a6486b7 /usr/lib/modules/6.12.
48+deb13-amd64/modules.symbols.bin
10 930f30158e4fa5d4eb5357325998178c08cc7fa3 ima-ng sha256:f45762f4a96a3e41daf64410c655c67ce67cbf1ef1cc93117b9e851ba112cb05 /usr/lib/modules/6.12.
48+deb13-amd64/modules.builtin.alias.bin
10 185bcdb71c43a4036ed7d19ba853894e0f5fc5ae ima-ng sha256:e42300e4ebcc587001c4fae5621507235fe4a90cf237433c193f2f9bc9d49427 /usr/lib/modules/6.12.
48+deb13-amd64/modules.builtin.bin
10 beb75887da8da7f7e0fa0c76f5f205f6a1b2ed36 ima-ng sha256:0a9bb34973c78987922b57f010e99c36ddf102e8a5a2fd198385566539f5d6d5 /init
10 4089036dac969d3695aaf4d12bbd90a9931ba869 ima-ng sha256:58deff9250ba6d61bb8756451a87a83abffa5ecfc7e61568b4b604028475a650 /usr/bin/sh
10 bb24b135e1c911c97aad8f1c1863efc08cd44c11 ima-ng sha256:d41dd4adacf5a35df426461dd8a92d7bdd5ba29bb61a1c3531bec0ada386f8dd /usr/lib/x86_64-linux-
gnu/libresolv.so.2
10 0f8b2256c6159adfec34fc26b0f70f62b189e9a6 ima-ng sha256:91f2413151b7b0451ce0b6cedc7e5919931acf792d9a26645c0deb3bc230d9fe /conf/arch.conf
10 10f146889a2045e21e09b125d7dc884437547016 ima-ng sha256:fc29caea4dbdbfd8891d3f7a64f136ba1a0c427fece0993063cb46846a105bdf /conf/initramfs.conf
10 533b3fb1e62f41c672b4e8cdb836068cc82de783 ima-ng sha256:d087b17b0875c351e4e62412552a6b71ed28131d7e272929e20f8005363f7789 /conf/conf.d/resume
10 07f573704dbdea05bf9d7b5306232f6873cdc0f0 ima-ng sha256:b328b49756e00ec7c692dcdd28526831def5e9e0d7a0d0963087b450c2db4743 /scripts/functions
10 cb34d52a83e5ccc1755ff868e81e7ad98c9febd8 ima-ng sha256:d550aefa50c796756833fe9b39441f55e50b87939f7451d381deb8a93d53cb7a /scripts/init-top/ORDE
```

TPM - Quotes

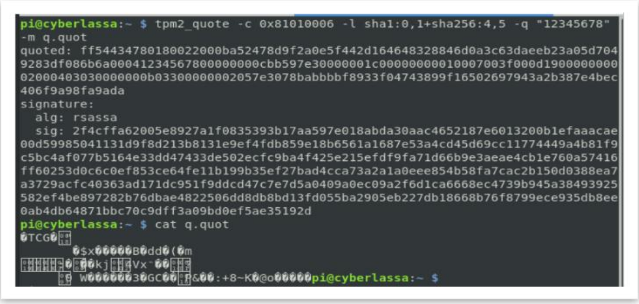


Field	Description
pcrDigest	hash of the selected PCR entries
pcrSelect	list of the selected PCR fields
magic, type	Fixed values denoting the type of the structure (TCG defined)
firmwareVersion	Firwmare version of the TPM 2.0 device
clockInfo::clock	Value of the TPM's internal clock
clockInfo::resetCount	Counters showing the number of power cycles
clockInfo::restartCount	Counters showing the number of sleep (S3) cycles
clockInfo::safe	Flag showing whether the TPM was powered off explicitly
extraData	Any user supplied data, eg: a nonce for replay attack prevention
qualifiedSigner	a hash of the public parts of the signing key's hierachy

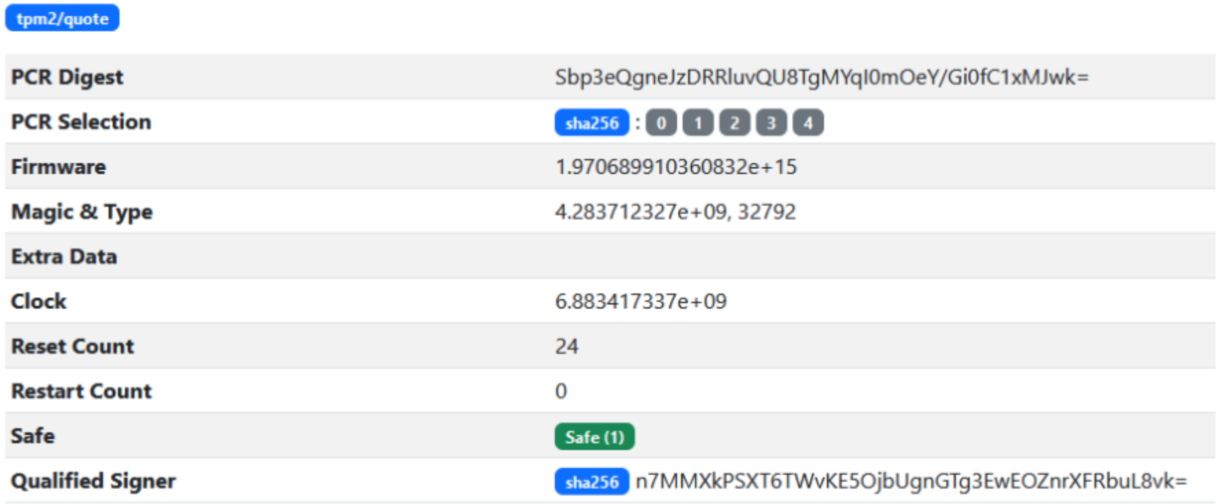
Table 1. TPM 2.0 Quote (TPMS_ATTEST) Fields



Name	Function	Description
Linux IMA ASCII Log	ima/asciilog	Retrieves the ASCII Log generated by Linux Integrity Measurement Architecture
Linux IMA with PCR 0	tpm2/quote	The Linux IMA measurements as stored in SHA256 PCRs
RATSD Chares call	ratsd/chares	Test call to the RATSD daemon
System Information	sys/info	Collects basic system information
TPM 2.0 PCRs	tpm2/pcrs	Returns the PCR values for all banks
UEFI Boot Configuration	uefi/bootconfig	Retreives the UEFI Boot Configuration
UEFI EFI Variables	uefi/efivars	Retreives the UEFI EFI Variables on Linux (and maybe Windows) systems
UEFI Eventlog	uefi/eventlog	Retreives the UEFI Eventlog on Linux systems
x86 Grub Full	tpm2/quote	The Grub measurements as stored in SHA256 PCRs
x86 Intel TXT	tpm2/quote	The Intel TXT measurements as stored in SHA256 PCRs
x86 UEFI Bootloader Only	tpm2/quote	The bootloader o
x86 UEFI Bootloader and CRTM	tpm2/quote	The bootloader a
x86 UEFI CRTM Firmware	tpm2/quote	The initial CRTM f
x86 UEFI CRTM only	tpm2/quote	The initial CRTM f
x86 UEFI SRTM	tpm2/quote	The initial SRTM r
x86 UEFI SRTM and Bootloader	tpm2/quote	The SRTM and bo

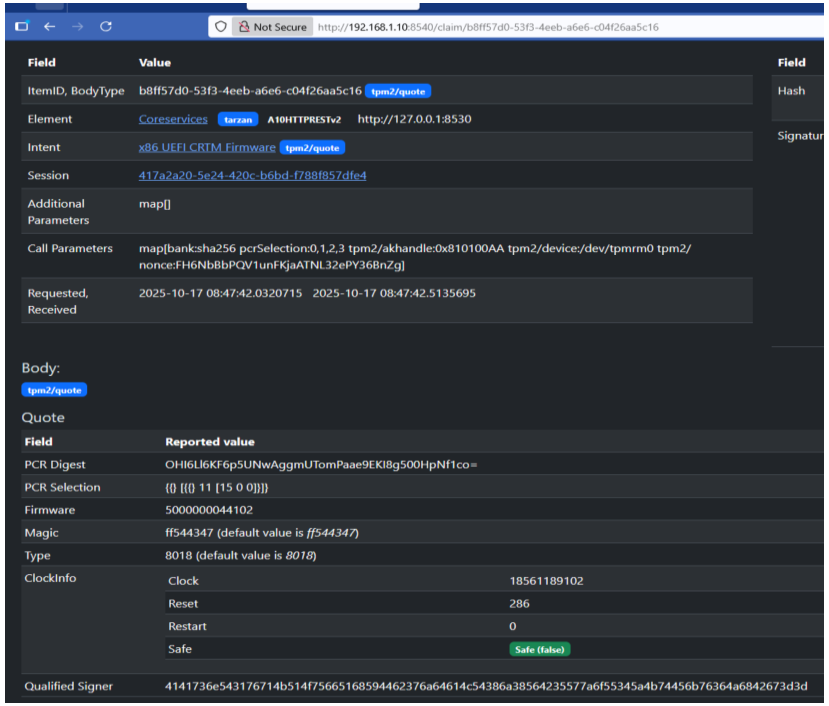


```
pi@cyberlassa:~ $ tpm2_quote -c 0x81010006 -l sha1:0,1+sha256:4,5 -q "12345678"
-m q.quot
quoted: ff54434780180022000ba52478d9f2a0e5f442d164648328846d0a3c63daeeb23a05d704
9283df086b6a000412345678000000000cbb597e30000001c000000000010007003f000d1900000000
0200040303000000b03300000002057e3078babbbbf8933f04743899f16502697943a2b387e4bec
406f9a98fa9ada
signature:
  alg: rsassa
  sig: 2f4cffa62005e8927a1f0835393b17aa597e018abda30aac4652187e6013200b1efaaacae
00d59985041131d9f8d213b8131e9ef4fdb859e18b6561a1687e53a4cd45d69cc11774449a4b81f9
c5bc4af077b5164e33dd47433de502ecfc9ba4f425e215efdf9fa71d66b9e3aeae4cb1e760a57416
ff60253d0c6c0ef853ce64fe11b199b35ef27bad4cca73a2a1a0eee854b58fa7cac2b150d0388ea7
a3729acfc40363ad171dc951f9ddcd47c7e7d5a0409a0ec09a2f6d1ca6668ec4739b945a38493925
582ef4be897282b76dbae4822506dd8db8bd13fd055ba2905eb227db18668b76f8799ece935db8ee
0ab4db64871bbc70c9dff3a09bd0ef5ae35192d
pi@cyberlassa:~ $ cat q.quot
�TCG��
     �$x�����B�dd�(�m
��������kj��Vx`����
  �� W������3�GC���P&��:+8~K�@o�����pi@cyberlassa:~ $
```



tpm2/quote

PCR Digest	Sbp3eQgneJzDRRluvQU8TgMYql0mOeY/Gi0fC1xMJwk=
PCR Selection	sha256 : 0 1 2 3 4
Firmware	1.970689910360832e+15
Magic & Type	4.283712327e+09, 32792
Extra Data	
Clock	6.883417337e+09
Reset Count	24
Restart Count	0
Safe	Safe (1)
Qualified Signer	sha256 n7MMXkPSXT6TWvKE5OjbUgnGTg3EwEOZnrXFRbuL8vk=



Not Secure
http://192.168.1.10:8540/claim/b8ff57d0-53f3-4eeb-a6e6-c04f26aa5c16

Field	Value
ItemID, BodyType	b8ff57d0-53f3-4eeb-a6e6-c04f26aa5c16 tpm2/quote
Element	Coreservices tarzan A10HTTPRESTv2 http://127.0.0.1:8530
Intent	x86 UEFI CRTM Firmware tpm2/quote
Session	417a2a20-5e24-420c-b6bd-f788f857dfe4
Additional Parameters	map[]
Call Parameters	map[bank:sha256 pcrSelection:0,1,2,3 tpm2/akhandle:0x810100AA tpm2/device:/dev/tpmrm0 tpm2/nonce:FH6NbBbPQV1unFKjaATNL32ePY36BnZg]
Requested, Received	2025-10-17 08:47:42.0320715 2025-10-17 08:47:42.5135695

Field
Hash
Signatur

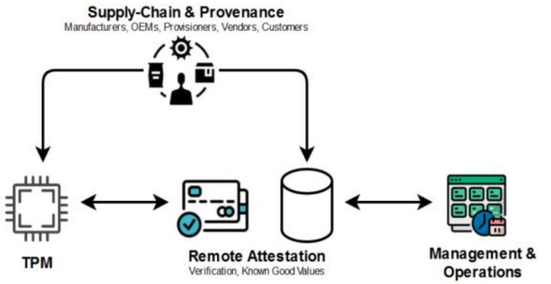
Body:

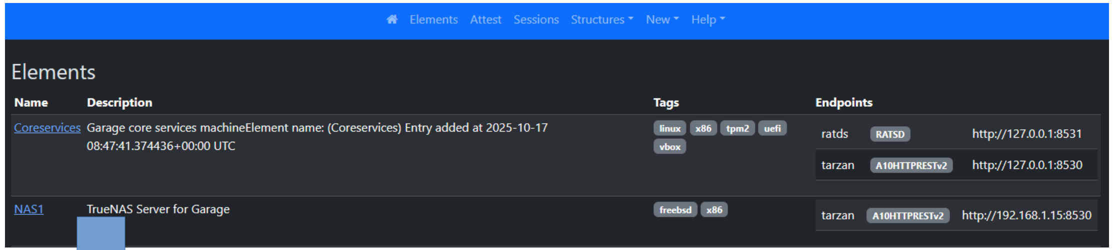
tpm2/quote

Quote

Field	Reported value	
PCR Digest	OHI6Ll6KF6p5UNwAggmUTomPaae9EKl8g500HpNf1co=	
PCR Selection	{{} [{{} 11 [15 0 0]}]}	
Firmware	5000000044102	
Magic	ff544347 (default value is *ff544347*)	
Type	8018 (default value is *8018*)	
ClockInfo	Clock	18561189102
	Reset	286
	Restart	0
	Safe	Safe (false)
Qualified Signer	4141736e543176714b514f75665168594462376a64614c54386a38564235577a6f55345a4b74456b76364a6842673d3d	

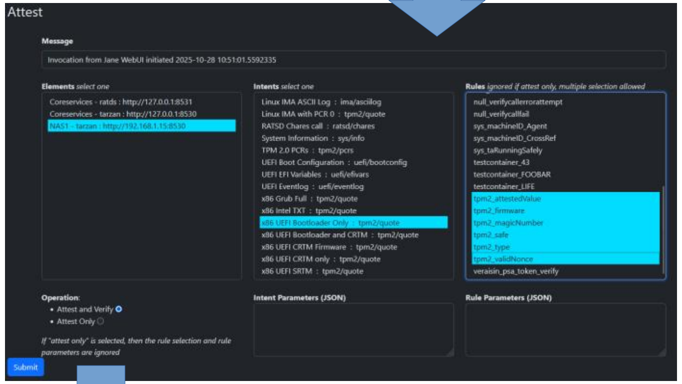
Attestation


Supply-Chain & Provenance
Manufacturers, OEMs, Provisioners, Vendors, Customers
TPM
Remote Attestation
Verification, Known Good Values
Management & Operations



Elements

Name	Description	Tags	Endpoints
Coreservices	Garage core services machineElement name: (Coreservices) Entry added at 2025-10-17 08:47:41.374436+00:00 UTC	linux x86 tpm2 uefi vbox	ratds RATSD http://127.0.0.1:8531 tarzan A10HTTPRESTv2 http://127.0.0.1:8530
NAS1	TrueNAS Server for Garage	freebsd x86	tarzan A10HTTPRESTv2 http://192.168.1.15:8530



Attest

Message

Invocation from Jane WebUI initiated 2025-10-28 10:51:01.5592335

Elements *select one*

- Coreservices - ratds : http://127.0.0.1:8531
- Coreservices - tarzan : http://127.0.0.1:8530
- [✓ NAS1 - tarzan : http://192.168.1.15:8530]

Intents *select one*

- Linux IMA ASCII Log : ima/asciilog
- Linux IMA with PCR 0 : tpm2/quote
- RATSD Chares call : ratsd/chares
- System Information : sys/info
- TPM 2.0 PCRs : tpm2/pcrs
- UEFI Boot Configuration : uefi/bootconfig
- UEFI EFI Variables : uefi/efivars
- UEFI Eventlog : uefi/eventlog
- x86 Grub Full : tpm2/quote
- x86 Intel TXT : tpm2/quote
- [✓ x86 UEFI Bootloader Only : tpm2/quote]
- x86 UEFI Bootloader and CRTM : tpm2/quote
- x86 UEFI CRTM Firmware : tpm2/quote
- x86 UEFI CRTM only : tpm2/quote
- x86 UEFI SRTM : tpm2/quote

Rules *ignored if attest only, multiple selection allowed*

- null_verifycallerrorattempt
- null_verifycallfail
- sys_machineID_Agent
- sys_machineID_CrossRef
- sys_taRunningSafely
- testcontainer_43
- testcontainer_FOOBAR
- testcontainer_LIFE
- [✓ tpm2_attestedValue]
- [✓ tpm2_firmware]
- [✓ tpm2_magicNumber]
- [✓ tpm2_safe]
- [✓ tpm2_type]
- [✓ tpm2_validNonce]
- veraisin_psa_token_verify

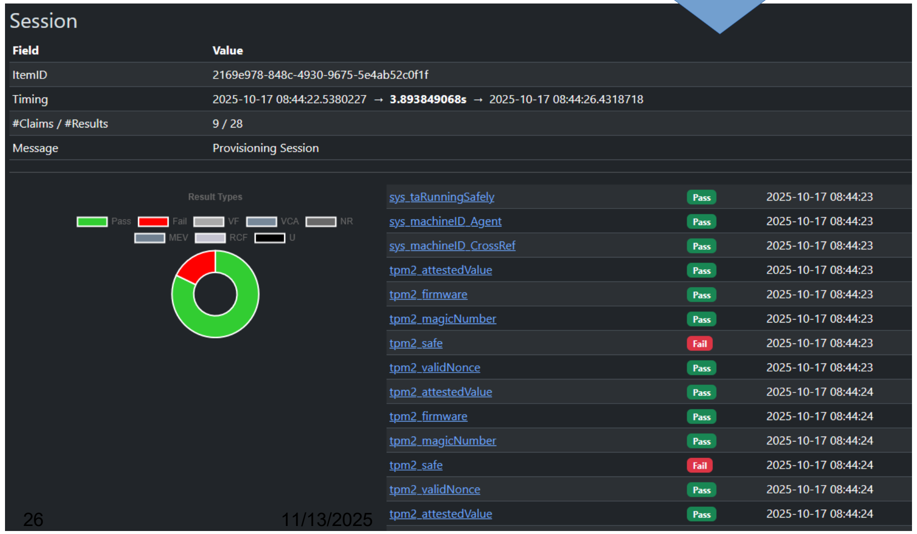
Operation:

- Attest and Verify ●
- Attest Only ○

If "attest only" is selected, then the rule selection and rule parameters are ignored

Intent Parameters (JSON)

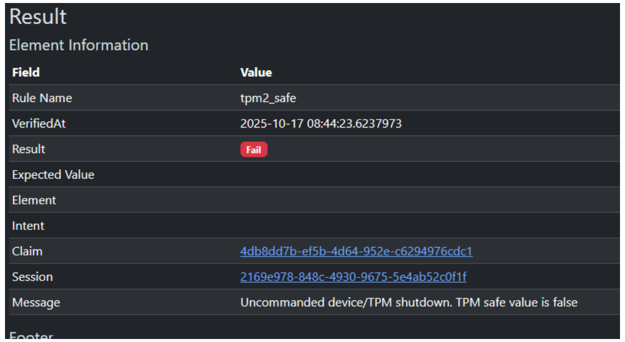
Rule Parameters (JSON)



Session

Field	Value
ItemID	2169e978-848c-4930-9675-5e4ab52c0f1f
Timing	2025-10-17 08:44:22.5380227 → **3.893849068s** → 2025-10-17 08:44:26.4318718
#Claims / #Results	9 / 28
Message	Provisioning Session

sys_taRunningSafely	Pass	2025-10-17 08:44:23
sys_machineID_Agent	Pass	2025-10-17 08:44:23
sys_machineID_CrossRef	Pass	2025-10-17 08:44:23
tpm2_attestedValue	Pass	2025-10-17 08:44:23
tpm2_firmware	Pass	2025-10-17 08:44:23
tpm2_magicNumber	Pass	2025-10-17 08:44:23
tpm2_safe	Fail	2025-10-17 08:44:23
tpm2_validNonce	Pass	2025-10-17 08:44:23
tpm2_attestedValue	Pass	2025-10-17 08:44:24
tpm2_firmware	Pass	2025-10-17 08:44:24
tpm2_magicNumber	Pass	2025-10-17 08:44:24
tpm2_safe	Fail	2025-10-17 08:44:24
tpm2_validNonce	Pass	2025-10-17 08:44:24
tpm2_attestedValue	Pass	2025-10-17 08:44:24

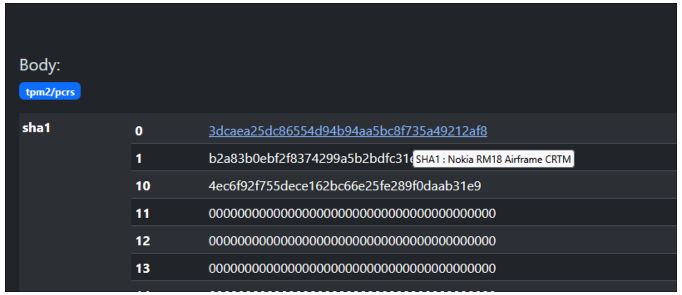


Result

Element Information

Field	Value
Rule Name	tpm2_safe
VerifiedAt	2025-10-17 08:44:23.6237973
Result	Fail
Expected Value	
Element	
Intent	
Claim	4db8dd7b-ef5b-4d64-952e-c6294976cdc1
Session	2169e978-848c-4930-9675-5e4ab52c0f1f
Message	Uncommanded device/TPM shutdown. TPM safe value is false

Footer

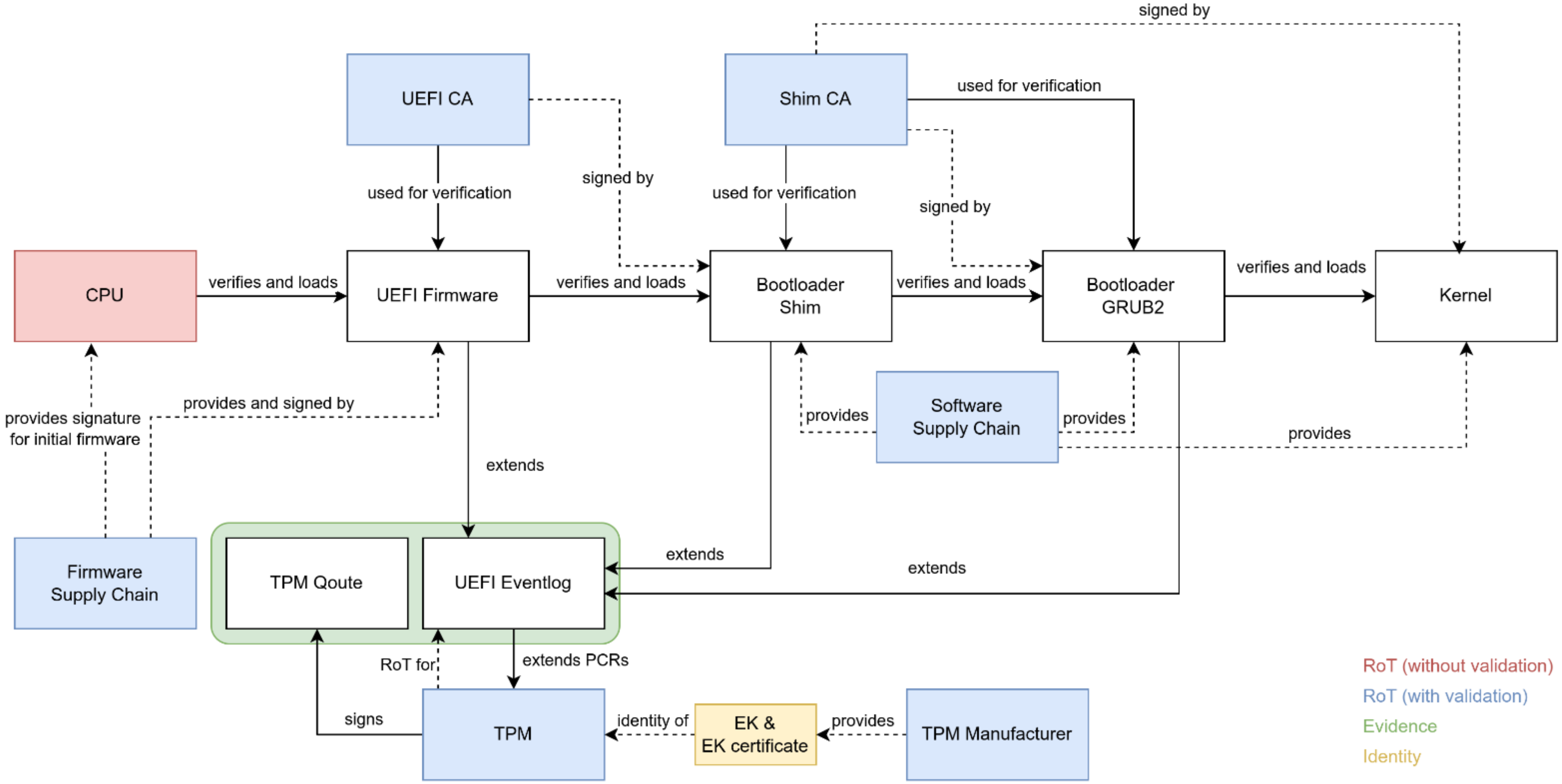


Body:

tpm2/pcrs

sha1	0	3dcaea25dc86554d94b94aa5bc8f735a49212af8
	1	b2a83b0ebf2f8374299a5b2bdfc31 SHA1 : Nokia RM18 Airframe CRTM
	10	4ec6f92f755dece162bc66e25fe289f0daab31e9
	11	0000000000000000000000000000000000000000
	12	0000000000000000000000000000000000000000
	13	0000000000000000000000000000000000000000

Chains of Trust



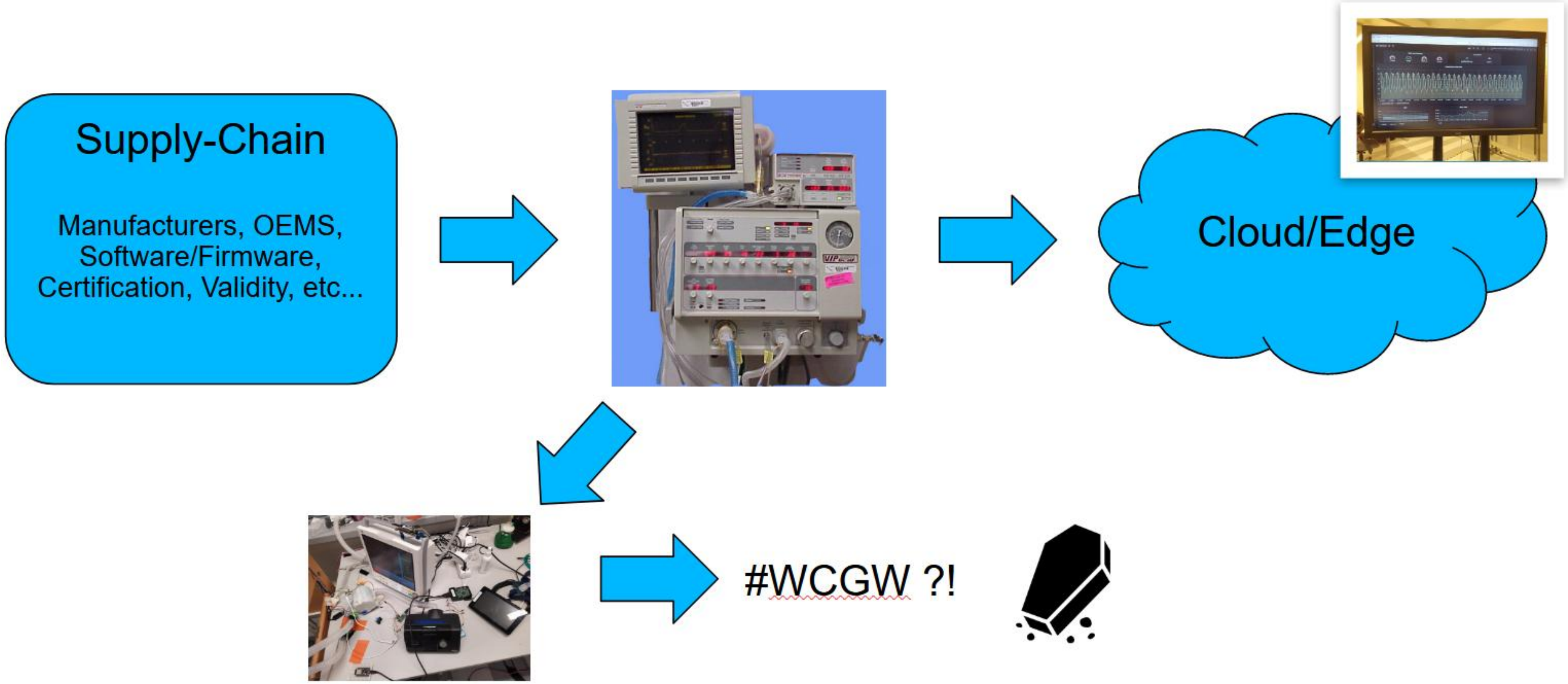
RoT (without validation)

RoT (with validation)

Evidence

Identity

Supply-Chain



Supply-Chain

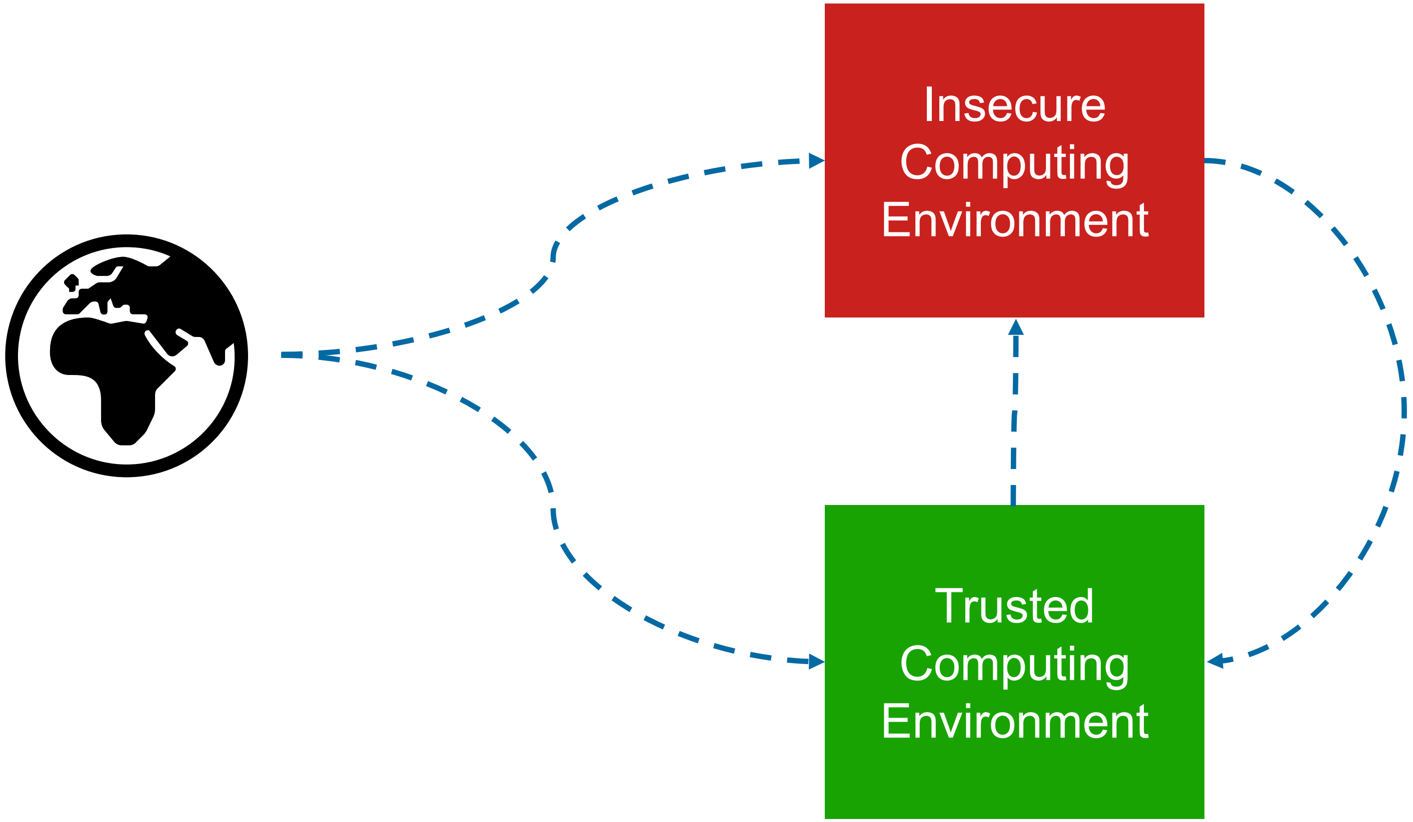
Manufacturers, OEMS, Software/Firmware, Certification, Validity, etc...

Cloud/Edge

#WCGW ?!

Images: Wikipedia #1 Brian Hall - Own work,
#2 https://wellcomeimages.org/indexplus/image/L0001305.html Wellcome Collection gallery (2018-03-29): CC-BY4.0
#3 © 2020 Ian Oliver

Enclaves & Confidential Computing



- Identity of the components
- Identity of the workload

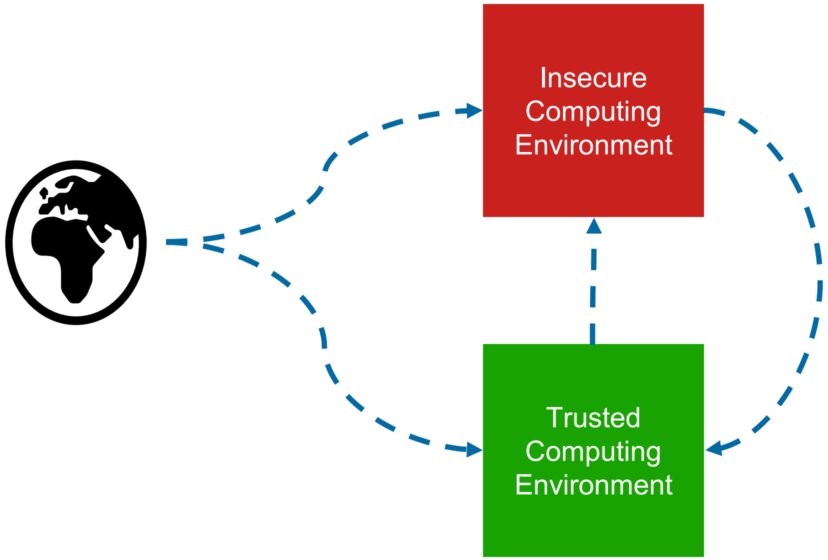
- Integrity of the components
- Integrity of the workload

- Ensuring that the workload is untampered, its data is untampered and is running in an identified and attested workspace.

Enclaves & Confidential Computing

- Intel TXT, SGX, TDX
- AMD PSP, SEV
- Arm TrustZone, CCA
- IBM Secure Execution (z15)
- RISC-V Keystone

- JavaCard,
- USIM,
- NFC Secure Execution
- HSM

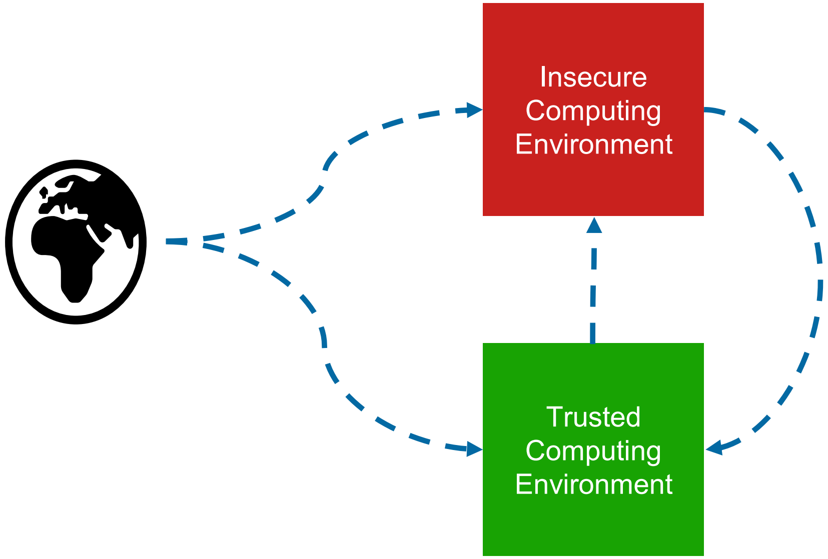


Enclaves & Confidential Computing

- Intel TXT, SGX, TDX
- AMD PSP, SEV
- Arm TrustZone, CCA
- IBM Secure Execution (z15)
- RISC-V Keystone

- JavaCard,
- USIM,
- NFC Secure Execution
- HSM

- Requires customized software (eg: SGX)
- Containers/Virtual Machines were too big
- Confidential Containers Project (https://confidentialcontainers.org/docs/overview/)



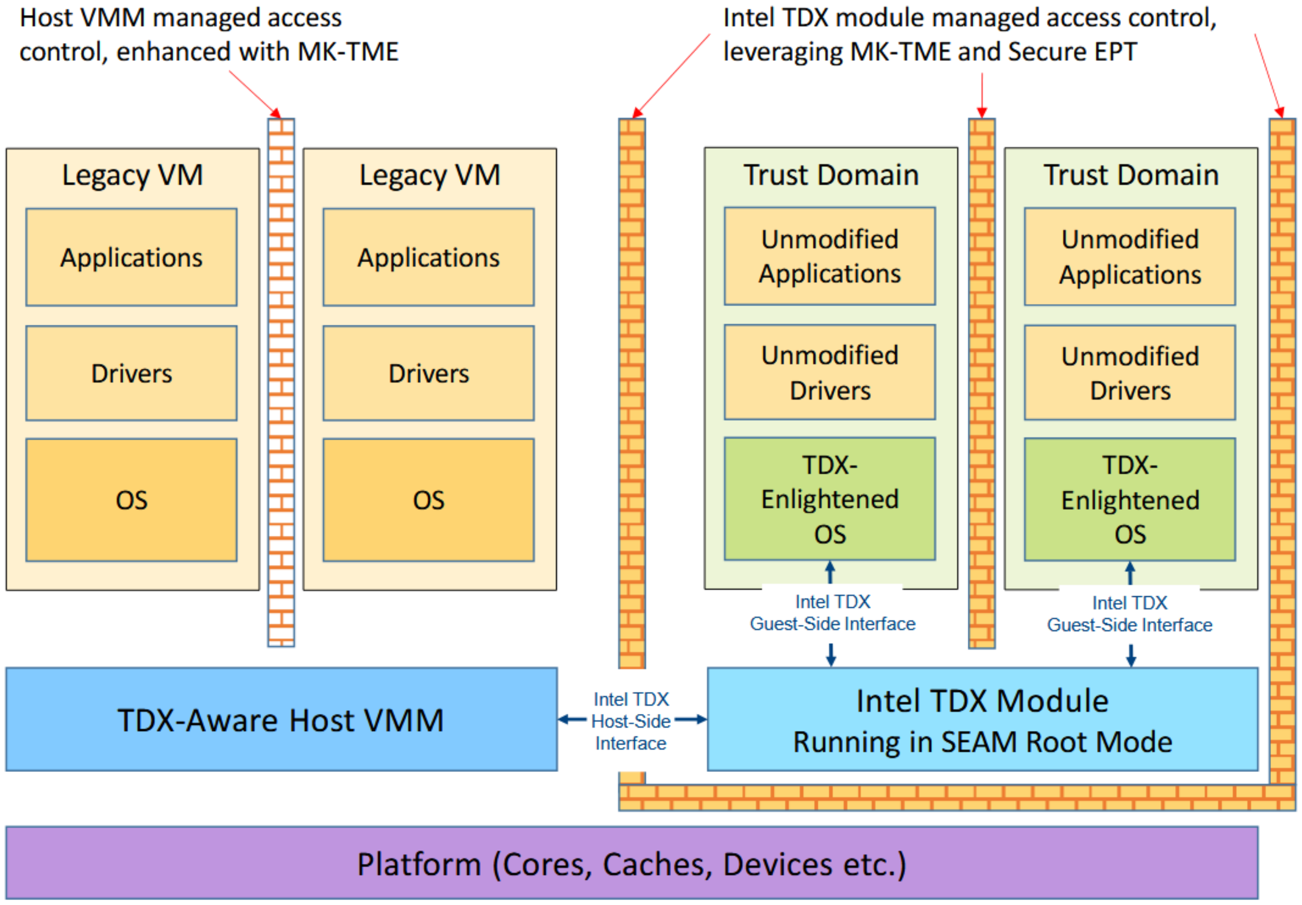
Insecure Computing Environment

Trusted Computing Environment

CONFIDENTIAL COMPUTING CONSORTIUM
A Technical Analysis of Confidential Computing

https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.3_unlocked.pdf

Intel TDX

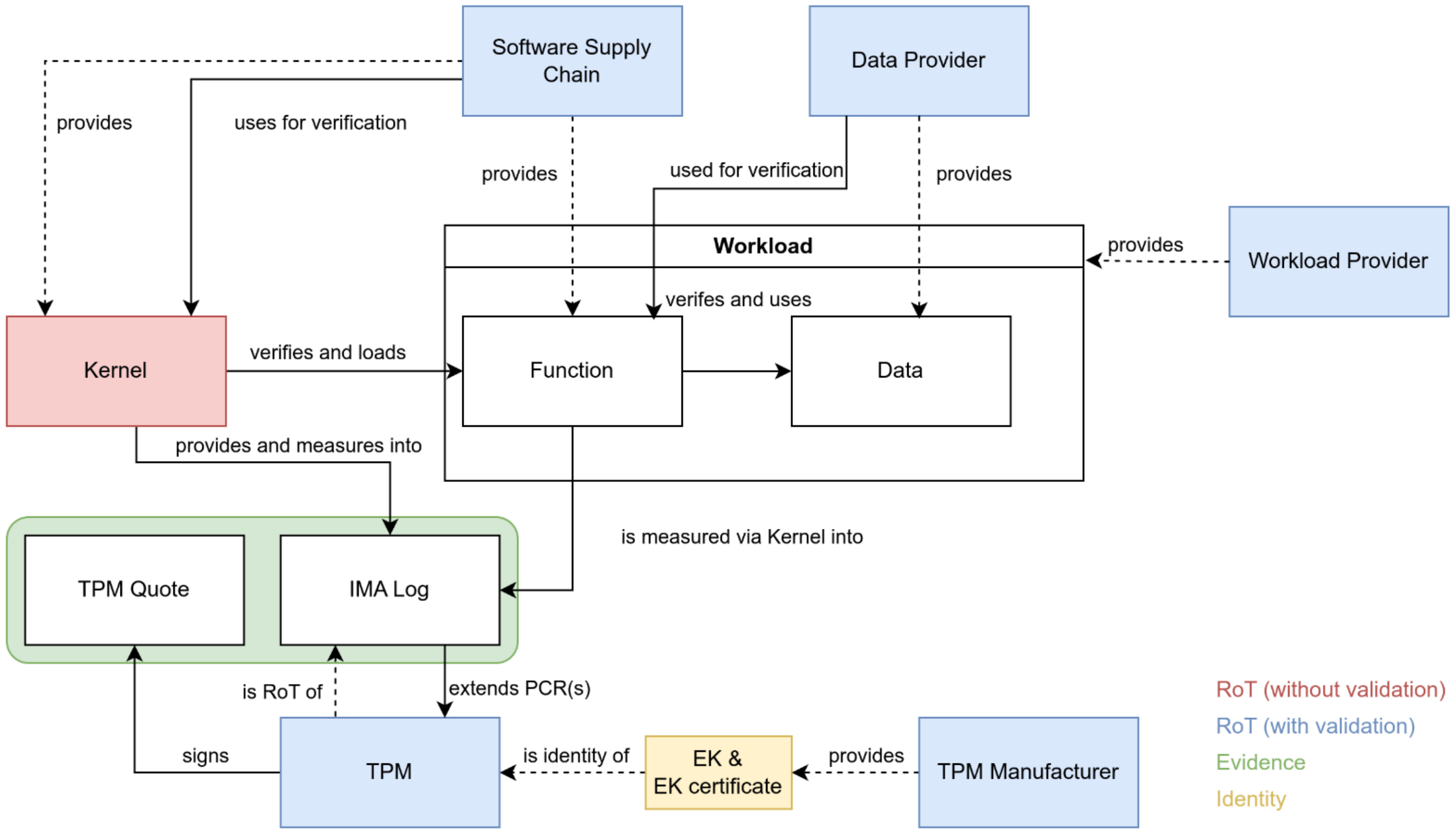


Host VMM managed access control, enhanced with MK-TME
Intel TDX module managed access control, leveraging MK-TME and Secure EPT
Legacy VM
Applications
Drivers
OS
Legacy VM
Applications
Drivers
OS
Trust Domain
Unmodified Applications
Unmodified Drivers
TDX-Enlightened OS
Intel TDX Guest-Side Interface
Trust Domain
Unmodified Applications
Unmodified Drivers
TDX-Enlightened OS
Intel TDX Guest-Side Interface
TDX-Aware Host VMM
Intel TDX Host-Side Interface
Intel TDX Module Running in SEAM Root Mode
Platform (Cores, Caches, Devices etc.)

Figure 2.1: Intel® Trust Domain Extension Components Overview

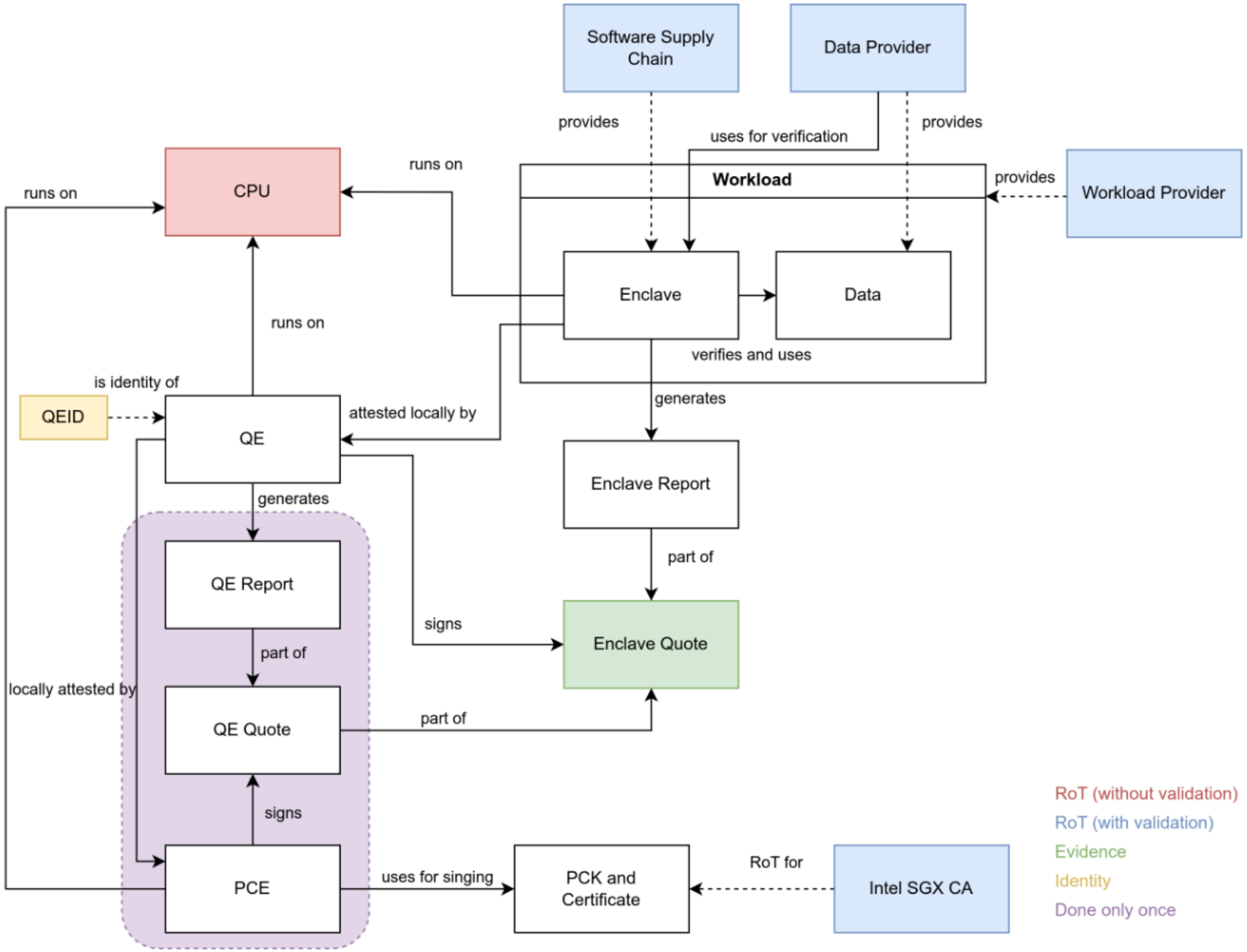
- CPU Overhead
- Early SGX was very limited
  - Cache coherency
  - Shared memory structures in CPU etc
- Untrusted-world communication
  - Requires additional silicon
  - Memory encryption
  - Cryptographic functions
  - IPC
  - I/O (off-chip)
- Attestation Mechanisms
- Malicious code is still code….
- Code signing/attestation before execution
- Privacy Concerns?
- Do you trust the CPU manufacturer’s code?

Chains of Trust (2):



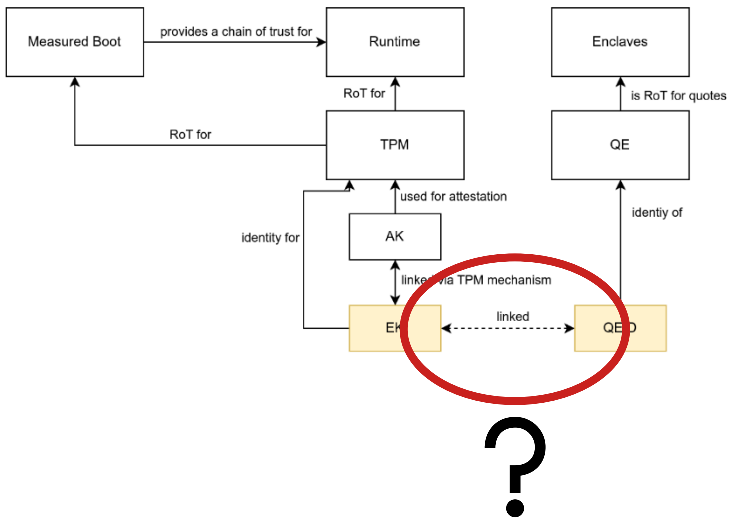
- We can use the TPM to establish the veracity of the system
- IMA to establish veracity at run-time
- No confidentiality

Chains of Trust (3):

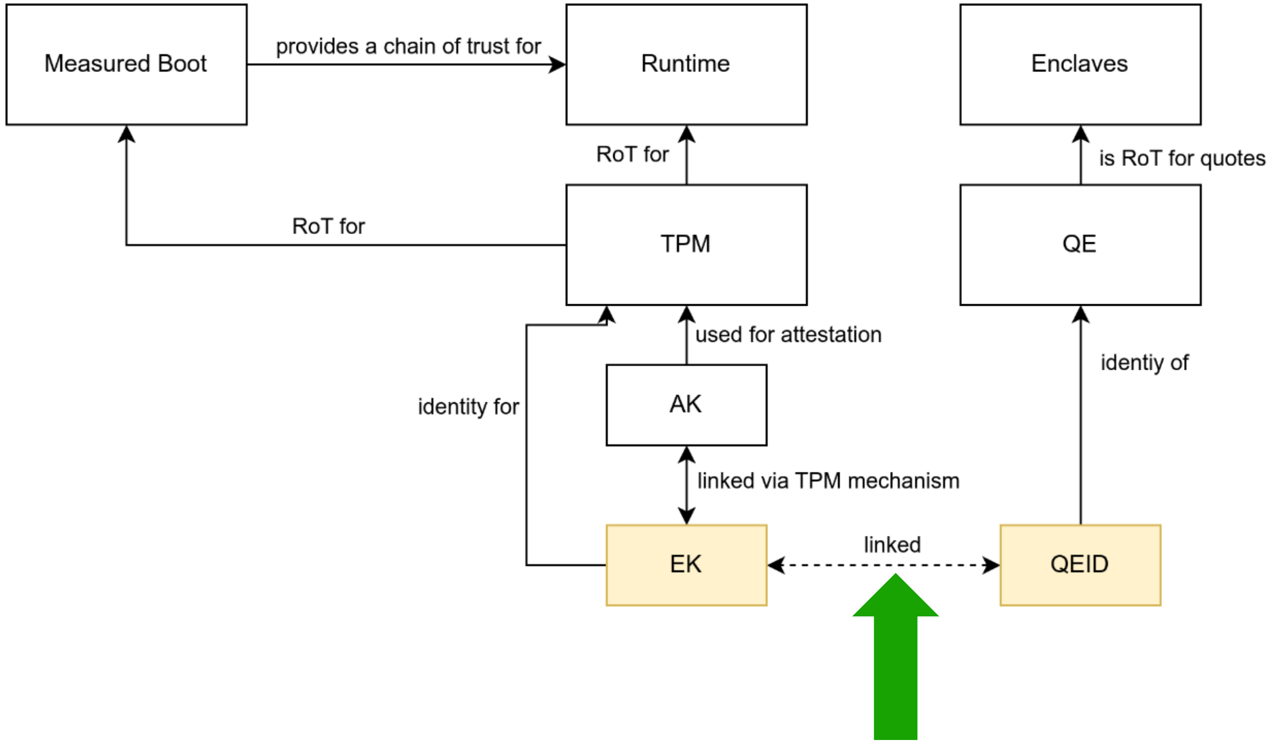


- CPU Enclaves vs TPM

- CPU identity not linked to TPM identity
- CPU integrity not linked to TPM measurements

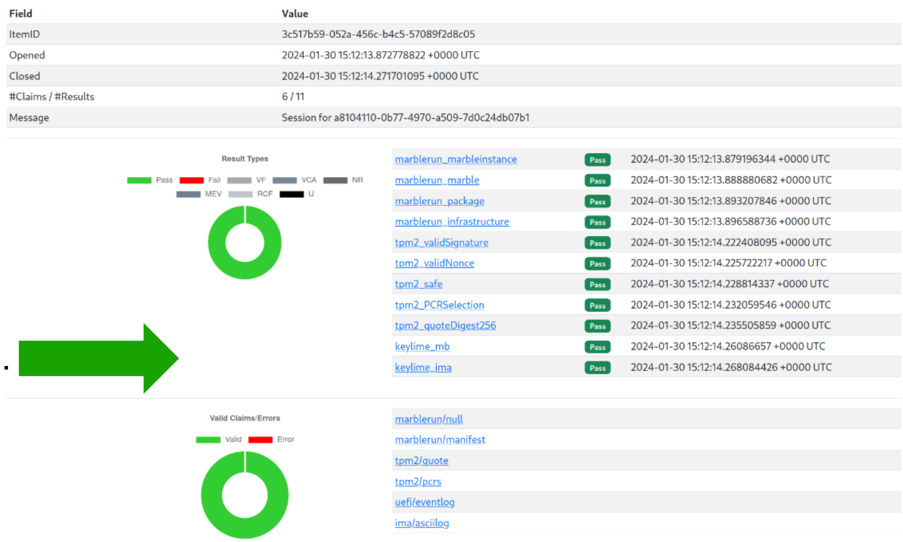


Chains of Trust (4)



CPU identity & integrity part of boot/run-time attestation processes….hard.

…and still unsolved for a general case…MSc/PhDs available



Field	Value
ItemID	3c517b59-052a-456c-b4c5-57089f2d8c05
Opened	2024-01-30 15:12:13.872778822 +0000 UTC
Closed	2024-01-30 15:12:14.271701095 +0000 UTC
#Claims / #Results	6 / 11
Message	Session for a8104110-0b77-4970-a509-7d0c24db07b1

Result Types

🟩 Pass 🟥 Fail ▨ VF ▨ VCA ▨ NR ▨ MEV ▨ RCF ■ U

marblerun_marbleinstance	Pass	2024-01-30 15:12:13.879196344 +0000 UTC
marblerun_marble	Pass	2024-01-30 15:12:13.888880682 +0000 UTC
marblerun_package	Pass	2024-01-30 15:12:13.893207846 +0000 UTC
marblerun_infrastructure	Pass	2024-01-30 15:12:13.896588736 +0000 UTC
tpm2_validSignature	Pass	2024-01-30 15:12:14.222408095 +0000 UTC
tpm2_validNonce	Pass	2024-01-30 15:12:14.225722217 +0000 UTC
tpm2_safe	Pass	2024-01-30 15:12:14.228814337 +0000 UTC
tpm2_PCRSelection	Pass	2024-01-30 15:12:14.232059546 +0000 UTC
tpm2_quoteDigest256	Pass	2024-01-30 15:12:14.235505859 +0000 UTC
keylime_mb	Pass	2024-01-30 15:12:14.26086657 +0000 UTC
keylime_ima	Pass	2024-01-30 15:12:14.268084426 +0000 UTC

Valid Claims/Errors

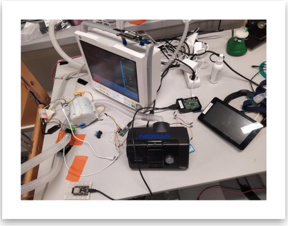
🟩 Valid 🟥 Error

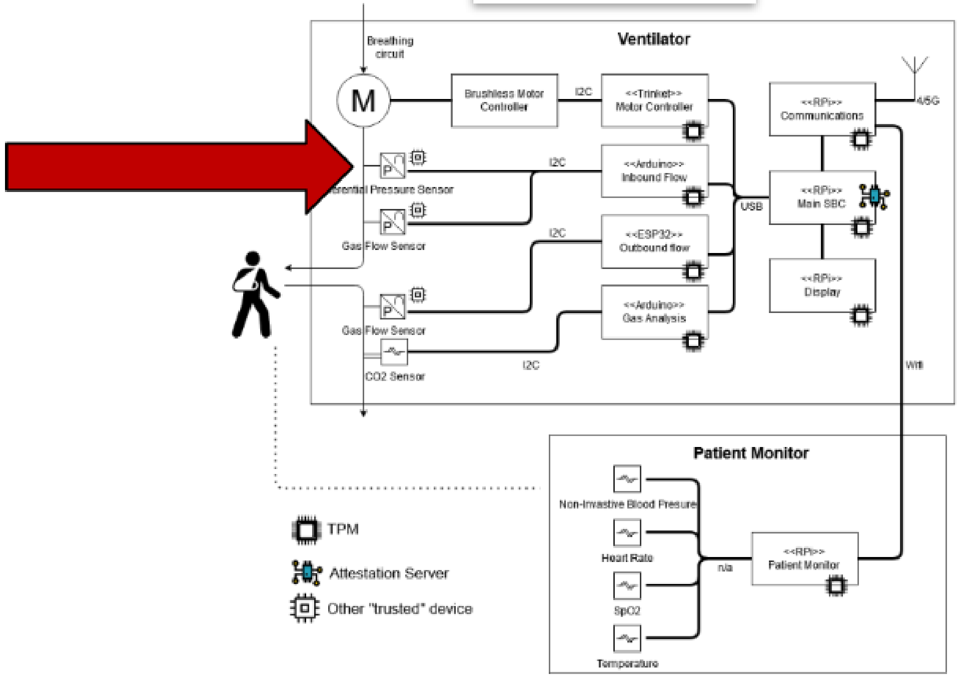
marblerun/null
marblerun/manifest
tpm2/quote
tpm2/pcrs
uefi/eventlog
ima/asciilog

Forensics

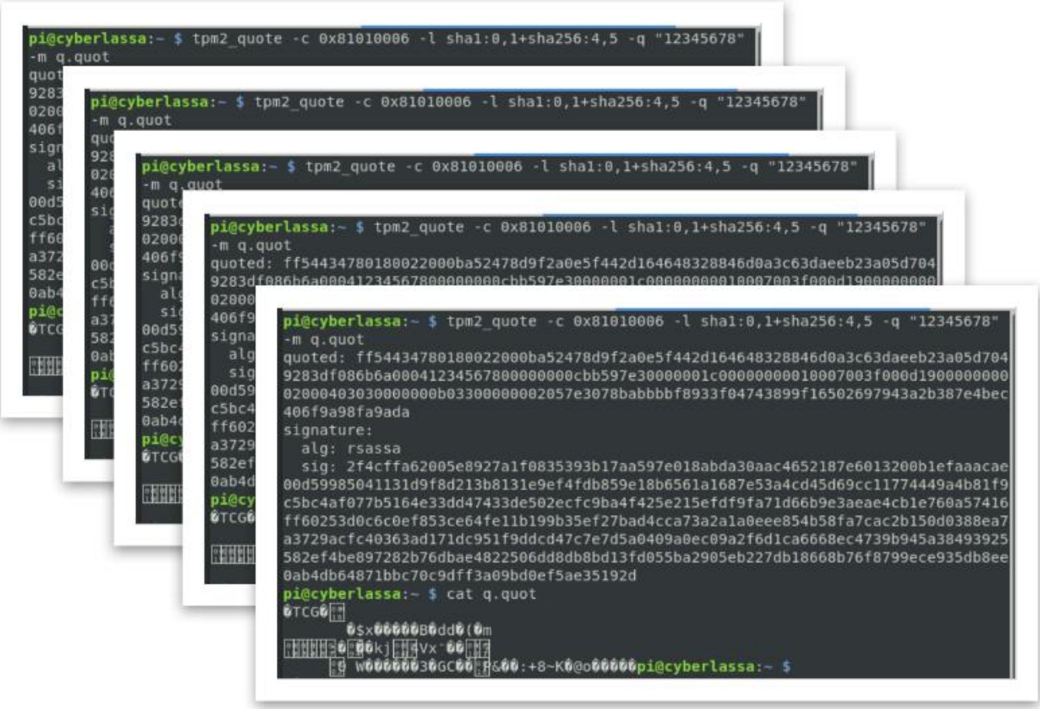
Changes...

If I change this sensor's firmware, identity, configuration...





Quotes...over time



```
pi@cyberlassa:~ $ tpm2_quote -c 0x81010006 -l sha1:0,1+sha256:4,5 -q "12345678"
-m q.quot
quoted: ff54434780180022000ba52478d9f2a0e5f442d164648328846d0a3c63daeeb23a05d704
9283df086b6a00041234567800000000cbb597e30000001c000000000010007003f000d190000000000
0200040303000000b033000000002057e3078babbbbf8933f04743899f16502697943a2b387e4bec
406f9a98fa9ada
signature:
  alg: rsassa
  sig: 2f4cffa62005e8927a1f0835393b17aa597e018abda30aac4652187e6013200b1efaaacae
00d59985041131d9f8d213b8131e9ef4fdb859e18b6561a1687e53a4cd45d69cc11774449a4b81f9
c5bc4af077b5164e33dd47433de502ecfc9ba4f425e215efdf9fa71d66b9e3aeae4cb1e760a57416
ff60253d0c6c0ef853ce64fe11b199b35ef27bad4cca73a2a1a0eee854b58fa7cac2b150d0388ea7
a3729acfc40363ad171dc951f9ddcd47c7e7d5a0409a0ec09a2f6d1ca6668ec4739b945a38493925
582ef4be897282b76dbae4822506dd8db8bd13fd055ba2905eb227db18668b76f8799ece935db8ee
0ab4db64871bbc70c9dff3a09bd0ef5ae35192d
pi@cyberlassa:~ $ cat q.quot
�TCG�▯
      �$x�����B�dd�(�m
▯▯▯▯▯▯�▯��kj▯▯Vx`��▯▯
     ▯�W������3�GC��▯P&��:+8~K�@o�����pi@cyberlassa:~ $
```

How do we understand this?

- Magic number? Type?
- Signed? Verified?
- QualifiedSigner?
- AttestedValue?
- Clock? Reset? Restart? Safe?

Periodic Attestation
Event Based Attestation

What about the history of quotes?

- Clock updating?
- PCRs chaning after updates?
- Which PCRs etc....
- UEFI eventlog, Manufacturer certs, Other roots of trust, other cross-referencing…
- etc...

Analysing Trust Failures

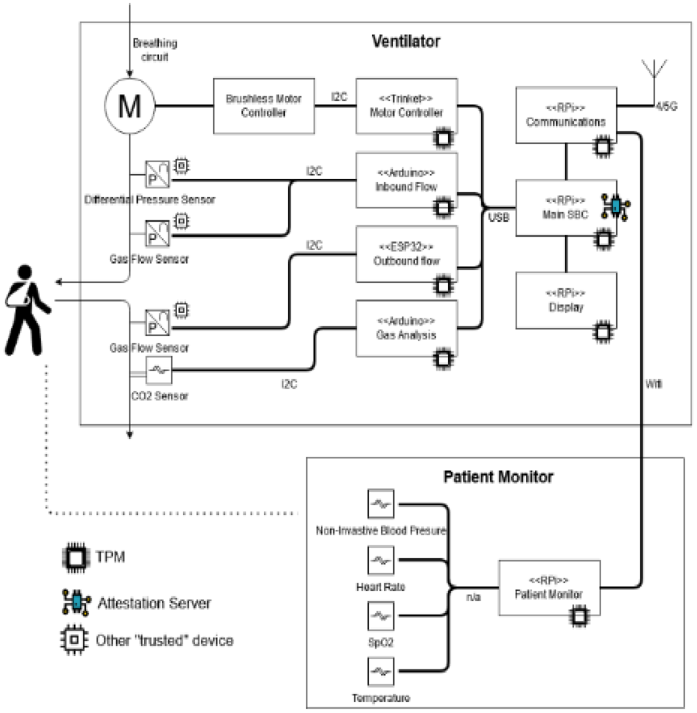
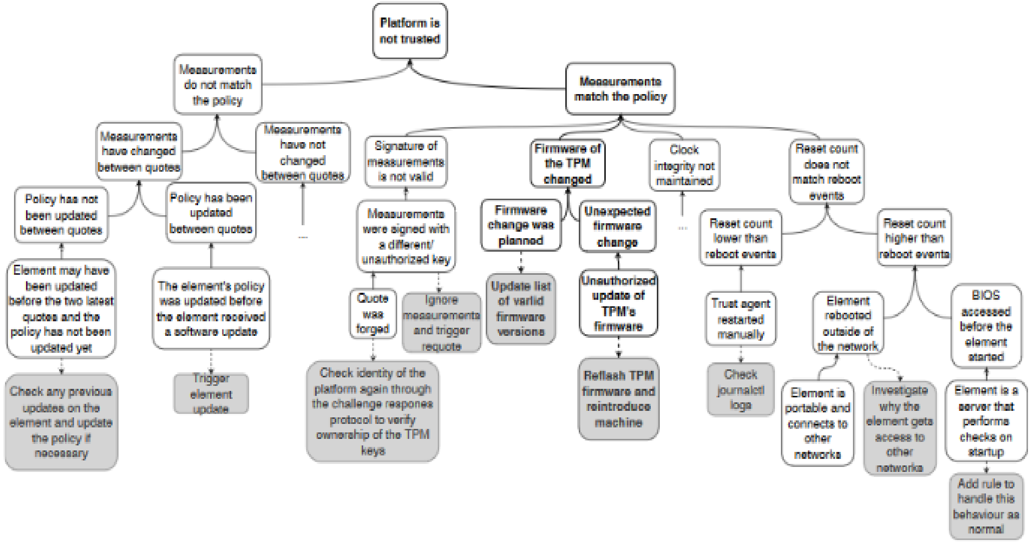


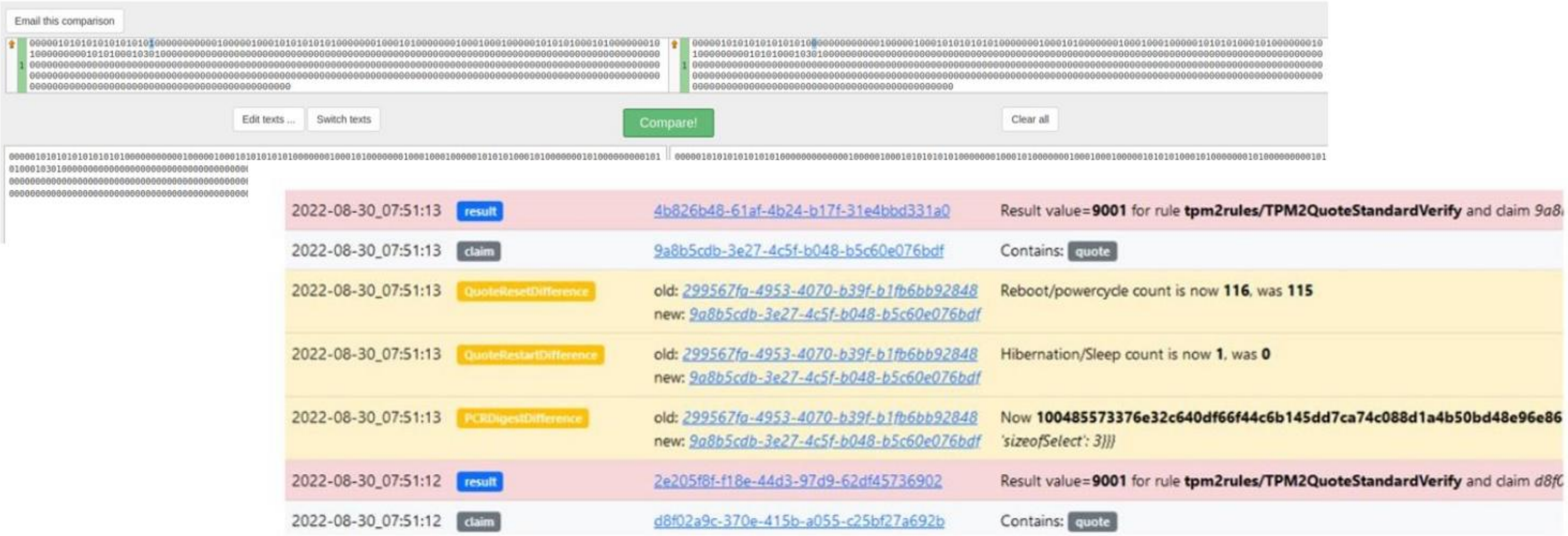
Fig. 1. Ventilator Components

Are we sure that this is a secure failure?



Platform is not trusted
Measurements do not match the policy
Measurements match the policy
Measurements have changed between quotes
Measurements have not changed between quotes
Policy has not been updated between quotes
Policy has been updated between quotes
Element may have been updated before the two latest quotes and the policy has not been updated yet
The element's policy was updated before the element received a software update
Check any previous updates on the element and update the policy if necessary
Trigger element update
...
Signature of measurements is not valid
Measurements were signed with a different/ unauthorized key
Quote was forged
Ignore measurements and trigger requote
Check identity of the platform again through the challenge respones protocol to verify ownership of the TPM keys
Firmware of the TPM changed
Firmware change was planned
Update list of varlid firmware versions
Unexpected firmware change
Unauthorized update of TPM's firmware
Reflash TPM firmware and reintroduce machine
Clock integrity not maintained
...
Reset count does not match reboot events
Reset count lower than reboot events
Trust agent restarted manually
Check journalctl logs
Reset count higher than reboot events
Element rebooted outside of the network
Element is portable and connects to other networks
Investigate why the element gets access to other networks
BIOS accessed before the element started
Element is a server that performs checks on startup
Add rule to handle this behaviour as normal

Real-life Example



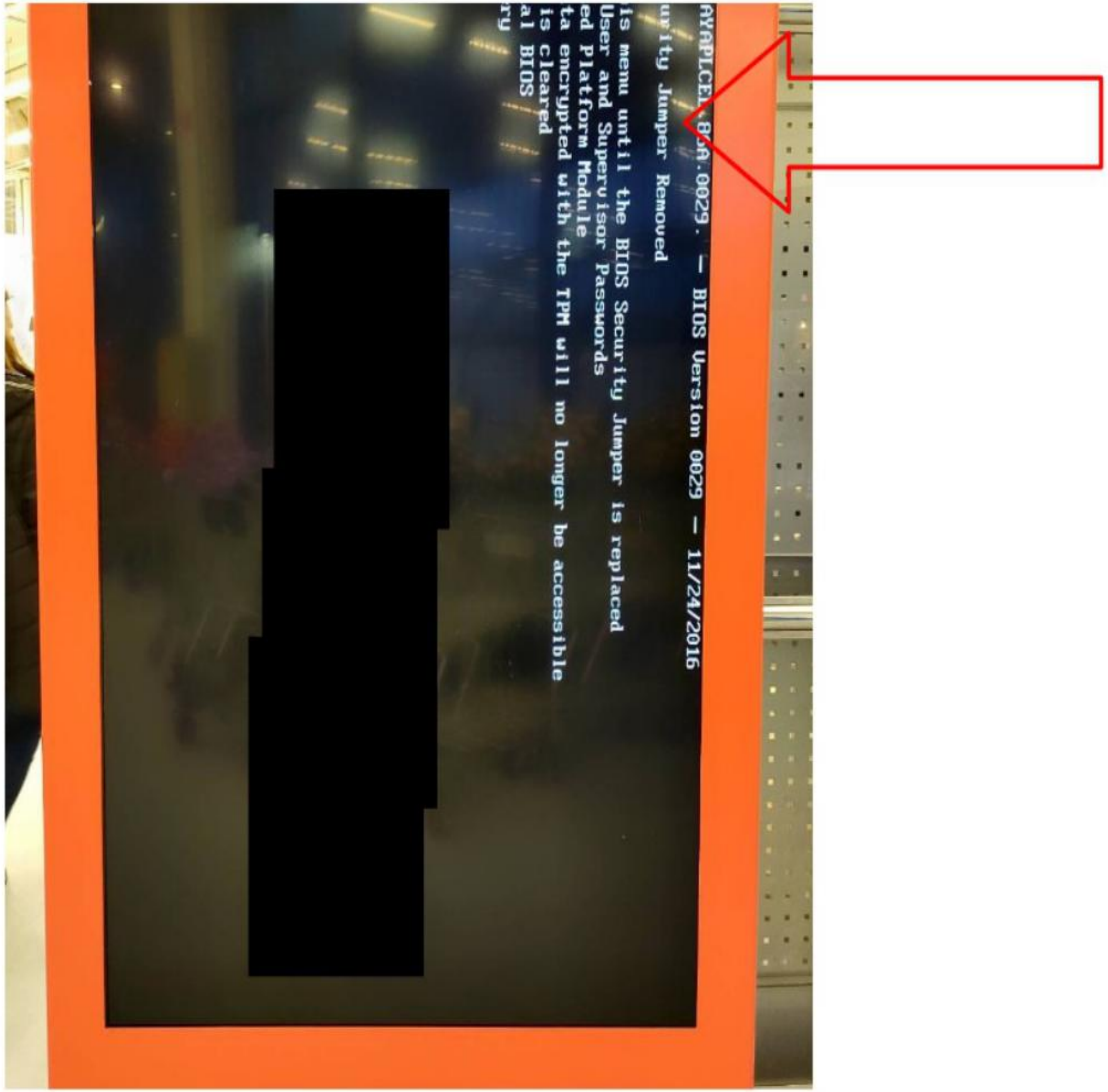
```
000001010101010101010100000000000010000010001010101010100000000100010100000000100010001000000101010100010100000000010
10000000001010100010301000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000
```

2022-08-30_07:51:13	result	4b826b48-61af-4b24-b17f-31e4bbd331a0	Result value=**9001** for rule **tpm2rules/TPM2QuoteStandardVerify** and claim *9a8*
2022-08-30_07:51:13	claim	9a8b5cdb-3e27-4c5f-b048-b5c60e076bdf	Contains: quote
2022-08-30_07:51:13	QuoteResetDifference	old: *299567fa-4953-4070-b39f-b1fb6bb92848* new: *9a8b5cdb-3e27-4c5f-b048-b5c60e076bdf*	Reboot/powercycle count is now **116**, was **115**
2022-08-30_07:51:13	QuoteRestartDifference	old: *299567fa-4953-4070-b39f-b1fb6bb92848* new: *9a8b5cdb-3e27-4c5f-b048-b5c60e076bdf*	Hibernation/Sleep count is now **1**, was **0**
2022-08-30_07:51:13	PCRDigestDifference	old: *299567fa-4953-4070-b39f-b1fb6bb92848* new: *9a8b5cdb-3e27-4c5f-b048-b5c60e076bdf*	Now **100485573376e32c640df66f44c6b145dd7ca74c088d1a4b50bd48e96e86** *'sizeofSelect': 3}}}*
2022-08-30_07:51:12	result	2e205f8f-f18e-44d3-97d9-62df45736902	Result value=**9001** for rule **tpm2rules/TPM2QuoteStandardVerify** and claim *d8f0*
2022-08-30_07:51:12	claim	d8f02a9c-370e-415b-a055-c25bf27a692b	Contains: quote

Roosa Risto (2022). **Forensics from Trusted Computing and Remote Attestation**. MSc Thesis. University of Oulu.

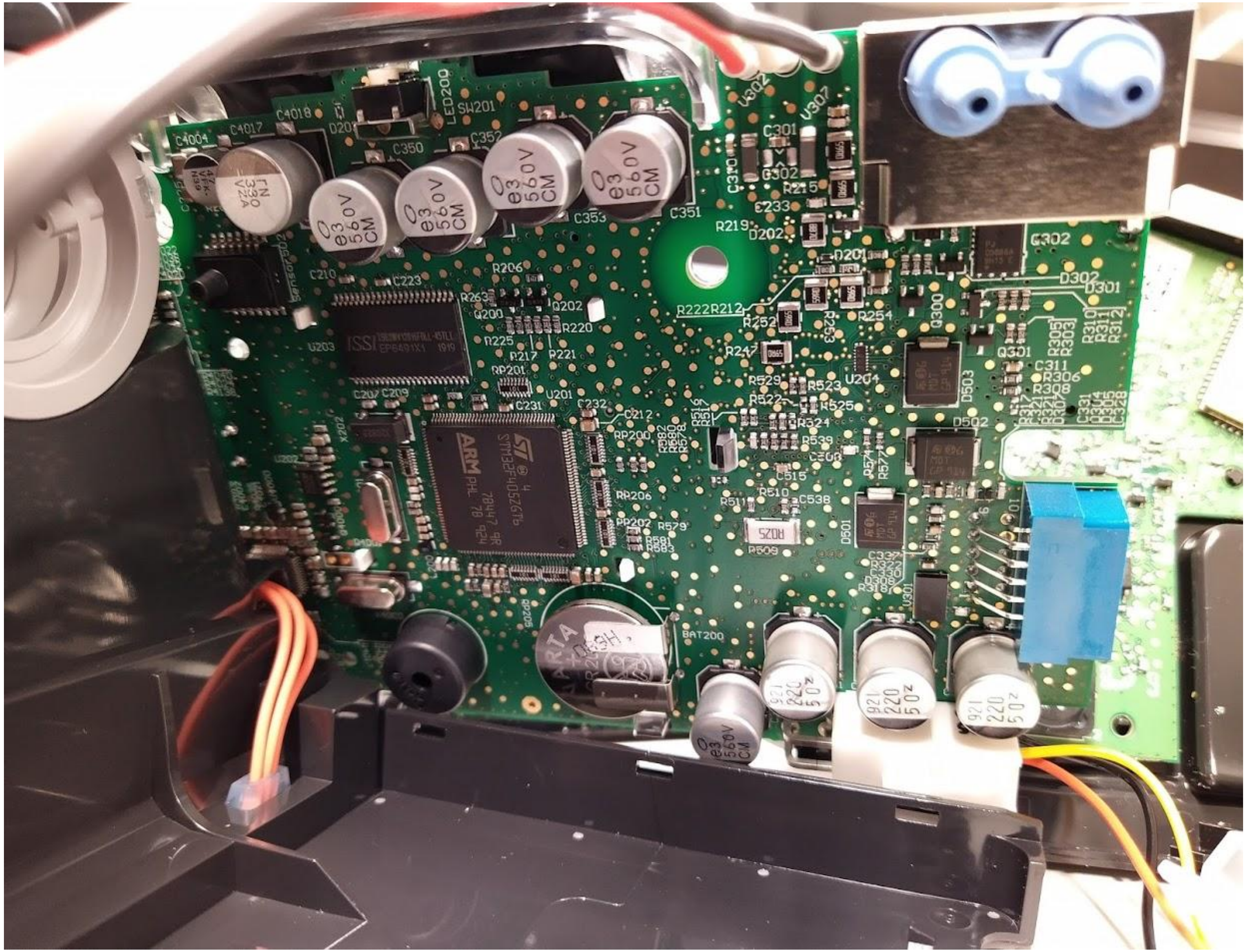
Examples

waterguard
SmartSens
2x
AA 1,5V
CE
A
B



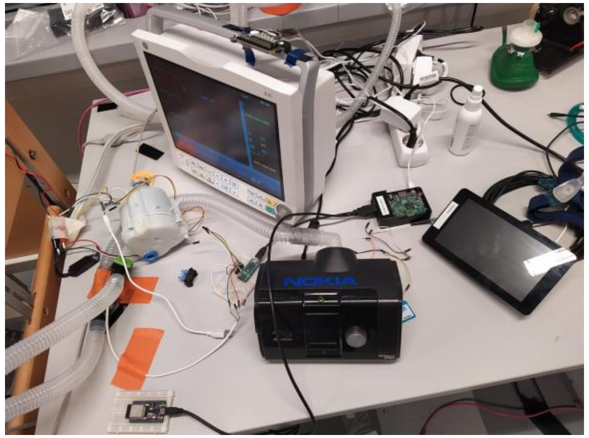
```
AYAPLCEL.86A.0029. — BIOS Version 0029 — 11/24/2016
urity Jumper Removed
is menu until the BIOS Security Jumper is replaced
User and Supervisor Passwords
ed Platform Module
ta encrypted with the TPM will no longer be accessible
is cleared
al BIOS
ry
```

[redacted]


ARM
STM32F405ZGT6
ISSI
VARTA
BAT200
SW201
LED200
560V
220
R025

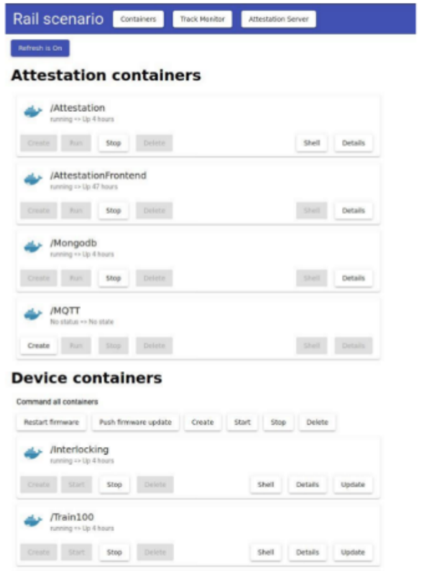
Case Studies

Case Study 1



1. Changing environment
2. Device provisioning vs Device Interactions
3. Real-Time Data Flows
    1. Trusted vs Untrusted flows
    2. Bulk vs Continuous
4. Data Provenance
5. Notarisation and Auditing
6. Trusted Control and Data Plane
7. Remote Working

Case Study 2



Attestation containers

/Attestation
running => Up 4 hours

/AttestationFrontend
running => Up 47 hours

/Mongodb
running => Up 4 hours

/MQTT
No status => No state

Device containers

Command all containers

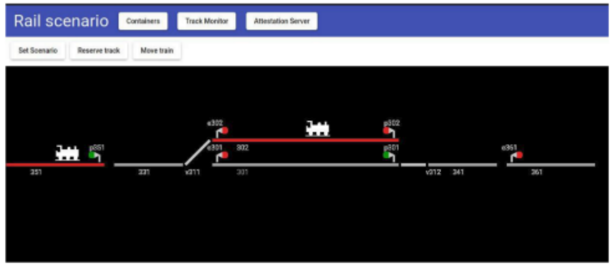
/Interlocking
running => Up 4 hours

/Train100
running => Up 4 hours

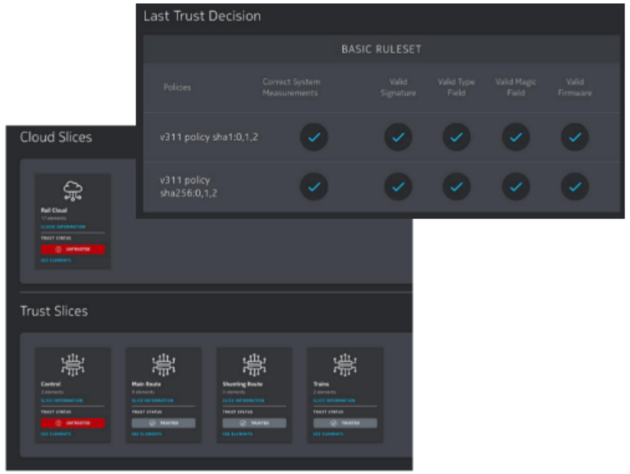
Administration

Attack Injection

Operator Response & Security Procedures



Operator & Simulation Control


Last Trust Decision

BASIC RULESET					
Policies	Correct System Measurements	Valid Signature	Valid Type Field	Valid Magic Field	Valid Firmware
v311 policy sha1:0,1,2	✓	✓	✓	✓	✓
v311 policy sha256:0,1,2	✓	✓	✓	✓	✓

Attestation

- Ronny Bäckman, Ian Oliver, Gabriela Limonta (2020). **Integrity Checking of Railway Interlocking Firmware**. In Proceedings of 15th International Workshop on Dependable Smart Embedded Cyber-Physical Systems and Systems-of-Systems (DECSoS), Lisbon, 15 Sept 2020
- Ronny Bäckman. **Simulating Rail Traffic Management with Trusted Computing**. BSc Thesis. XAMK Kotka Finland. May 2020

Additional Information

Additional Information

IC00AZ56 Trusted and Confidential Computing, 5 op
4 Jan 2026 – 8 March 2026

MSc/BSc thesis topics available

Jane: Experimental Attestation Server
https://github.com/iolivergithub/jane/
Includes: attestation server, trust agent, policy system, example code,

TPM Course (forked from Nokia TPM Course)
https://github.com/iolivergithub/TPMCourse
Includes docker container with TPM simulator, TPM tools, CRIM worksheets!

The End