JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

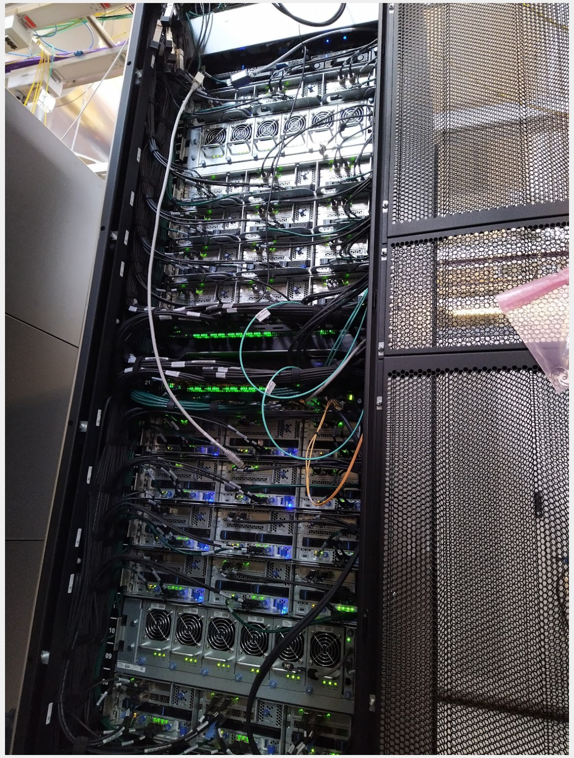
Attesting the Verticals

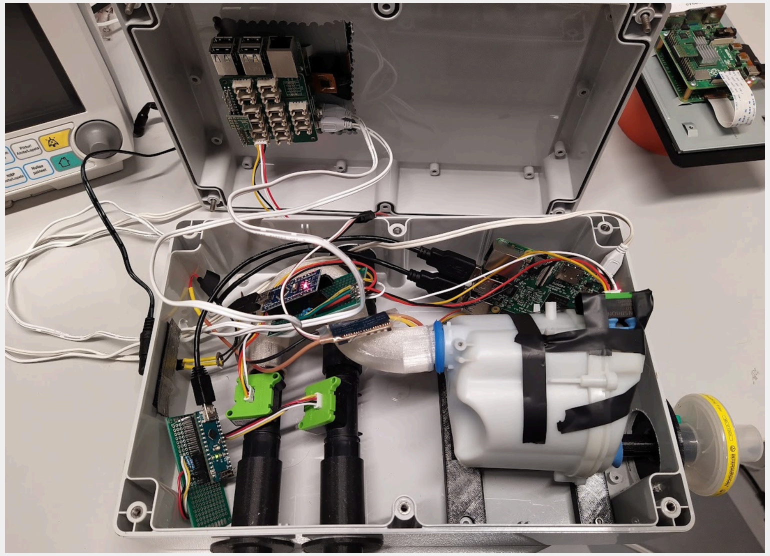
Prof. Ian Oliver

Faculty of IT

University of Jyväskylä, Finland

How we got here…

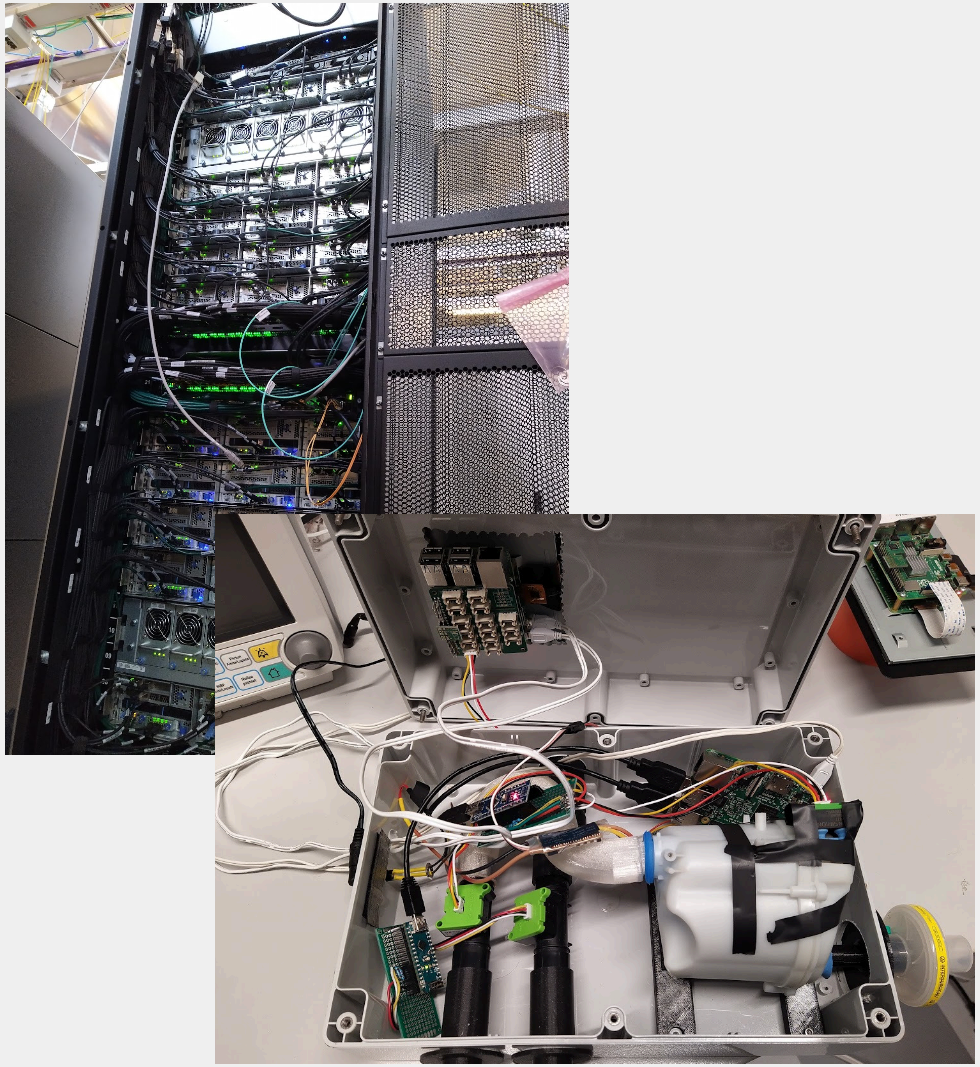




Attesting these to attesting these…

…while not forgetting about the rest of the World…

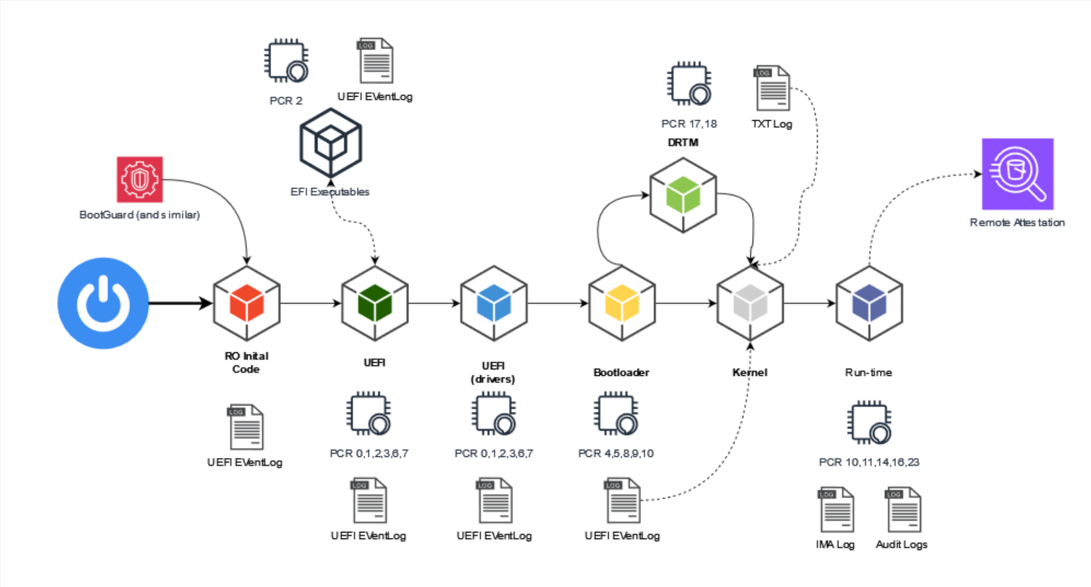
How we got here…



The internet of **attestable** things

Attestable?
Trustable?

Nokia Attestation Engine
- TPM2, VNF, Containers…



How we got here…

WhatTheXYZamIdoing.txt

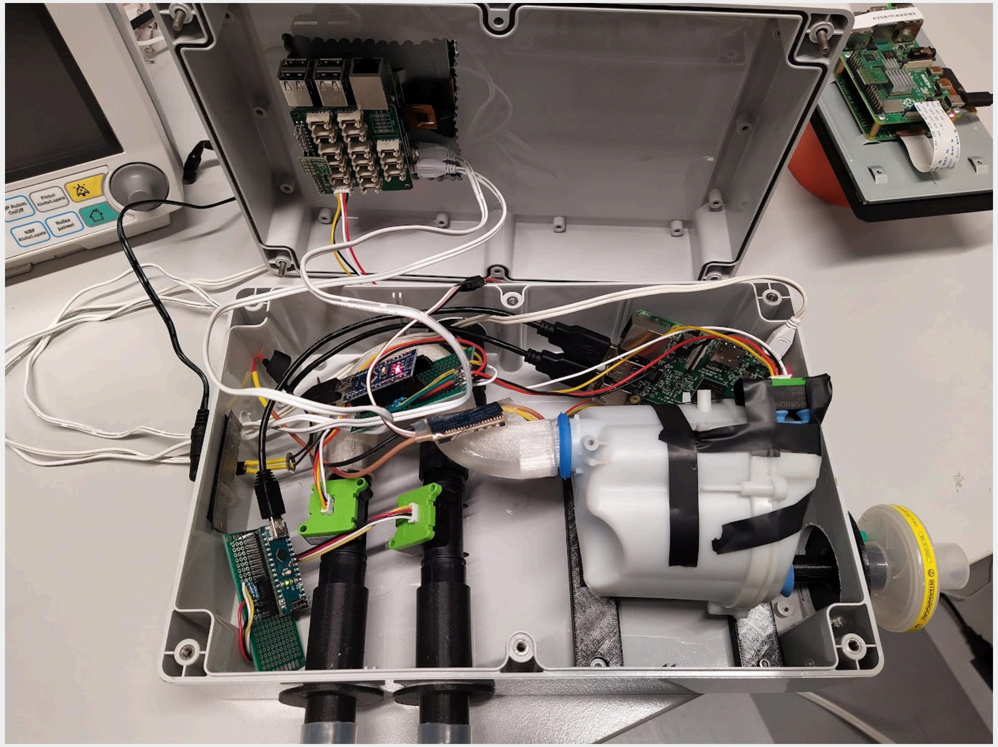
How we got here…

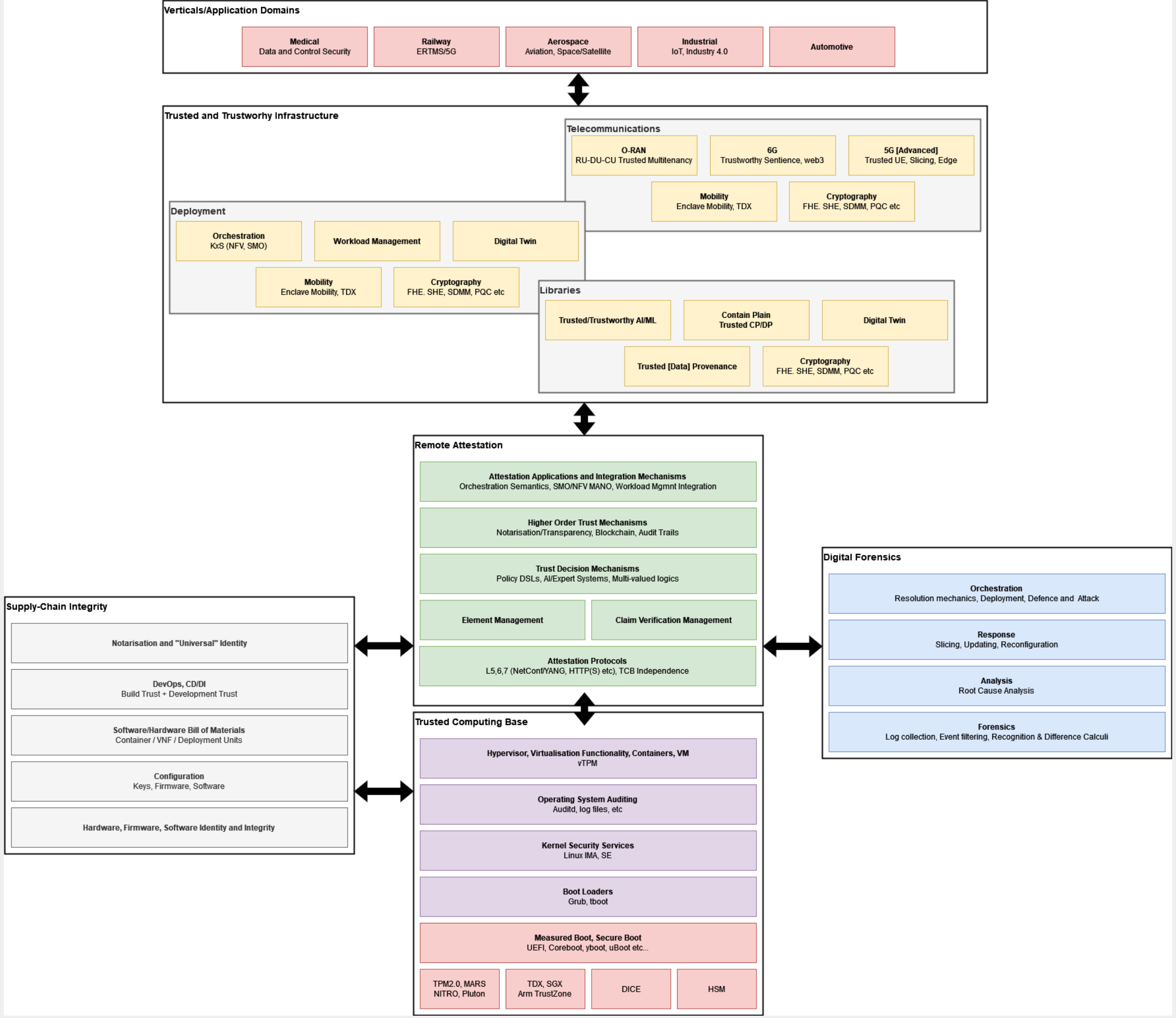
Surprisingly this isn’t enough….

Verticals

- Railways, Medical (our first targets)
  - Industry 4.0/IoT/Edge, but you might kill someone
  - Extra requirements (apart from the safety thing), eg: latency, accuracy, resiliency etc.
  - Not just devices, but “trusted data/control plane”
  - At lot of things need attesting
  - End-to-End
  - Integration with Infrastructure, eg: 5G/6G
  - Interesting failure modes:

Big Picture





Verticals/Application Domains

Medical
Data and Control Security

Railway
ERTMS/5G

Aerospace
Aviation, Space/Satellite

Industrial
IoT, Industry 4.0

Automotive

Trusted and Trustworhy Infrastructure

Telecommunications

O-RAN
RU-DU-CU Trusted Multitenancy

6G
Trustworthy Sentience, web3

5G [Advanced]
Trusted UE, Slicing, Edge

Mobility
Enclave Mobility, TDX

Cryptography
FHE. SHE, SDMM, PQC etc

Deployment

Orchestration
KxS (NFV, SMO)

Workload Management

Digital Twin

Mobility
Enclave Mobility, TDX

Cryptography
FHE. SHE, SDMM, PQC etc

Libraries

Trusted/Trustworthy AI/ML

Contain Plain
Trusted CP/DP

Digital Twin

Trusted [Data] Provenance

Cryptography
FHE. SHE, SDMM, PQC etc

Remote Attestation

Attestation Applications and Integration Mechanisms
Orchestration Semantics, SMO/NFV MANO, Workload Mgmnt Integration

Higher Order Trust Mechanisms
Notarisation/Transparency, Blockchain, Audit Trails

Trust Decision Mechanisms
Policy DSLs, AI/Expert Systems, Multi-valued logics

Element Management

Claim Verification Management

Attestation Protocols
L5,6,7 (NetConf/YANG, HTTP(S) etc), TCB Independence

Supply-Chain Integrity

Notarisation and "Universal" Identity

DevOps, CD/DI
Build Trust + Development Trust

Software/Hardware Bill of Materials
Container / VNF / Deployment Units

Configuration
Keys, Firmware, Software

Hardware, Firmware, Software Identity and Integrity

Digital Forensics

Orchestration
Resolution mechanics, Deployment, Defence and Attack

Response
Slicing, Updating, Reconfiguration

Analysis
Root Cause Analysis

Forensics
Log collection, Event filtering, Recognition & Difference Calculi

Trusted Computing Base

Hypervisor, Virtualisation Functionality, Containers, VM
vTPM

Operating System Auditing
Auditd, log files, etc

Kernel Security Services
Linux IMA, SE

Boot Loaders
Grub, tboot

Measured Boot, Secure Boot
UEFI, Coreboot, yboot, uBoot etc...

TPM2.0, MARS
NITRO, Pluton

TDX, SGX
Arm TrustZone

DICE

HSM

Smaller Picture

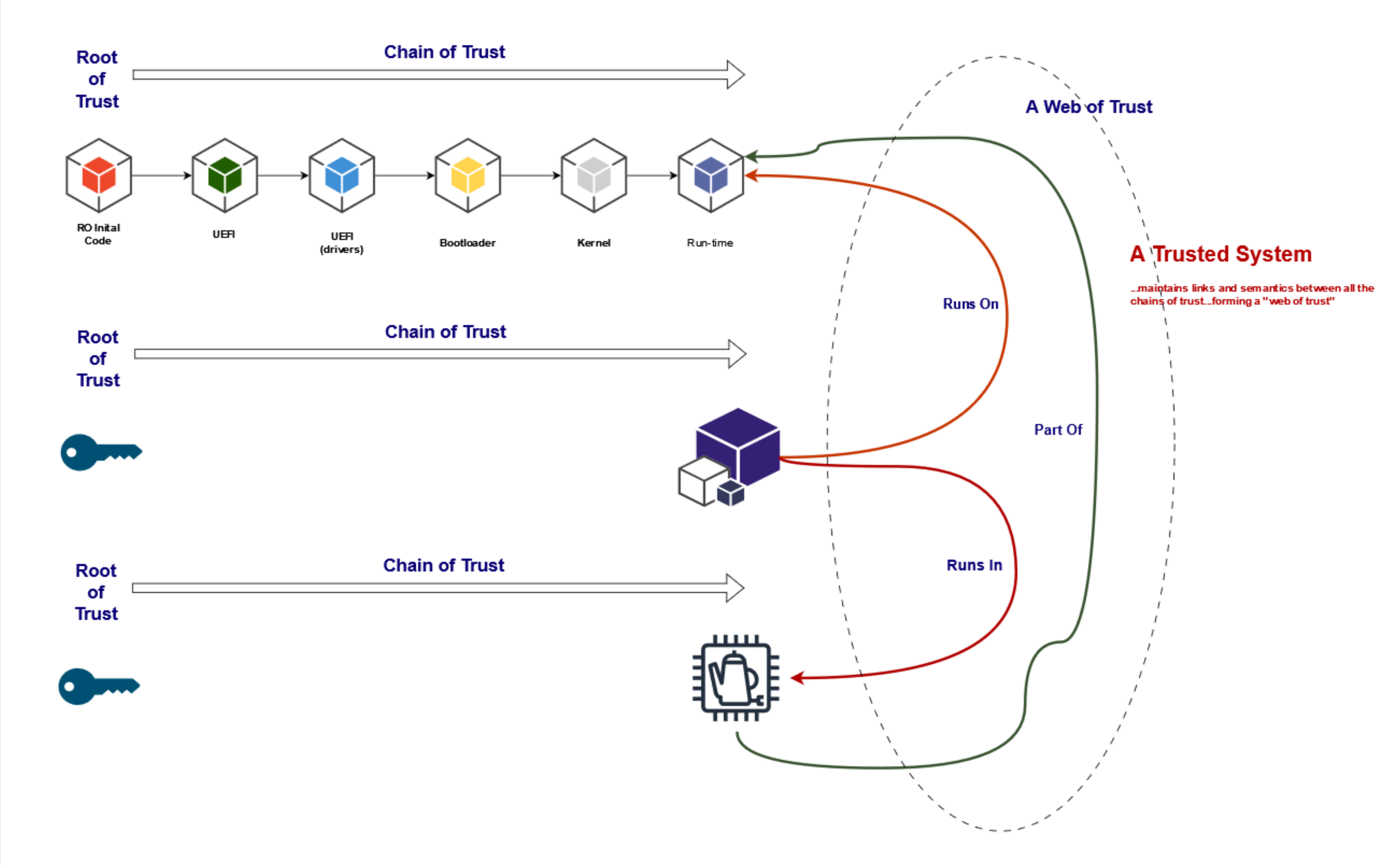
CRTM->Chain of Trust

Chains of Trust

Cross-referencing

Web of Trust

Webs of Trust



Questions Arising

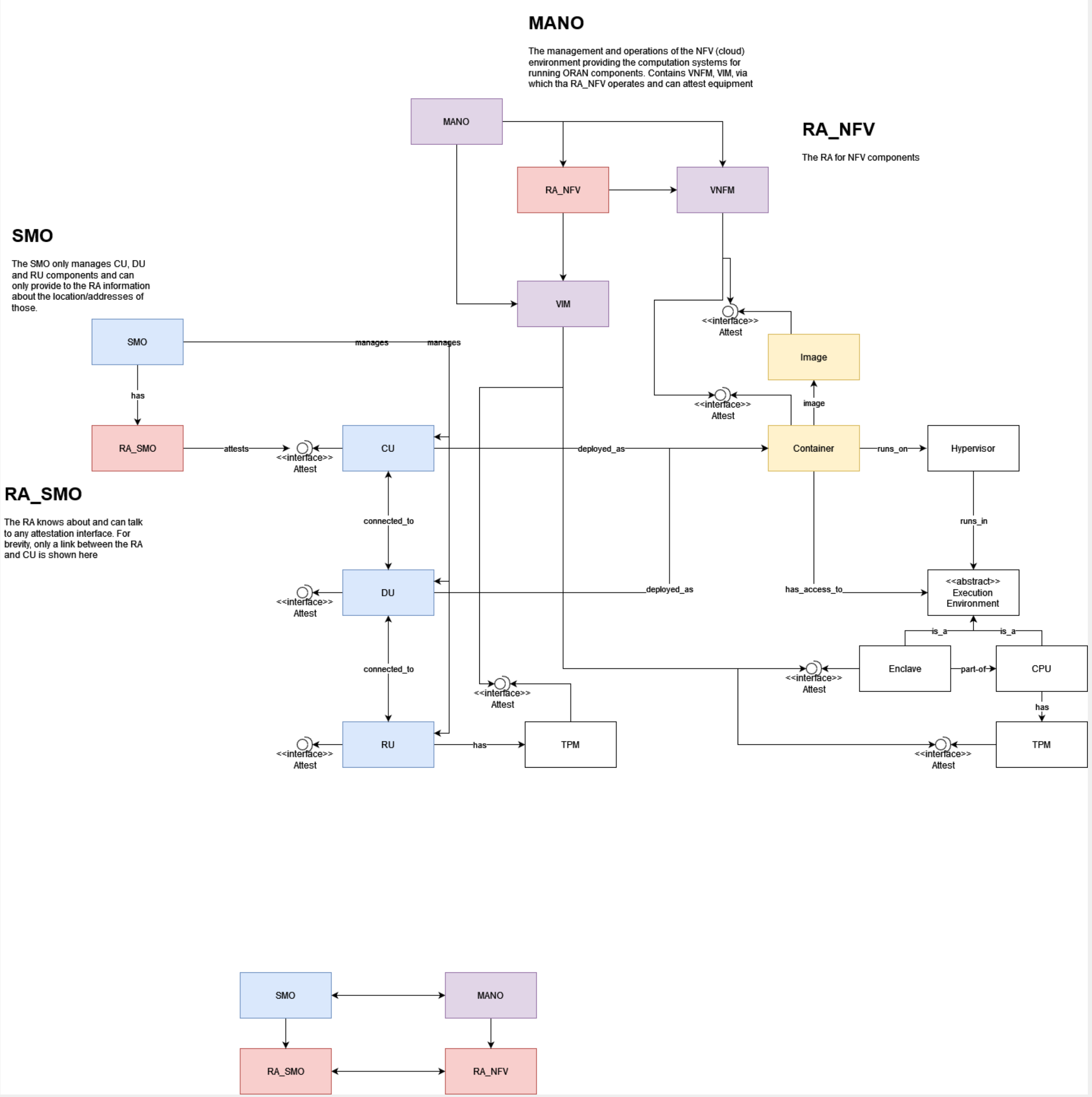
- What other structures exist? Higher-order webs of trust? Systems thinking
- A formal, ontological model
- **SYSTEMS THINKING**
- What other trust relationships are there?
- What kinds of trust do we want?
- Logical reasoning
- Trust is not binary….subjective, time based…
- What are the mathematics of trust?
- Does it differentiate/integrate over time, d_trust/dt ?
- Quantum trust?
- Risk and Game Theory

$$\begin{tikzcd}
Element \arrow[r, "measure"] \arrow[rr, dashed, bend right, "attestable"'] \arrow[rrr, dashed, bend right=40, "trustworthy"'] & Measure \arrow[r, "attest"] & Claim \arrow[r, "verify"] & Result \arrow[r, "decide"] & Decision
\end{tikzcd}$$

$$\begin{tikzcd}
TrustedElement \arrow[r] \arrow[d, tail] & 1 \arrow[d, "true"] \\
Element \arrow[r, dashed, "\phi_{Decision}"'] & Decision
\end{tikzcd}$$

OpenRAN (ORAN)

- O-RU runs on hardware (gNB)
- O-DU/O-CU are “generally” container based on cloud
- SMO contains remote attestation server
- O-DU/O-CU communicate with and run on NFV environments
- 5G core runs within an NFV environment
- NFV has MANO
- Mutli-vendor
- Exercise: trusted(X), trusts(X,Y), runson(X)
- If a gNB becomes untrusted, what does this means
- Webs of trust, eg: 5G core vs O-Cloud



MANO

The management and operations of the NFV (cloud) environment providing the computation systems for running ORAN components. Contains VNFM, VIM, via which tha RA_NFV operates and can attest equipment

RA_NFV

The RA for NFV components

SMO

The SMO only manages CU, DU and RU components and can only provide to the RA information about the location/addresses of those.

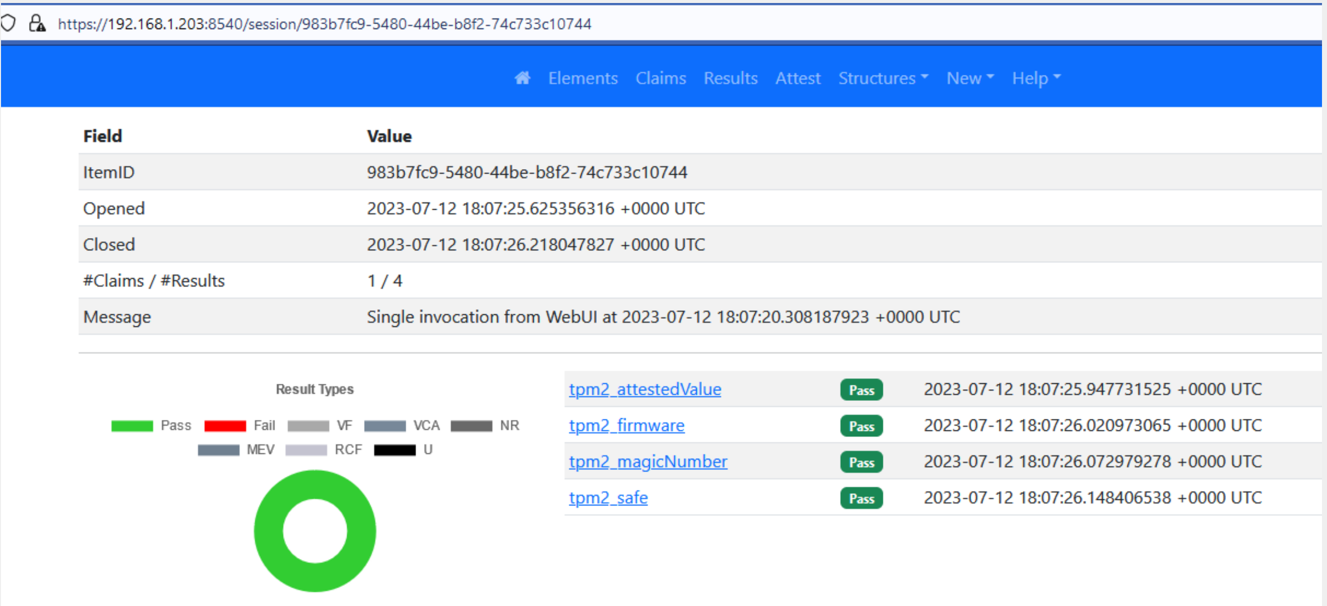
RA_SMO

The RA knows about and can talk to any attestation interface. For brevity, only a link between the RA and CU is shown here

Next Steps

Ontologies for trust are required for formalisation - more powerful models
Other structures: cross-referencing, webs, multiple chains of trust
Better definitions of “trusted” -> Systems Thinking/Engineering
Metrics a_0 | untrusted > + a_1 | trusted > + a_2 | eh? > + … a_n | ¯_(ツ)_/ >
TPMs and Enclaves are not a full solution
Tooling (Jane, was NAE). https://gitlab.jyu.fi/ijoliver/jane. <- DEMO AVAILABLE NOW
Interesting cases: Medical, Defence, Aerospace
Forensics, Failure Modes and Responses

- Borger, Ravidas, Turcanu - Container Trust
- Backman - Railway
- Jatkola - Blockchain, supply-chain, data trust
- Thore - Enclaves + TPM + Containers
- Kuure -> ORAN
- David -> Nuclear
- Risto, Sunden -> Digital Forensics



https://192.168.1.203:8540/session/983b7fc9-5480-44be-b8f2-74c733c10744

Field	Value
ItemID	983b7fc9-5480-44be-b8f2-74c733c10744
Opened	2023-07-12 18:07:25.625356316 +0000 UTC
Closed	2023-07-12 18:07:26.218047827 +0000 UTC
#Claims / #Results	1 / 4
Message	Single invocation from WebUI at 2023-07-12 18:07:20.308187923 +0000 UTC

tpm2_attestedValue	Pass	2023-07-12 18:07:25.947731525 +0000 UTC
tpm2_firmware	Pass	2023-07-12 18:07:26.020973065 +0000 UTC
tpm2_magicNumber	Pass	2023-07-12 18:07:26.072979278 +0000 UTC
tpm2_safe	Pass	2023-07-12 18:07:26.148406538 +0000 UTC

PhD Positions available

- trusted/confidential computing
- quantum trust