NOKIA Bell Labs

Integrating Trust and Attestation in 5G, O-RAN and Edge Computing

Ian Oliver

ETSI Security Week 2022

3 October 2022

Trusted Computing Revisited

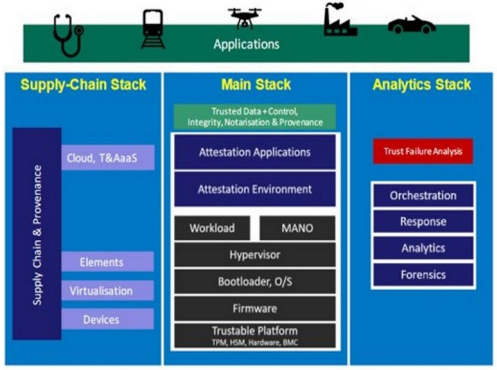
VNFs, VM Images, Containers, Clouds, Core, Edge, MEC, IoT, Sensors

Attestable? **Trustable?**

Object ⟶ Measurement ⟶ Claim ⟶ Result ⟶ Decision

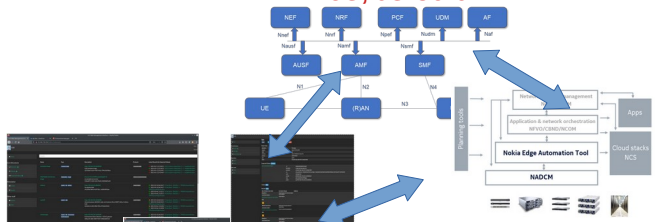
Trusted Computing “Architecture”

Case Studies:
Medical, Railways

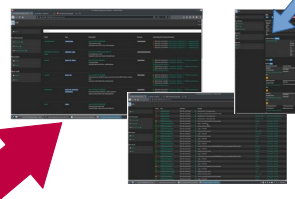


Trust Stack

5G, 6G Core



Deployment



Integration:
Remote Attestation Services
MANO, 5G Core, 6G Core
Attestation Applications, Data/Control Provenance

Montoring, Forensics and Analytics

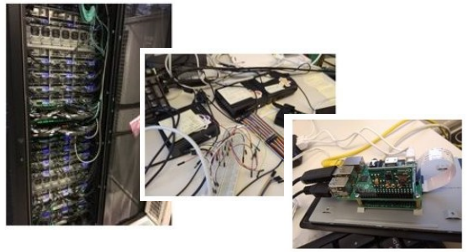
Conmtainer Identity/Integrity:
root-of-build-trust, provenance & lifecycle

kubernetes docker

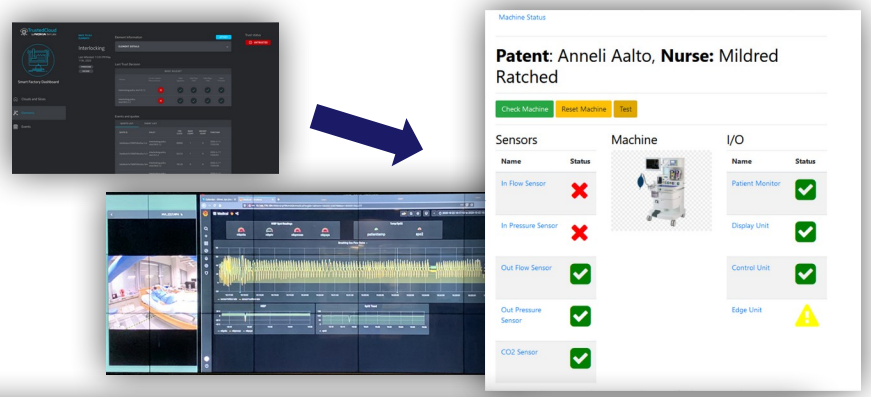
Notarisation:
TransparencyLog,
Blockchain, etc

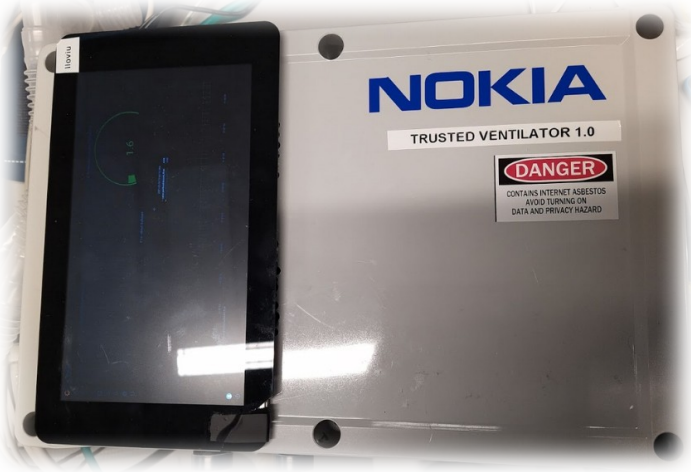
Supply-Chain/Load/Run-time Integrity:
Container Trust,
Cloud/Edge MANO Orchestration
Trusted Containers + Trusted Provenance of Containers

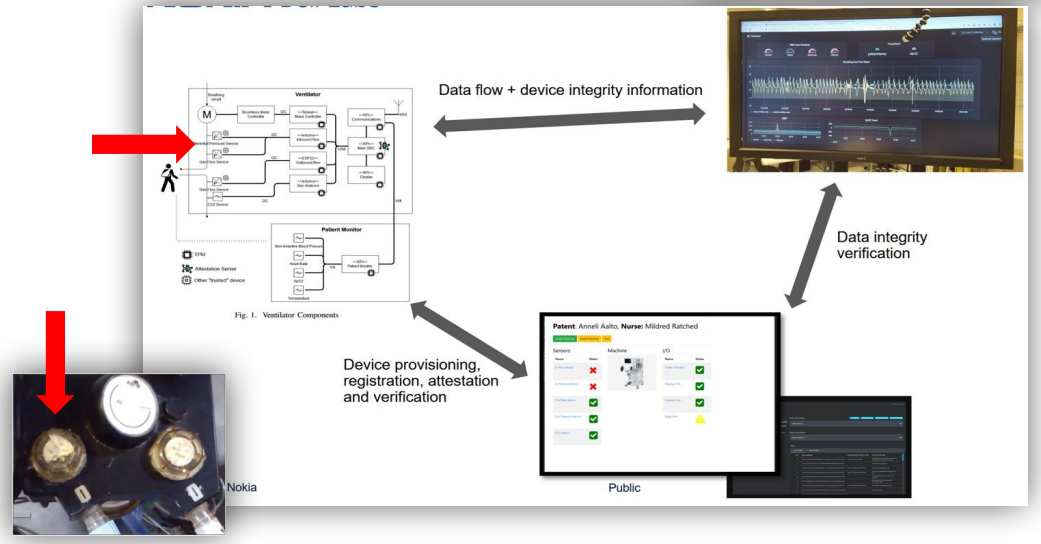
Deployment:
Servers, IoT, Edge, Far-Edge, UE, Sensors
Firmware supply-chain questions?



Trusted Computing: Medical Systems



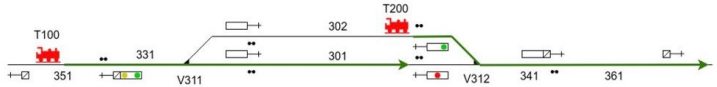




Trusted Computing: Railways

Trust Slices/Domains:

Low Speed Section → Passing Section → High Speed Section



Trust Slice Verification Rule Sets:

Core/Basic LoA

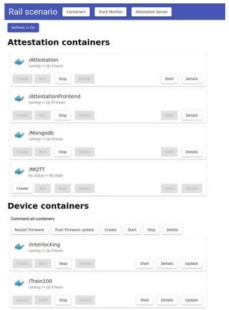
TPM 2.0 Quote Rules	Attestation Timeliness Rules	History/Assurance Rules
Is it a quote?	Did the device respond to the quote request in a timely manner?	
Signed and matches the qualified signer?	Did the device process the quote request in a timely manner?	
Nonce + additional data correct?		
Does the attested value match the known good value?	-	
Is the device running the correct firmware?	-	-
Has the device been rebooted?	-	-
Is the clock increasing correctly?	-	-
	-	-

Intermediate LoA

TPM 2.0 Quote Rules	Attestation Timeliness Rules	History/Assurance Rules
Is it a quote?	Did the device respond to the quote request in a timely manner?	
Signed and matches the qualified signer?	Did the device process the quote request in a timely manner?	
Nonce + additional data correct?	Was the response consistent with network latencies (where applicable)?	
Does the attested value match the known good value?	-	
Is the device running the correct firmware?	-	-
Has the device been rebooted?	-	-
Is the clock increasing correctly?	-	-
Was the device shutdown correctly?	-	-

Critical LoA

TPM 2.0 Quote Rules	Attestation Timeliness Rules	History/Assurance Rules
Is it a quote?	Did the device respond to the quote request in a timely manner?	Has the device changed in any way since the last quote?
Signed and matches the qualified signer?	Did the device process the quote request in a timely manner?	...and for what properties?
Nonce + additional data correct?	Was the response consistent with network latencies (where applicable)?	Does the device verify against the selected rules for its LoA ?
Does the attested value match the known good value?	-	What set of PCRs is required for a minimum LoA?
Is the device running the correct firmware?	-	-
Has the device been rebooted?	-	-
Is the clock increasing correctly?	-	-
Was the device shutdown correctly?	-	-

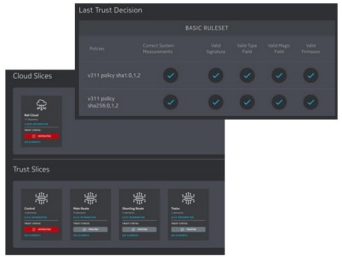


Administration

Attack Injection

Operator Response & Security Procedures

Operator & Simulation Control



Attestation

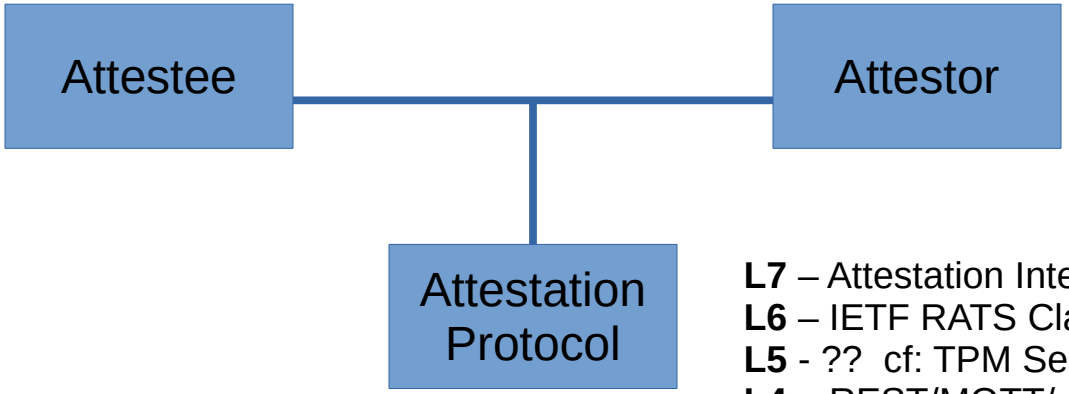
Communication Infrastructure

Device ID
Signalling Devices as 5G/6G UEs
Integrity and Identity of Components
Control and Data Plane Trust/Provenance

Eurobalise picture: Public Domain, Wikipedia https://commons.wikimedia.org/wiki/File:Siemens_Eurobalise.jpg 15 June 2004
Train Picture: © 2021 Ian Oliver

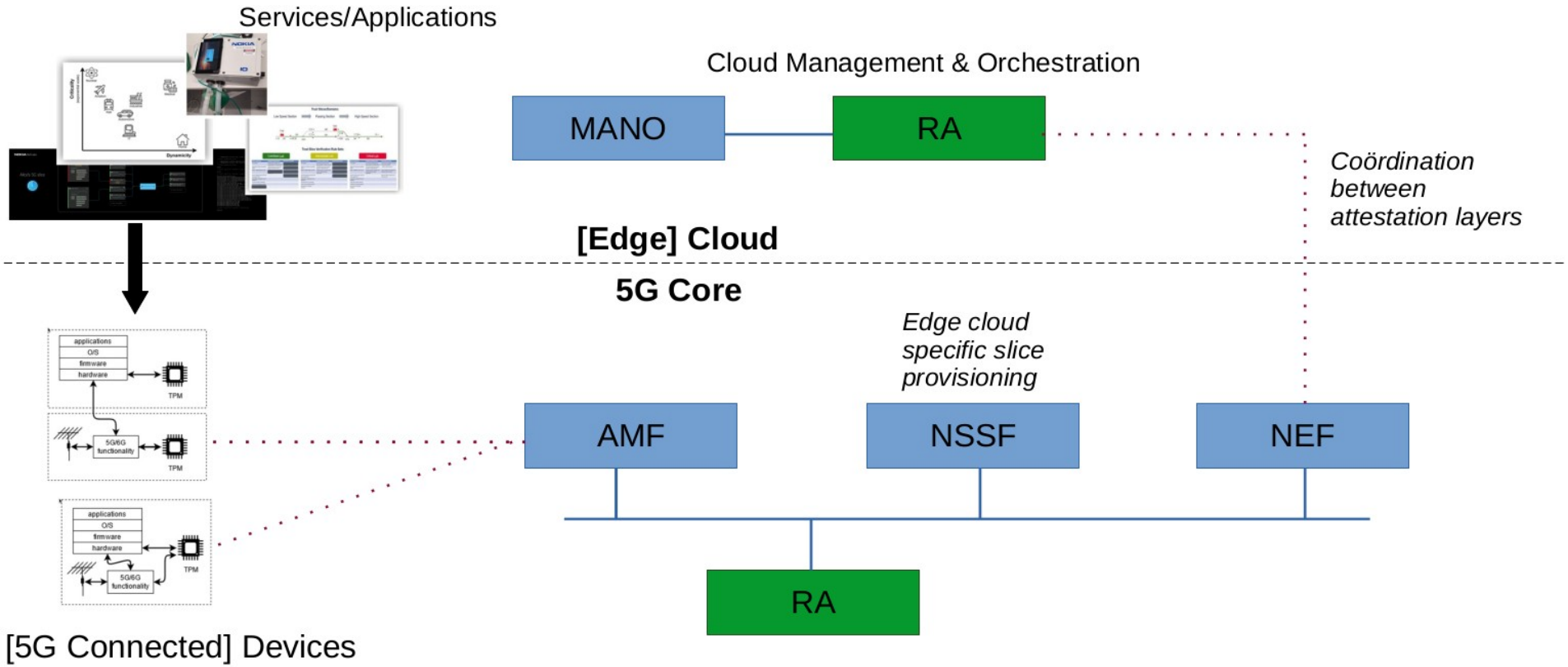
Generic Model

H/W TPM 2.0
CNF/VNF
Other...

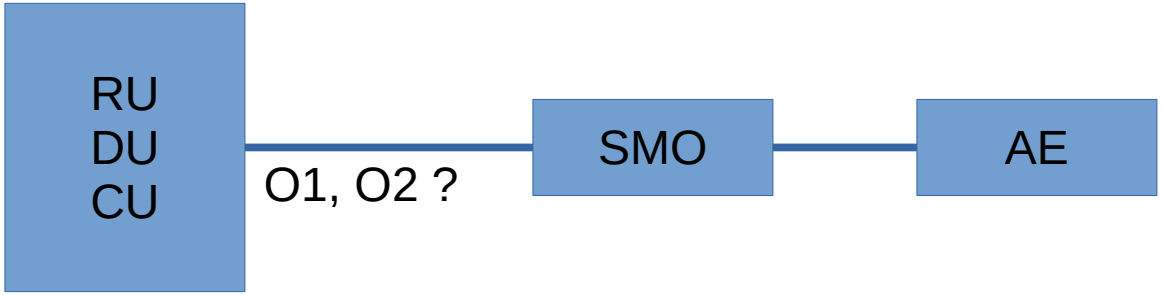


L7 – Attestation Intents
L6 – IETF RATS Claims
L5 - ?? cf: TPM Sessions?
L4 – REST/MQTT/... over IP/RAN7...

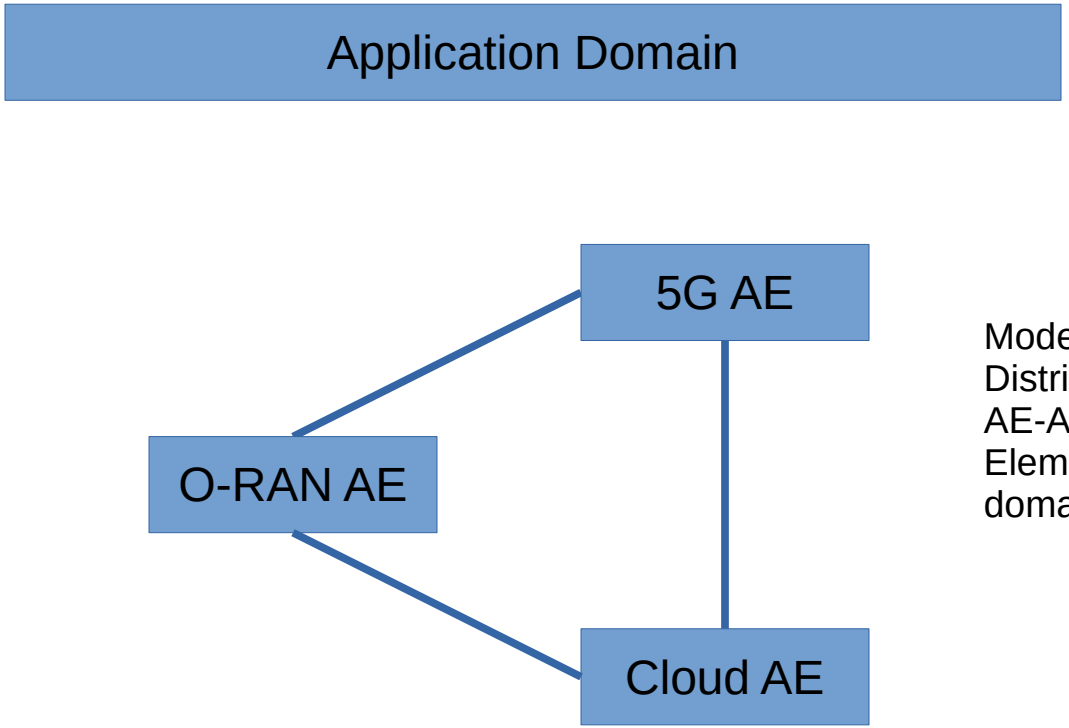
5G



O-RAN

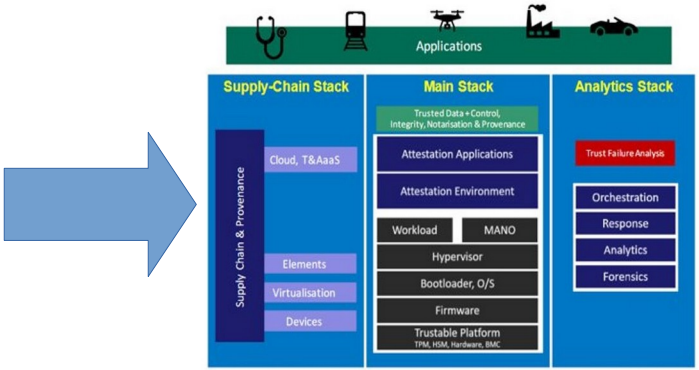


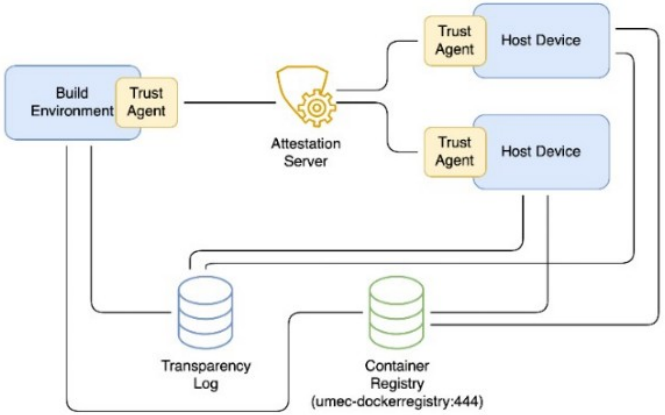
O-RAN+5G+Cloud+Domain



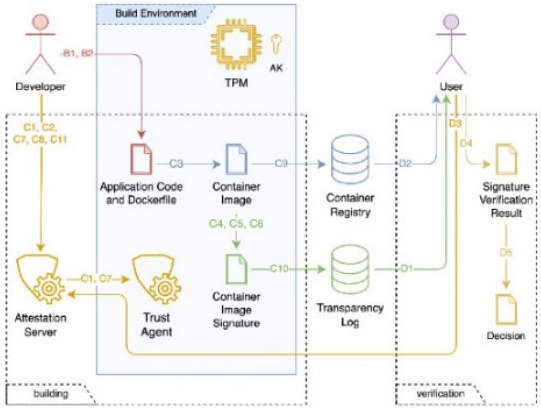
Model of Trust?
Distribution of Responsibilities
AE-AE Protocols
Element Identity across infrastructure domains and application domains

Supply-Chain, CD/CI, DevOps



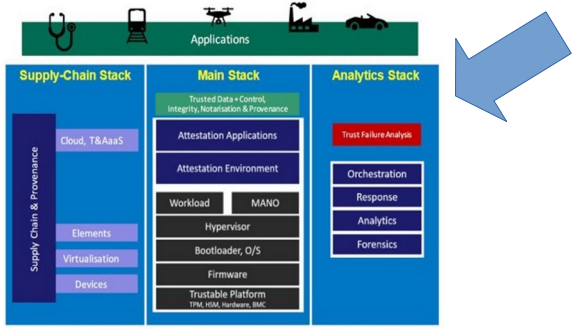


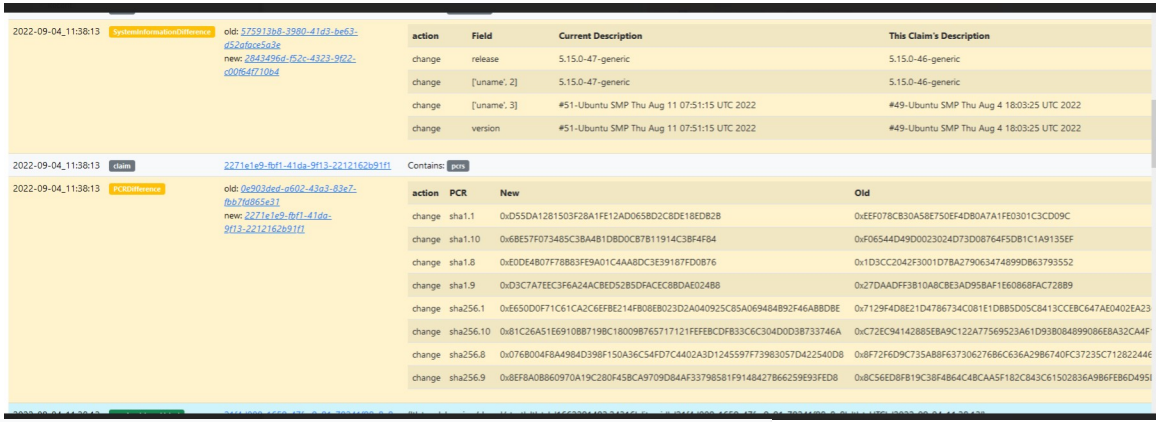
[Core,Edge,Far-Edge] RAS Architecture

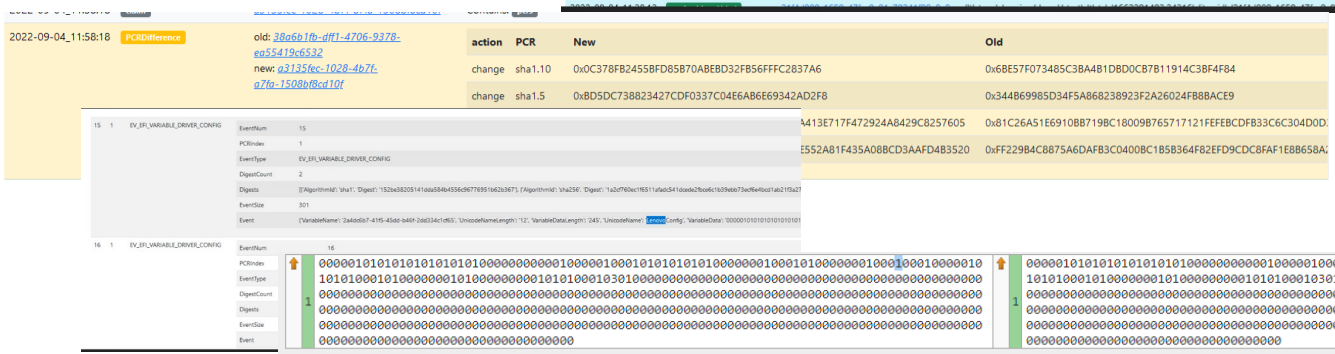


Container Attestation

Forensics-Analytics-Response-Orchestration



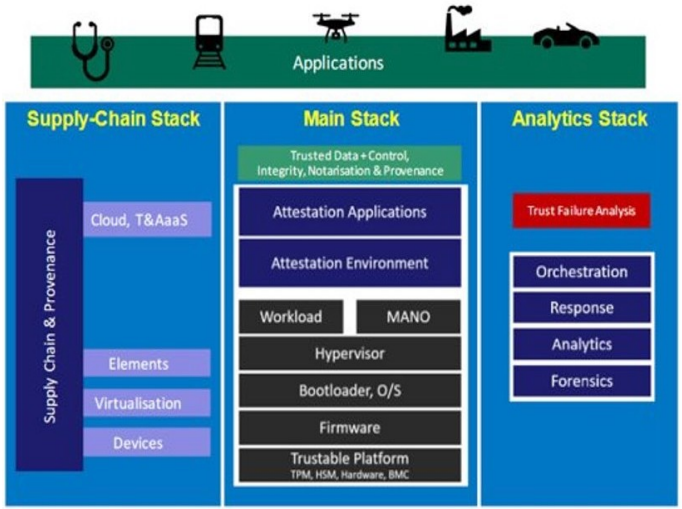




Summary

Grand Challenge

- Where the attestation takes place
- How and when(!) the attestation communicates with the element being attested
- Interface definitions and requirements
- Trust loss, Detection, Response and Orchestration



Thanks & Demo

Roosa Risto, Nokia
Kaisa Jatkola, Nokia
Pekka Kurre, Nokia
Victor Trucanu, Nokia
Don McBride, Nokia Bell Labs
Gary Atkinson, Nokia Bell Labs
Kiti Muller, Aalto University (Neurobiology)


NOKIA Bell Labs

Copyright and confidentiality