

# 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"



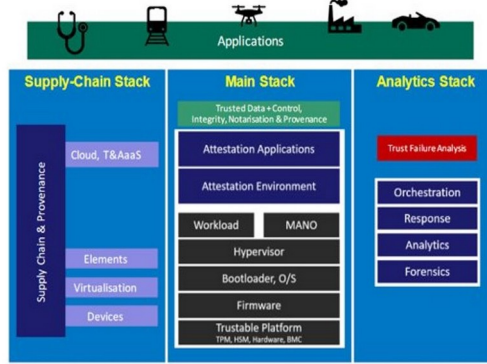
**Case Studies:**  
Medical, Railways

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

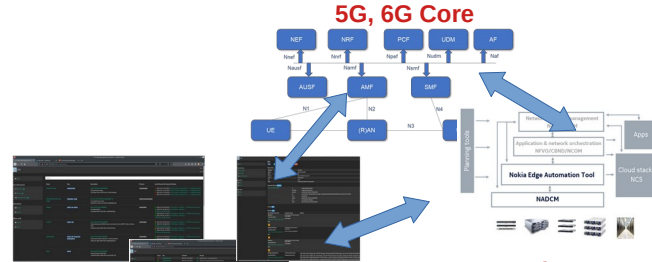


**Notarisation:**  
TransparencyLog,  
Blockchain, etc

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



**Trust Stack**



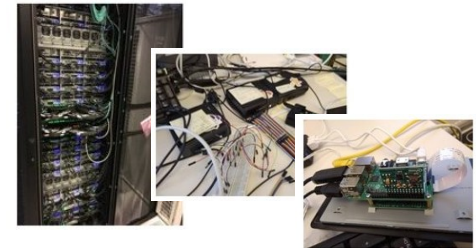
**Integration:**  
Remote Attestation Services  
MANO, 5G Core, 6G Core  
Attestation Applications,  
Data/Control Provenance

**Deployment**

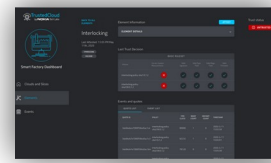


**Monitoring,  
Forensics and  
Analytics**

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



# Trusted Computing: Medical Systems

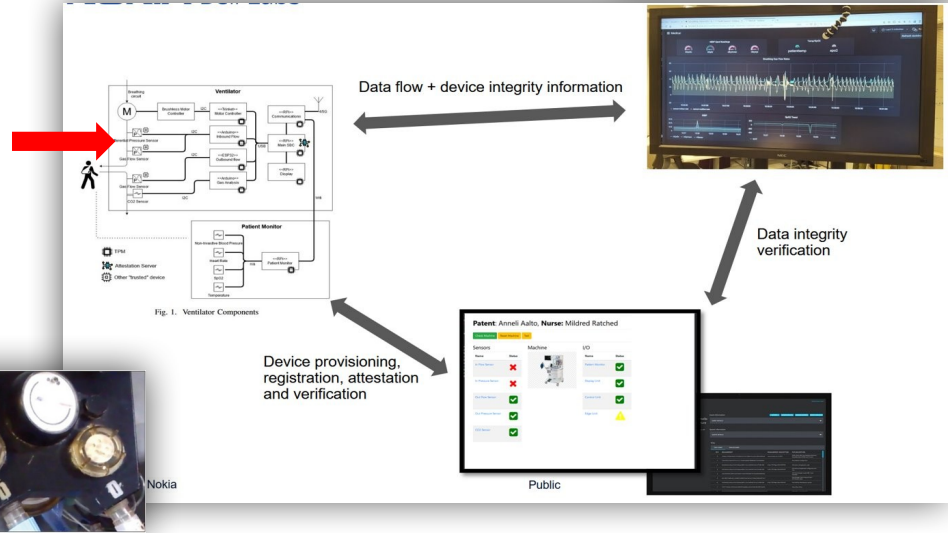
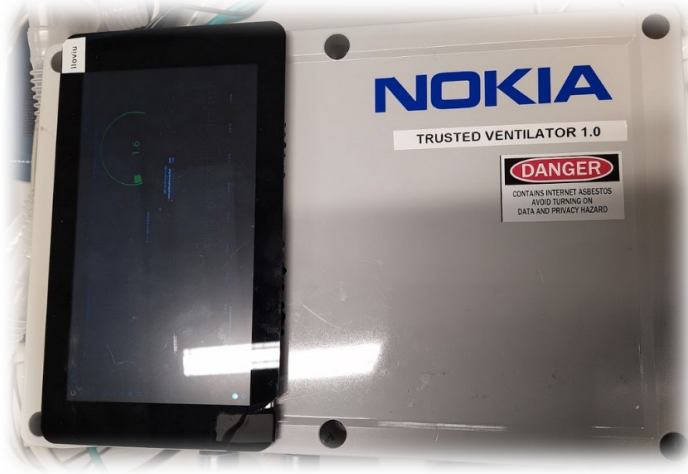


Machine Status

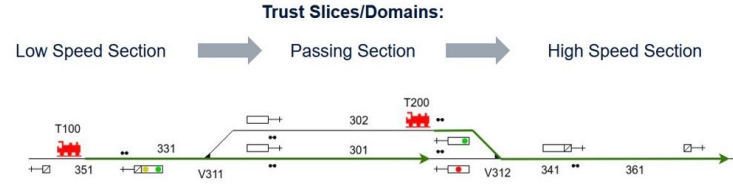
**Patent:** Anneli Aalto, **Nurse:** Mildred Ratched

Check Machine | Base Machine | Test

Sensors		Machine	I/O	
Name	Status		Name	Status
In Flow Sensor	✗		Patient Monitor	✓
In Pressure Sensor	✗		Display Unit	✓
Out Flow Sensor	✓		Control Unit	✓
Out Pressure Sensor	✓		Edge Unit	⚠
CO2 Sensor	✓			

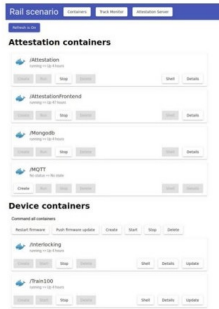


# Trusted Computing: Railways



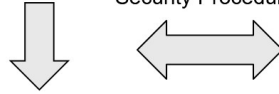
**Trust Slice Verification Rule Sets:**

Core/Basic LoA			Intermediate LoA			Critical LoA		
TMF 2.0 Quote Rules	Attestation Timeliness Rules	History/Assurance Rules	TMF 2.0 Quote Rules	Attestation Timeliness Rules	History/Assurance Rules	TMF 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?		Is it a quote?	Did the device respond to the quote request in a timely manner?		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?		Signed and matches the qualified signer?	Did the device process the quote request in a timely manner?		Signed and matches the qualified signer?	Did the device process the quote request in a timely manner?	...and for what properties?
None + additional data correct?			None + additional data correct?	Why the response consistent with network latencies (where applicable)?		None + additional data correct?	Why the response consistent with network latencies (where applicable)?	Does the device verify against the selected rules for its LoA? (where applicable)?
Does the attested value match the known good value?			Does the attested value match the known good value?			Does the attested value match the known good value?		What set of PCs is required for a minimum LoA?
Is the device running the correct firmware?			Is the device running the correct firmware?			Is the device running the correct firmware?		
Has the device been rebooted?			Has the device been rebooted?			Has the device been rebooted?		
Is the clock increasing correctly?			Is the clock increasing correctly?			Is the clock increasing correctly?		
			Was the device shutdown correctly?			Was the device shutdown correctly?		

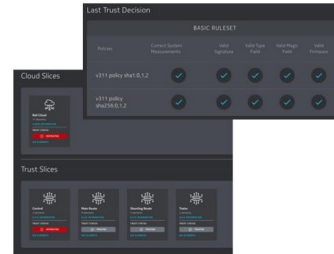


Administration

Attack Injection      Operator Response & Security Procedures



Operator & Simulation Control

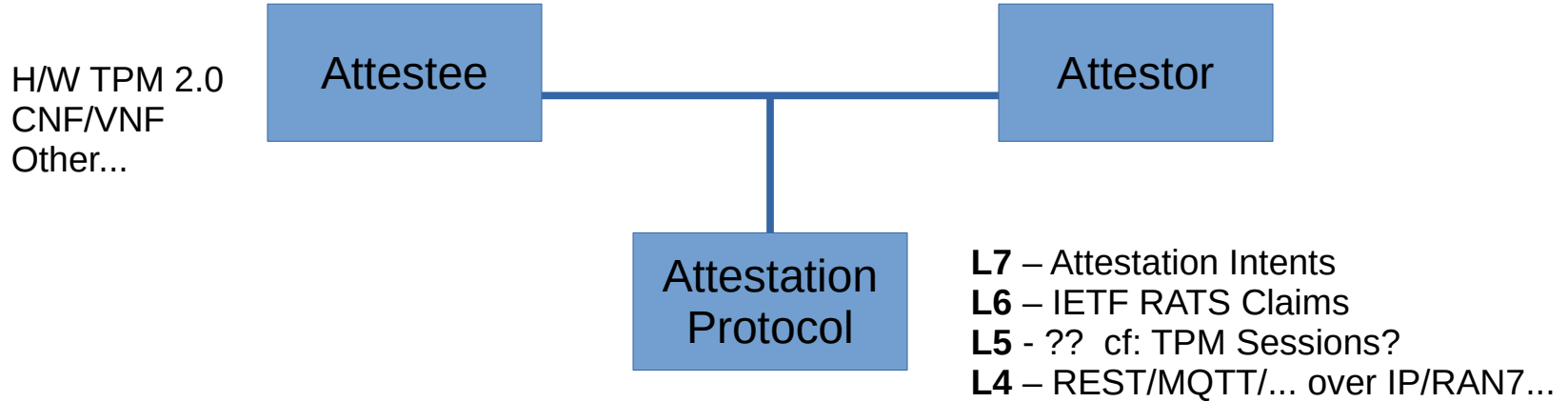


Attestation

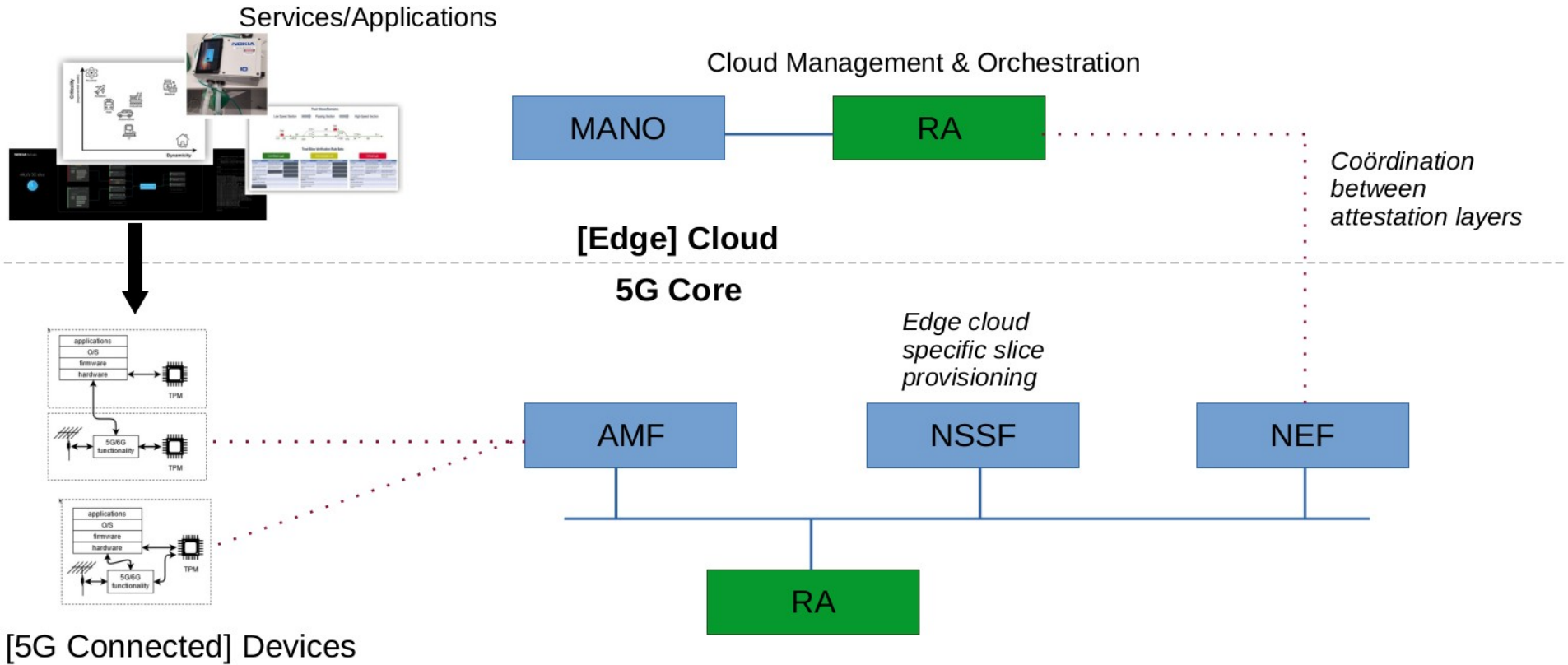
**Communication Infrastructure**

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

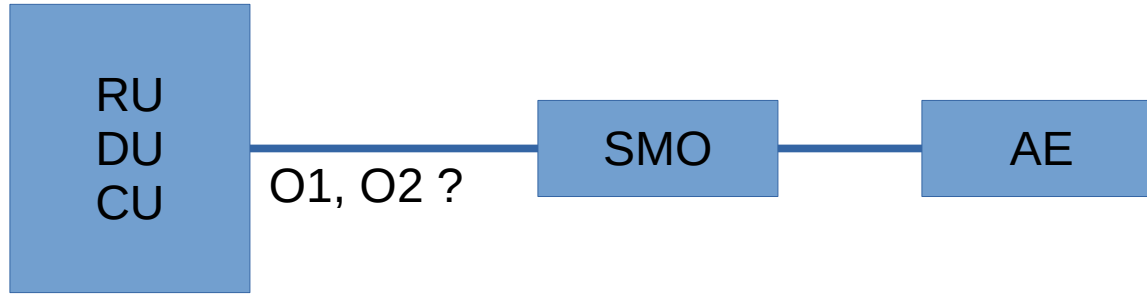
# Generic Model



# 5G



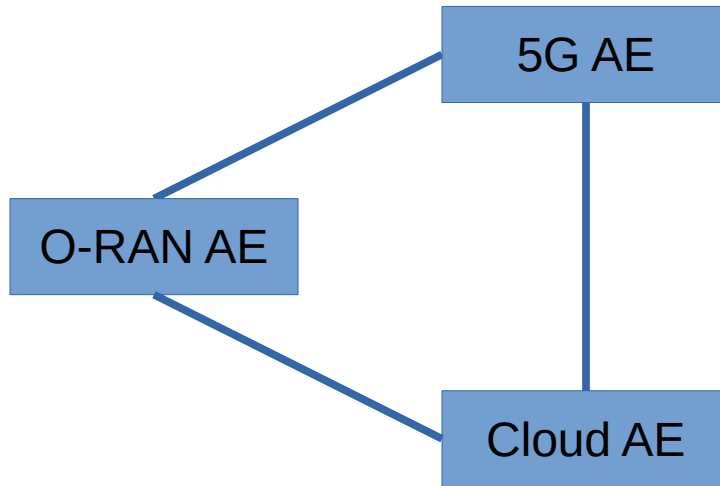
# O-RAN





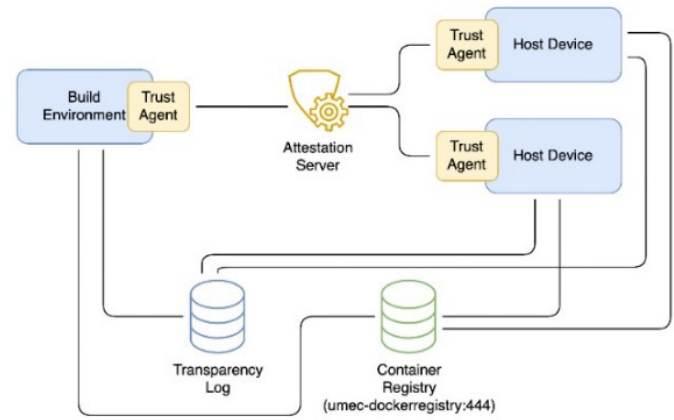
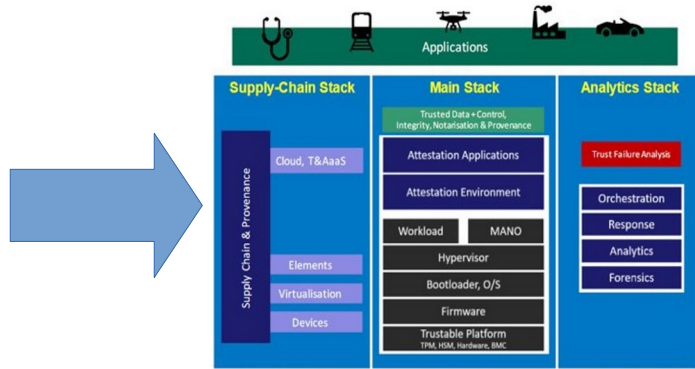
# O-RAN+5G+Cloud+Domain

Application Domain

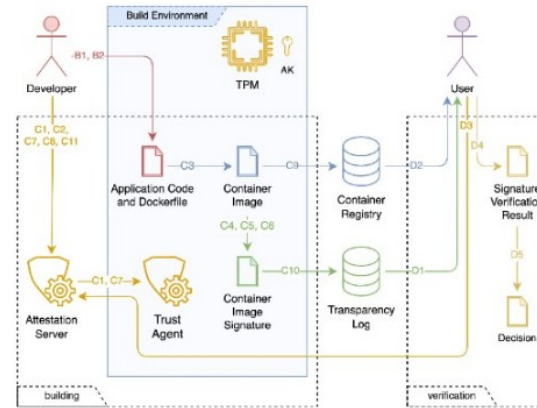


Model of Trust?  
Distribution of Responsibilities  
AE-AE Protocols  
Element Identity across infrastructure  
domains and application domains

# Supply-Chain, CD/CI, DevOps



## [Core,Edge,Far-Edge] RAS Architecture



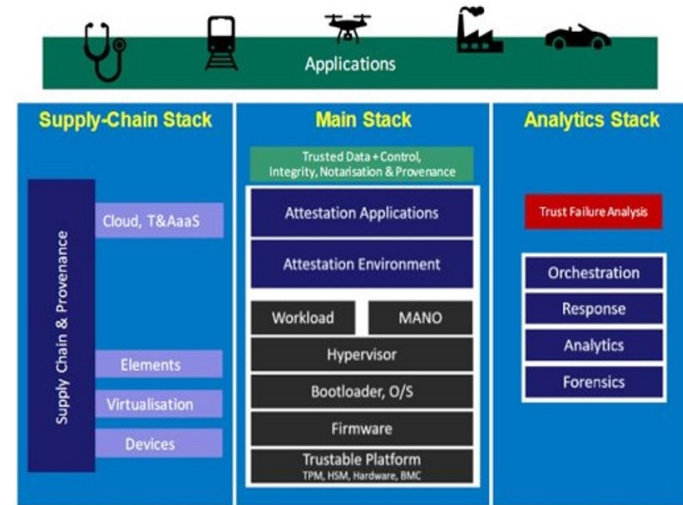
## Container Attestation



# 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

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use of Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback").

Such Feedback may be used in Nokia products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the

implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.