Remote Attestation & Formal Methods: The Bigger Picture

Prof. Ian Oliver

University of Oulu, Finland

PaveTrust Workshop @FM24, 9 Sept 2024, Milano, Italy

Contents

- This is the story of how we got here
- Formal Methods + Attestation ….
- ….what’s the BIGGER picture

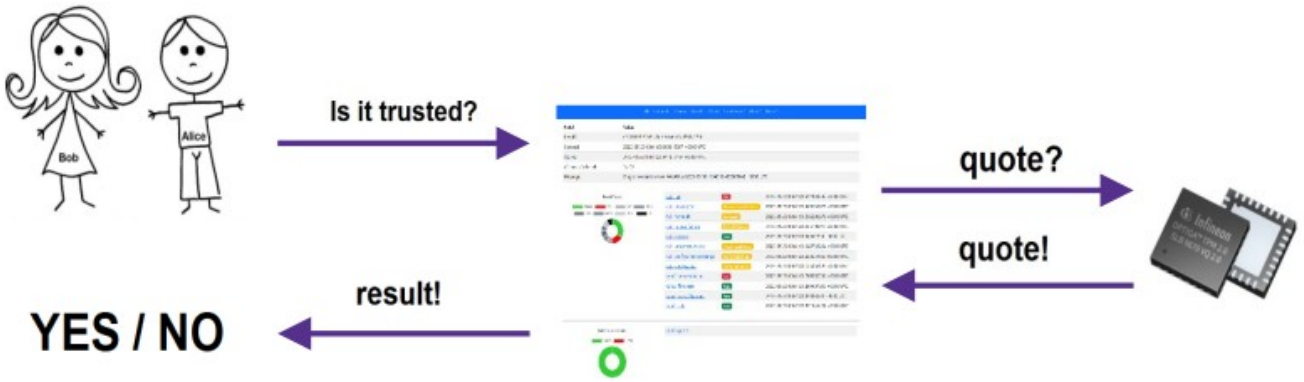
History

- UML Semantics
  - UML for Telecommunications
- HW/SW Co-design
  - B → Bluespec → SystemVerilog → FPGA/ASIC
- Graph DB/Semantic Web systems
  - Alloy → ”Python”

History

- Basically I spent all my time integrating systems
- ”Verticals applications”

Attesting Telcosystems



- Identity and integrity of a device/container/system
- Attestable, Trustable, Trustworthy, Trusted
- Integration of attestation into a system
- Establishment of trustworthiness (and whatever that means!)

- NOT, about TPM (just one component in the confidential computing concept)

Attesting Telcosystems

- Decision algorithms get more complex
- [Attestation] Policy languages

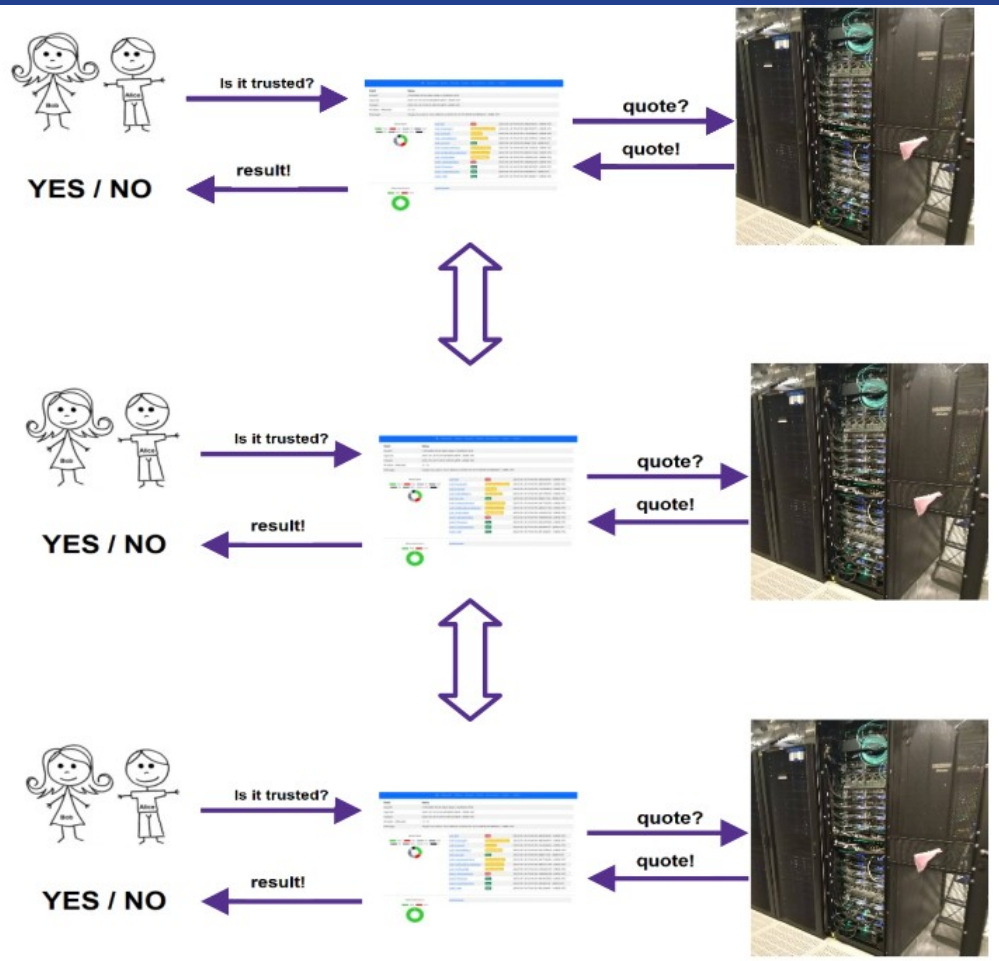
```
~/python/AttestationEngine-0.11.0/apps/attdsl2/examplescripts $ cat a2.att

template testx86
 attest
   SRTM-SHA1,{}
      [[
         q1firmware <- tpm2rules/TPM2FirmwareVersion, {}
      ]]

   CheckCredentials,{},copycredentials
      [[
         id <-  tpm2rules/TPM2CredentialVerify  ,{}
      ]]
  decision
    !q1firmware ^ id~/python/AttestationEngine-0.11.0/apps/attdsl2/examplescripts $
~/python/AttestationEngine-0.11.0/apps/attdsl2/examplescripts $ cat a2.eva
```

I have a good story about this….

Attesting Telcosystems



- **Distributed vs Parallel**
  - Not load balancing
- **Attestation Server communication protocols**
- **Consistency**

- **Consistency (via database)**
- **Consensus (blockchain?)**

- **Edge, Far-Edge, Remote Devices & latency**
- **cf: railways**
  - UDP and unreliable transport
  - *failure to attest != failure of attestation*

A common question...

- Where does PCR0 come from?

A common question...

- Where does PCR0 come from?

A common question...

- Where does PCR0 come from?

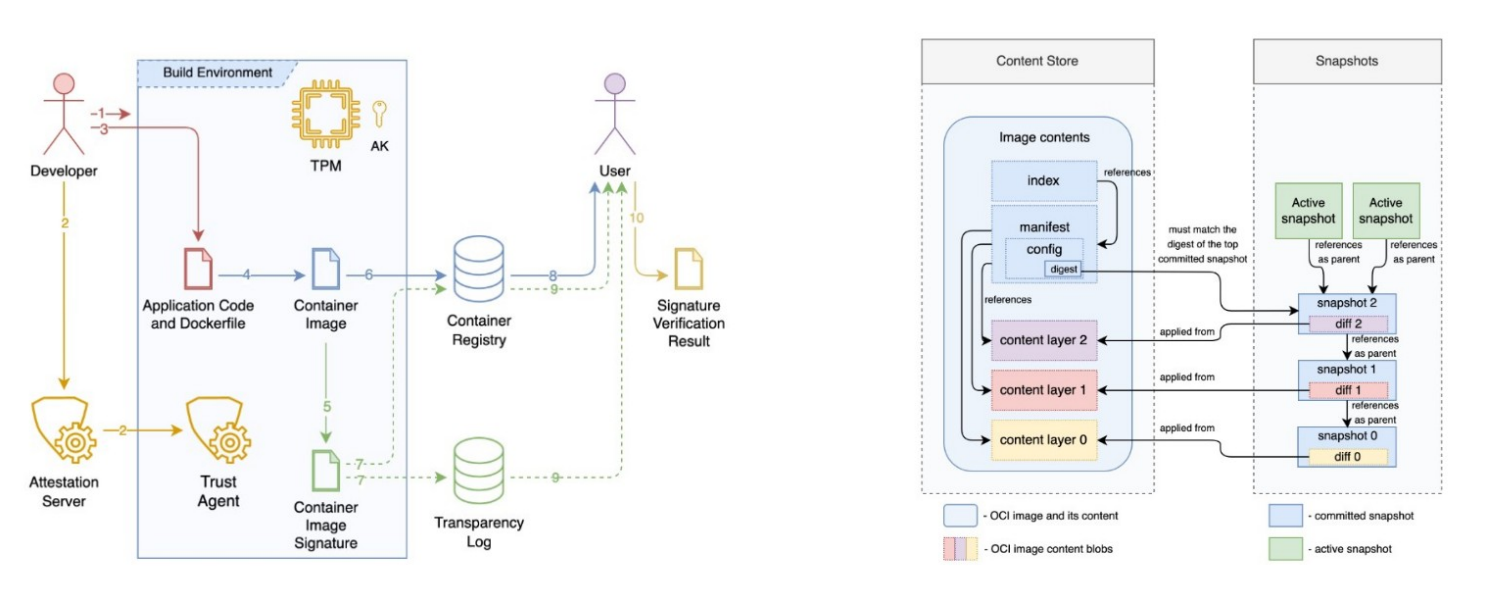
A common question...

- Where does PCR0 come from?
- And, do you actually know it?

Supply-Chain ← Boot → Run-Time

Not just TPMs

- Containers too...Kubernetes….yay!
- Lifecycle: start, stop, migrate etc…
- Process calculi, Model checking (eg: Alloy)



Adjectives

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

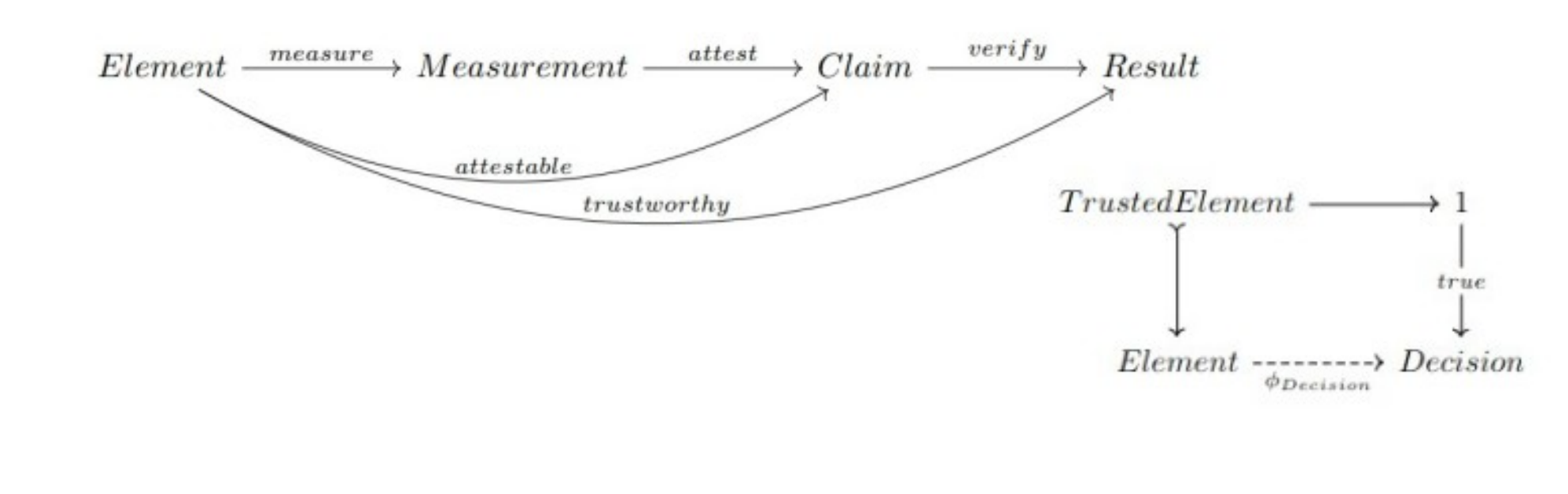
Attestable? **Trustable?**

Adjectives…trustable to trusted?

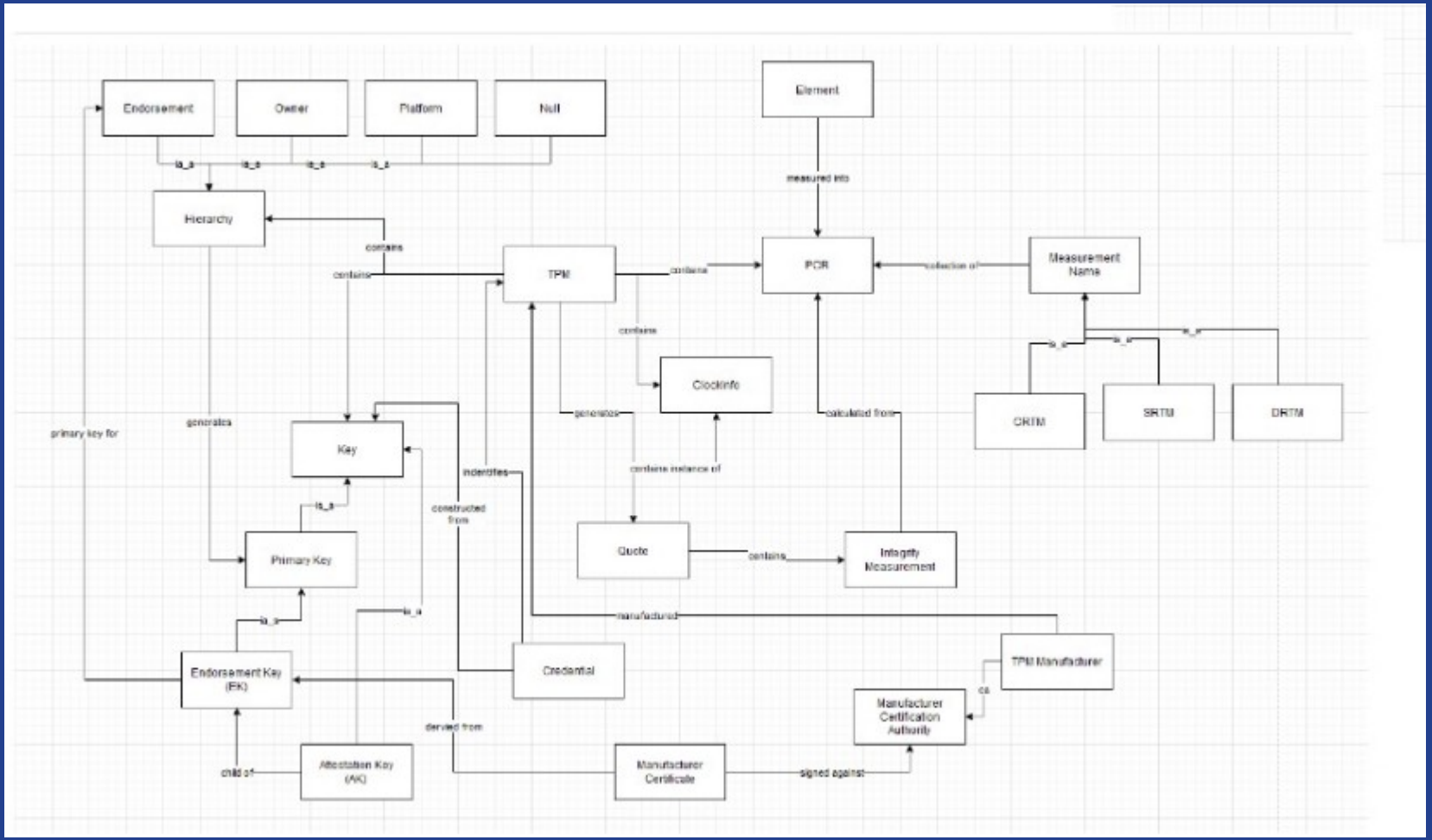
Belief logics
Modality and agency
Many worlds, probability, superposition, dirac notation and quantum trust….

Or...is the famous cat trusted before you open the box? And if it isn’t, so what?

Elements to Results



What attestable things?

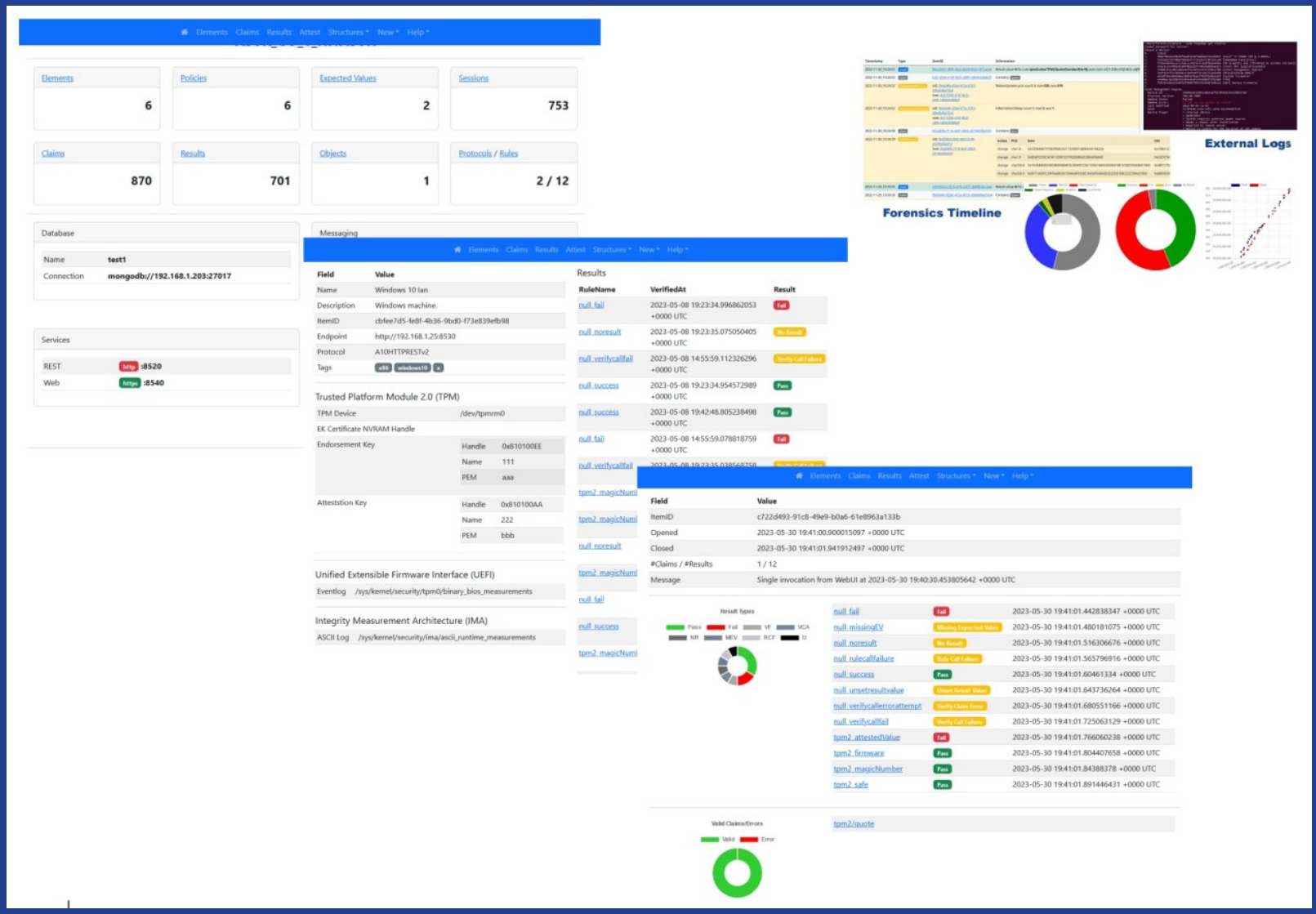


Typical 5G Core Trust Requirements

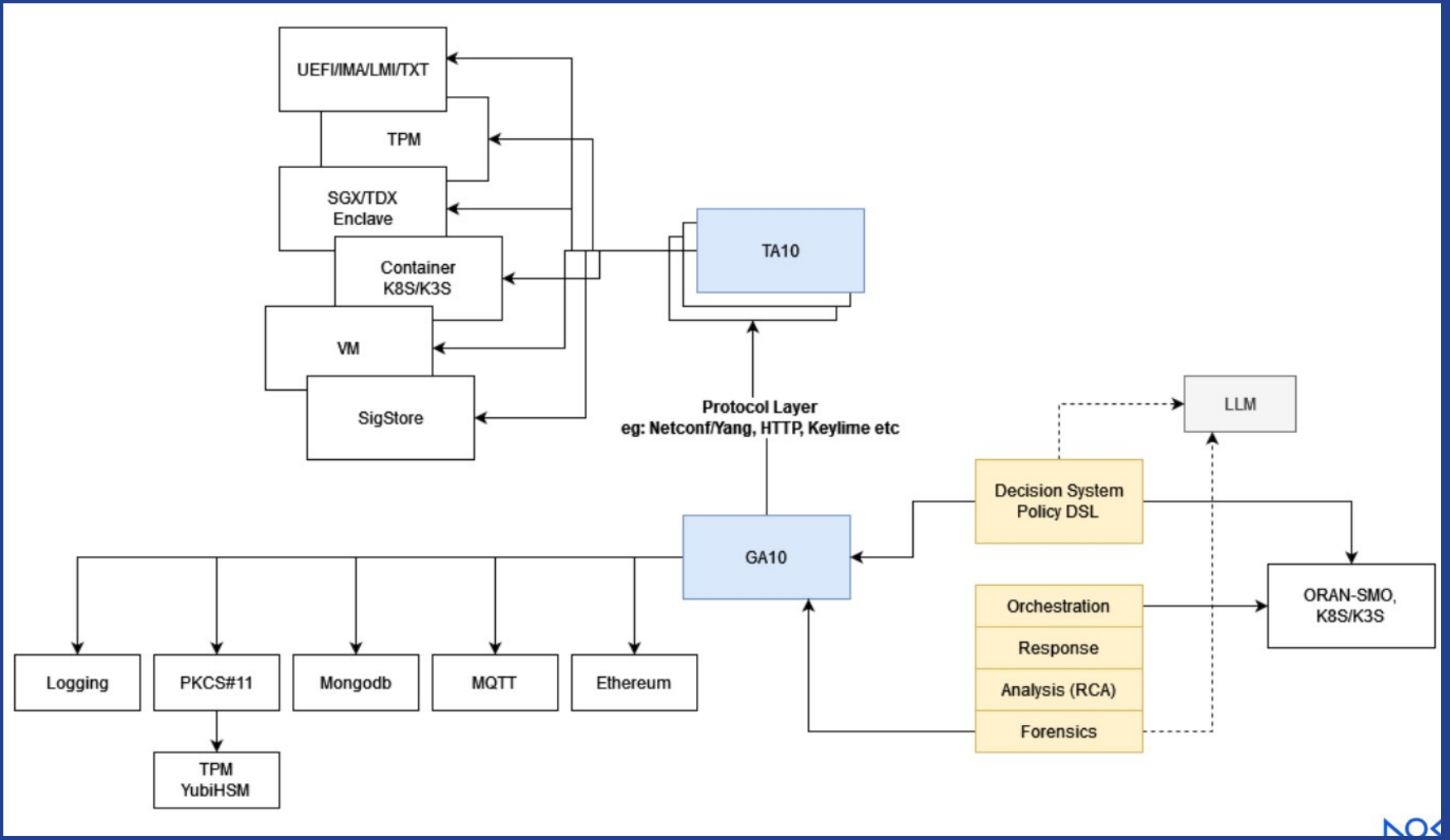
- Container Image
- Container Instances
- Machine(s) with TPM
- Kubernetes Cluster (workload management)
- Kubernetes Management and Orchestration
- SGX, TDX, CCA, Bare Metal, TrustZone
- Enclaved processes / containers
- Network Connections (attested TLS, in and out of enclaves)
- Distributed elements: gNB --
- Cients (SIM,eSIM devices, apps: Android etc)
- OSS/BSS, Customer Networks, MVNOs, Breakout etc.
- Confidentiality Requirements (shared gNB in ORAN)

More to say about this later…..ORAN and the Grand Challenge

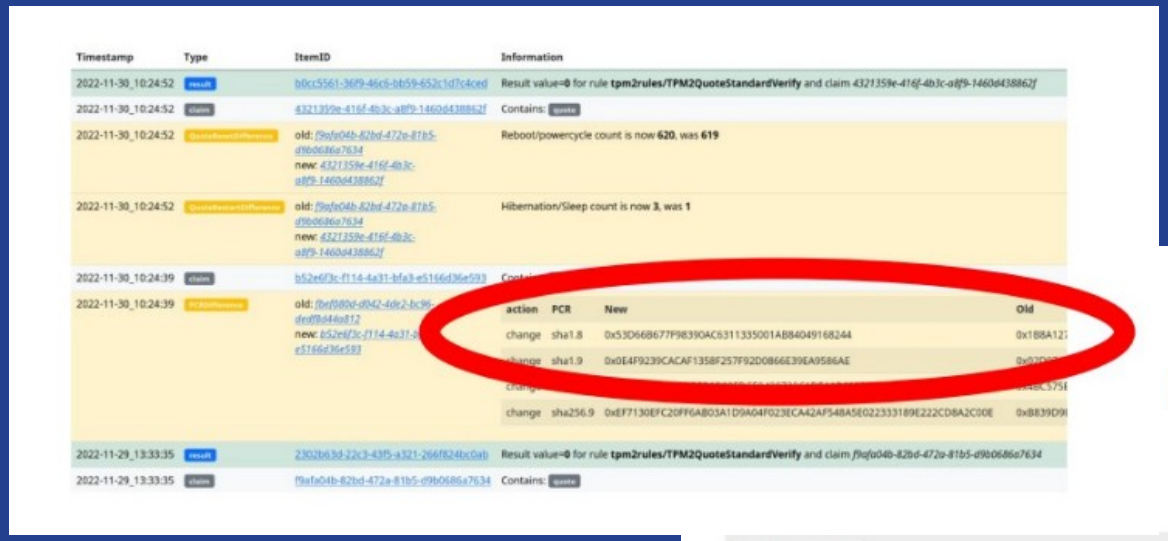
Attesting things with Jane (and Tarzan)



Attesting things with Jane (and Tarzan)



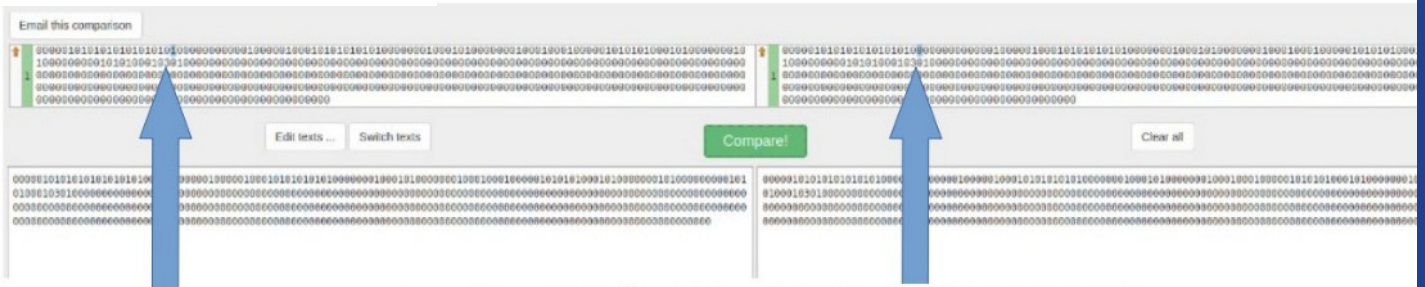
Digital Forensics



Timestamp	Type	ItemID	Information
2022-11-30_10:24:52	result	b0cc5561-36f9-46c6-bb59-652c1d7c4ced	Result value=0 for rule **tpm2rules/TPM2QuoteStandardVerify** and claim *4321359e-416f-4b3c-a8f9-1460d438862f*
2022-11-30_10:24:52	claim	4321359e-416f-4b3c-a8f9-1460d438862f	Contains: quote
2022-11-30_10:24:52	QuoteRebootDifference	old: *f9afa04b-82bd-472e-81b5-d9b0686a7634* new: *4321359e-416f-4b3c-a8f9-1460d438862f*	Reboot/powercycle count is now **620**, was **619**
2022-11-30_10:24:52	QuoteResetDifference	old: *f9afa04b-82bd-472e-81b5-d9b0686a7634* new: *4321359e-416f-4b3c-a8f9-1460d438862f*	Hibernation/Sleep count is now **3**, was **1**
2022-11-30_10:24:39	claim	b52e6f3c-f114-4a31-bfa3-e5166d36e593	Cont
2022-11-30_10:24:39	PCRDifference	old: *f0ef080d-d042-4de2-bc96-dea9b44ea812* new: *b52e6f3c-f114-4a31-b…* *e5166d36e593*	action PCR New Old change sha1.8 0x53D66B677F98390AC6311335001AB840491682440x188A12… change sha1.9 0x0E4F9239CACAF1358F257F92D0866E39EA9586AE 0x… change sha256.9 0xEF7130EFC20FF6AB03A1D9A04F023ECA42AF548A5E022333189E222CD8A2C00E 0xB839D9…
2022-11-29_13:33:35	result	2302b63d-22c3-43f5-a321-266f824bc0ab	Result value=0 for rule **tpm2rules/TPM2QuoteStandardVerify** and claim *f9afa04b-82bd-472a-81b5-d9b0686a7634*
2022-11-29_13:33:35	claim	f9afa04b-82bd-472a-81b5-d9b0686a7634	Contains: quote

action	PCR	New	Old
change	sha1.1	0x2D407D1DF44E266E449992E56838889FF8EA1214	0x0FA3E35EEB30…
change	sha1.10	0xB6A299FE3E5429CE5F1F739743CCA5485599CF86	0xFC8D9C5DA19…
change	sha256.1	0x1EF720FCC908445AF91650B21871B25EB5E76FE6017C76066D5ABAC347621D3E	0xB853D270677E…
change	sha256.10	0xA1058CB87BC083B1EFB2F7881B541FD4FDBB1F7E0CD5CD11E5DD1239B2F9D1EA	0xBA54C5233A9…

- Firmware configuration update detected after re-attestation
- PCR 1 change and a UEFI eventlog diff



- Firmware configuration update detected after re-attestation
- PCR 1 change and a UEFI eventlog diff
- LVFS did not run. No PCR1 related updates, No Lenovo updates at that time (PCR0)
- PCR0 matched the correct firmware for that laptop

Summary

- Story of real-world research, deployment and experiences
- Attestable things
- Ontologies

Grand Challenge

- Library of Interoperable and composable specifications
- Abstaction of attest and trust
- Supply-chain, run-time and life-cycle specifications

Grand Challenge: ORAN/NFV

Views = isomorphic Policies