



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"

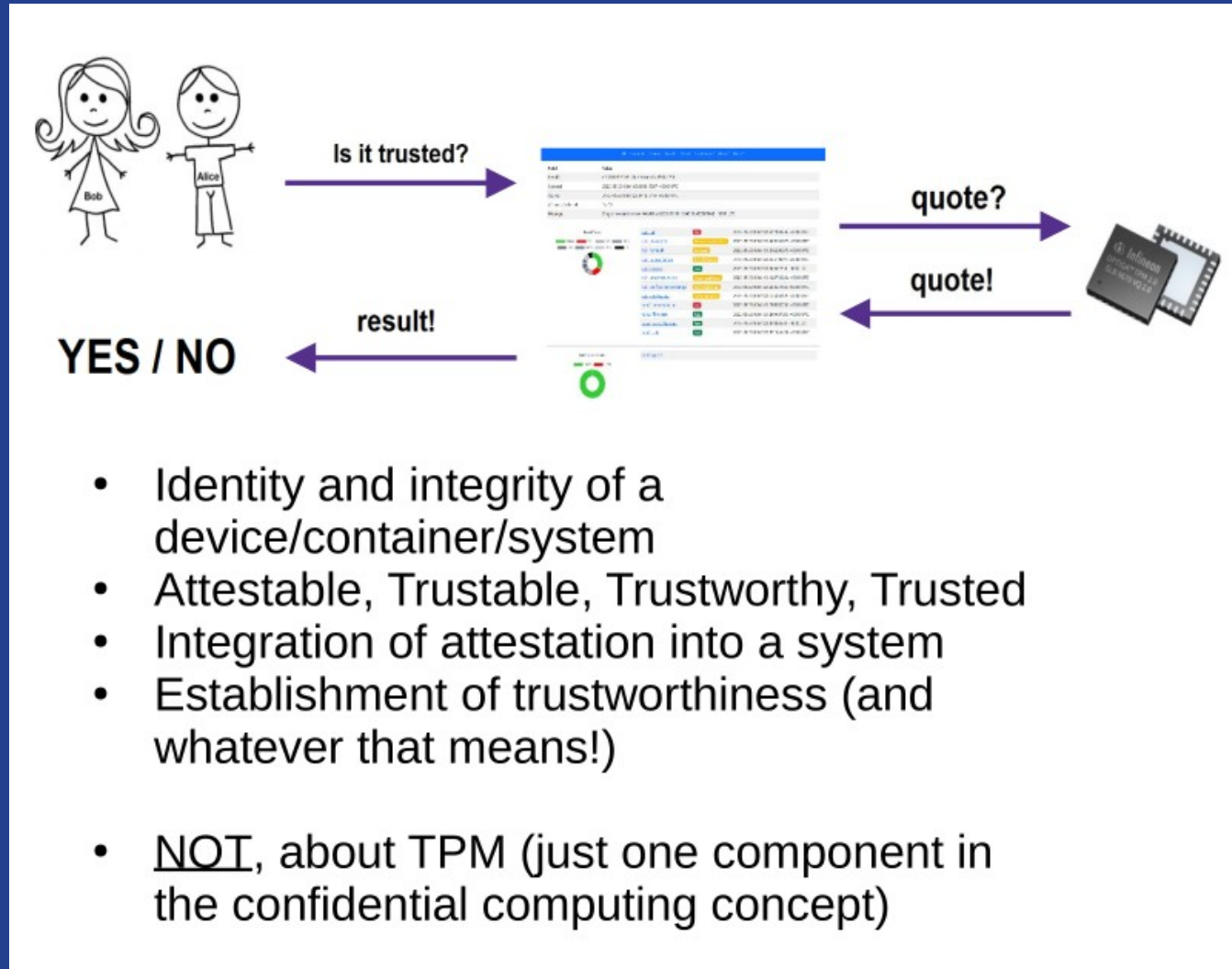


History

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

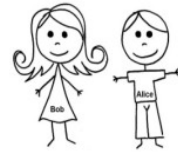


Attesting Telcosystems





Attesting Telcosystems



Is it trusted?



quote?

quote!

YES / NO

result!



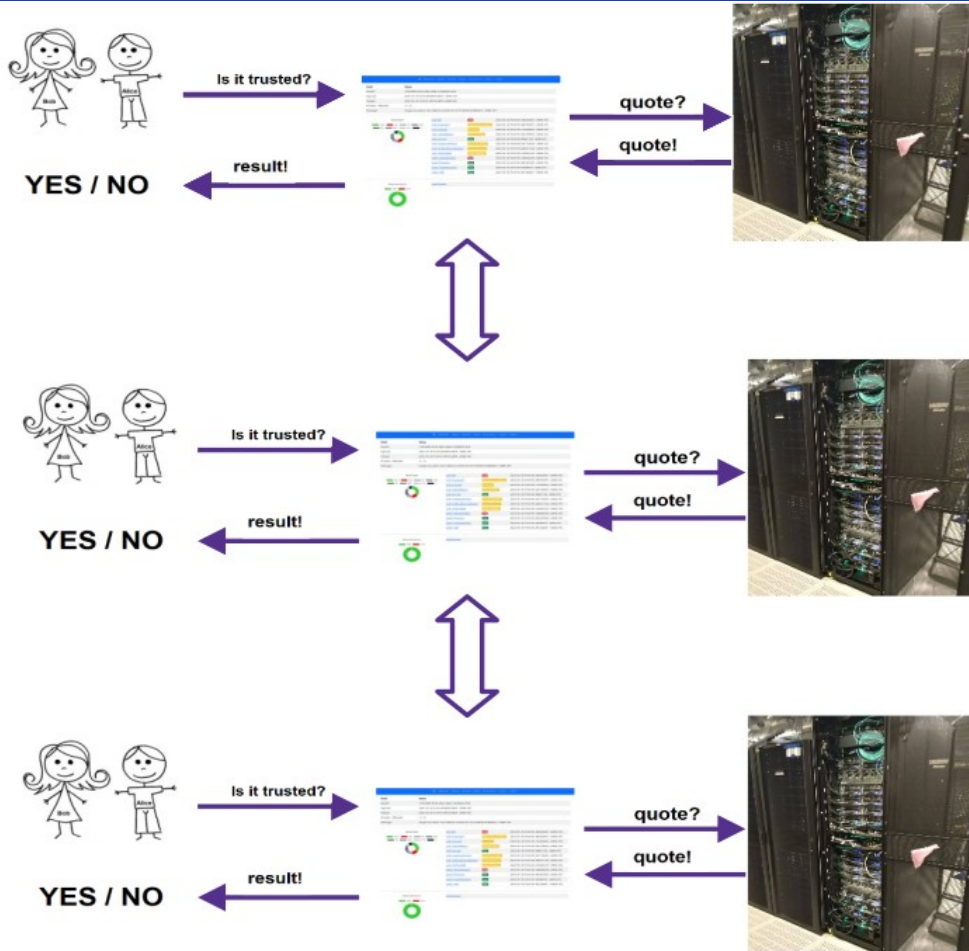
- Decision algorithms get more complex
- [Attestation] Policy languages

```
~/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...

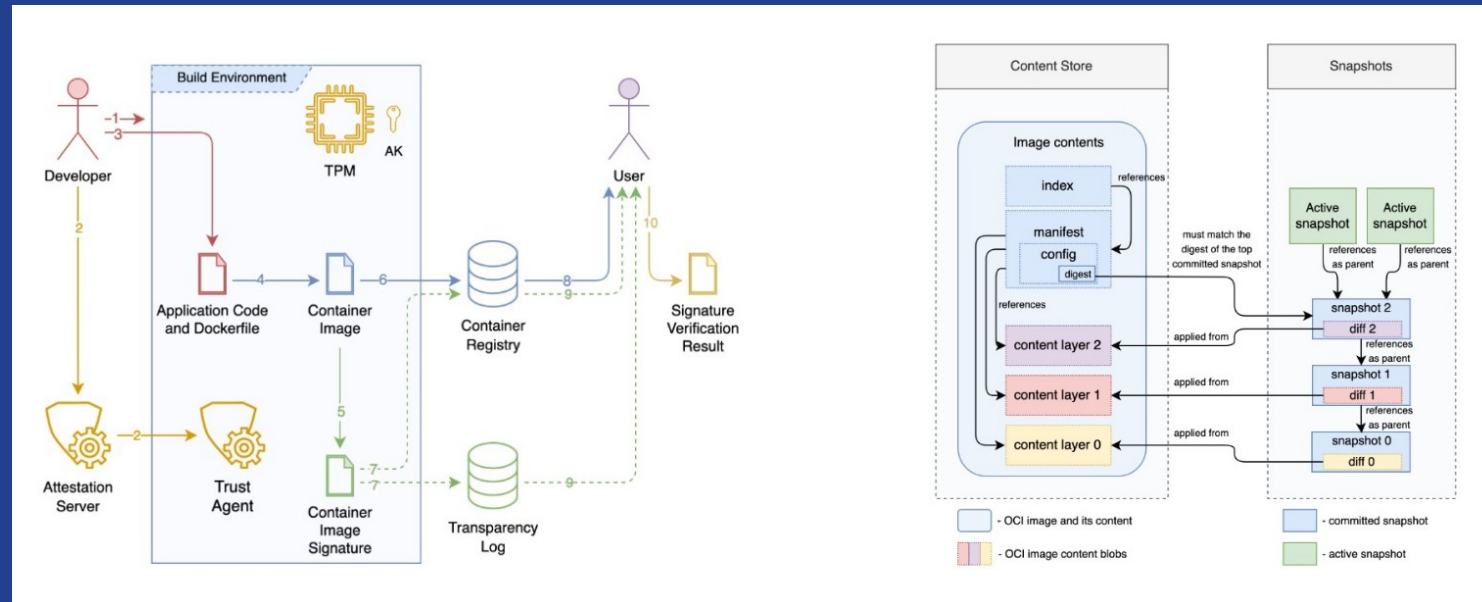
- Where does PCR0 come from?
- And, do you actually know it?





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

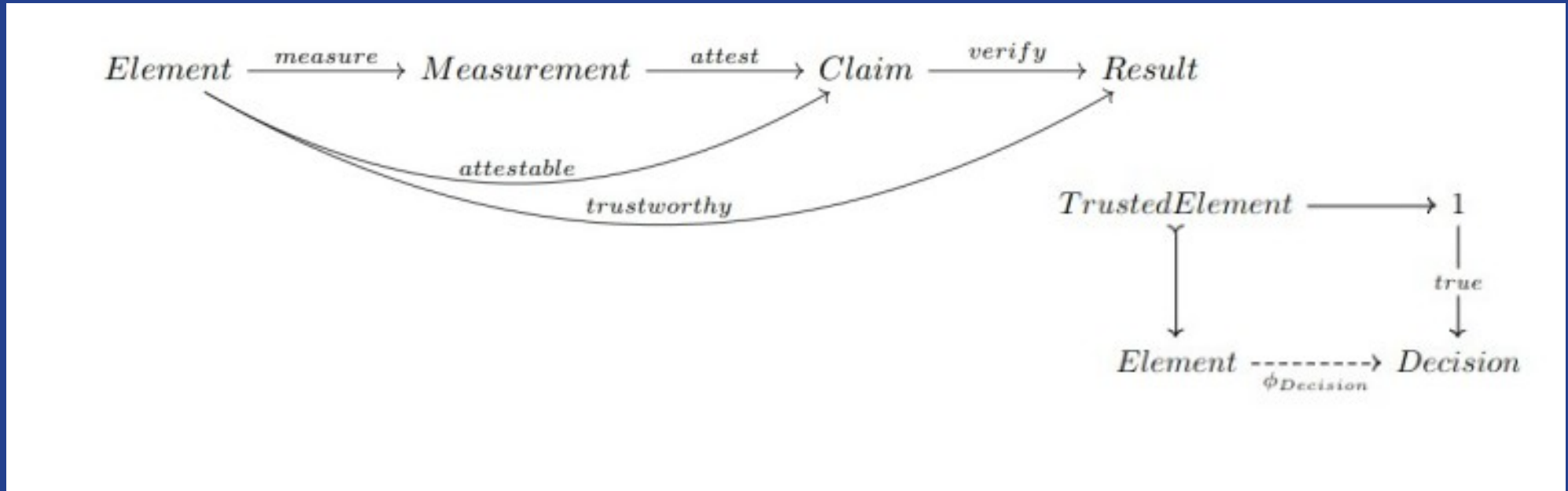
Many worlds, probability, superposition, dirac notation and quantum trust....

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



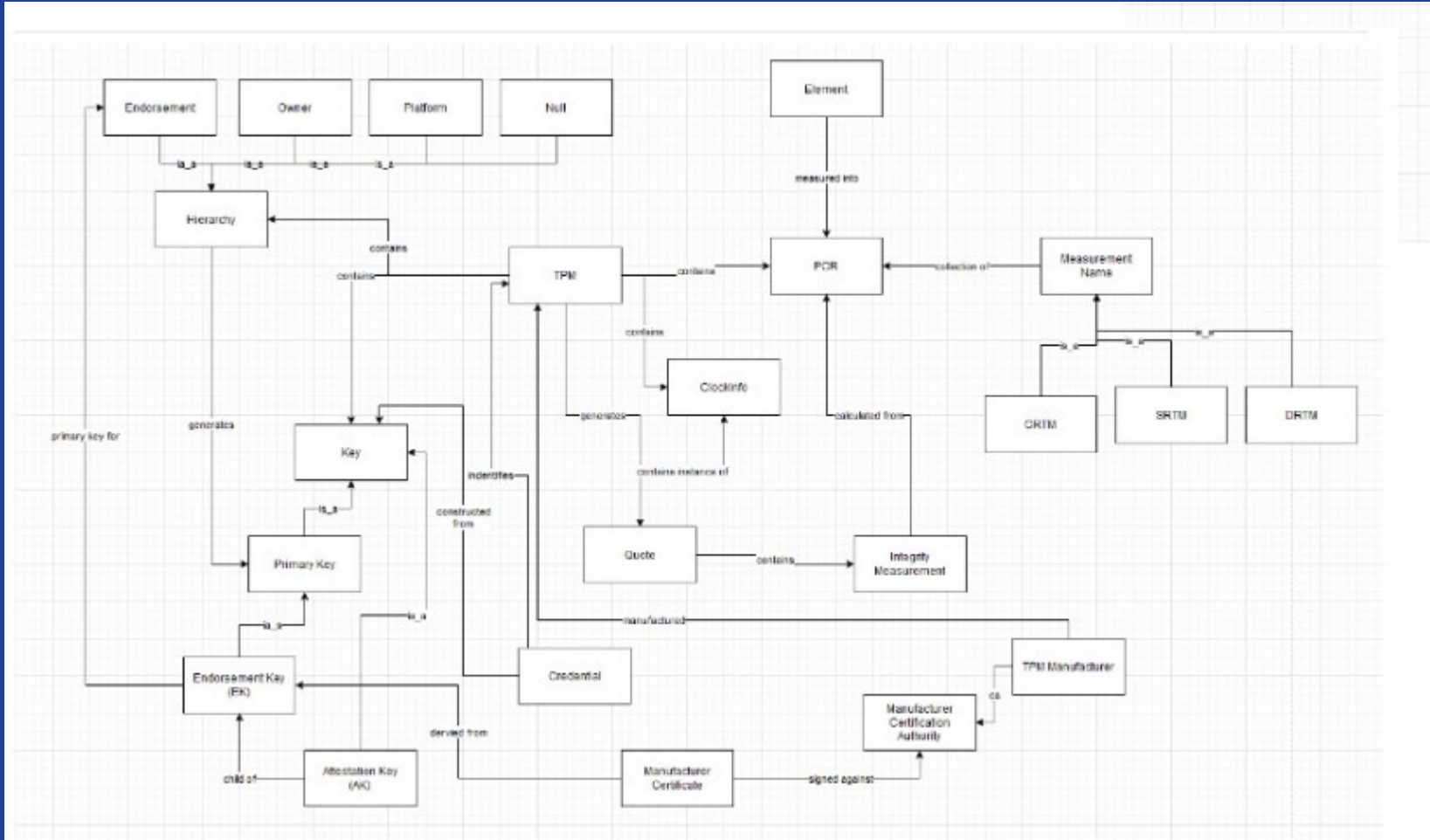


Elements to Results





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 --
- Clients (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)

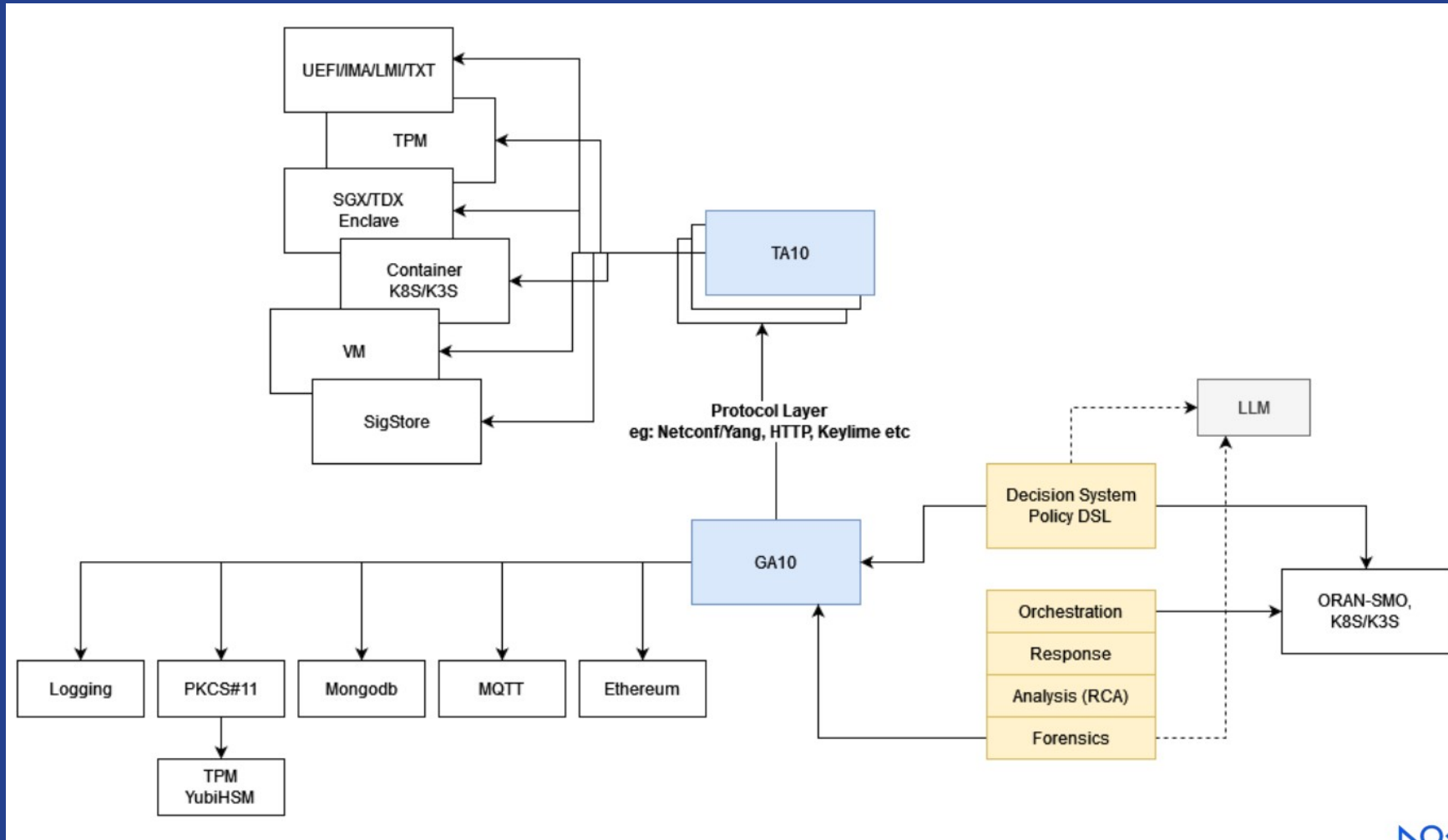
The screenshot displays the Jane web interface with the following components:

- Summary Dashboard:**
 - Elements: 6
 - Policies: 6
 - Expected Values: 2
 - Sessions: 753
 - Claims: 870
 - Results: 701
 - Objects: 1
 - Protocols / Rules: 2 / 12
- Database:**
 - Name: test1
 - Connection: mongodb://192.168.1.203:27017
- Services:**
 - REST: https://:8520
 - Web: https://:8540
- Messaging:**
 - Field: Name (Windows 10 lan), Description (Windows machine), ItemID (cb1ee7d5-4ef8-4b36-9bd0-f73e839efb98), Endpoint (http://192.168.1.25:8530), Protocol (A10HTTPRESTv2), Tags (ada, validobject)
- Trusted Platform Module 2.0 (TPM2):**
 - TPM Device: /dev/tpmrm0
 - EK Certificate NVIRAM Handle:
 - Endorsement Key: Handle (0xd10100EE), Name (111), PEM (aaa)
 - Attestation Key: Handle (0xd10100AA), Name (222), PEM (bbb)
- Unified Extensible Firmware Interface (UEFI):**
 - Eventlog: /sys/kernel/security/tpm0/binary_bios_measurements
- Integrity Measurement Architecture (IMA):**
 - ASCII Log: /sys/kernel/security/ima/ascii_runtime_measurements
- Results Table:**

RuleName	VerifiedDat	Result
null_fail	2023-05-08 19:23:34.996662053 +0000 UTC	Fail
null_noresult	2023-05-08 19:23:35.075050405 +0000 UTC	No Result
null_verifycallfail	2023-05-08 14:55:59.112326296 +0000 UTC	Verify Call Failure
null_success	2023-05-08 19:23:34.954572989 +0000 UTC	Pass
null_success	2023-05-08 19:42:48.805238498 +0000 UTC	Pass
null_fail	2023-05-08 14:55:59.078818759 +0000 UTC	Fail
null_verifycallfail	2023-05-08 19:23:35.026639258 +0000 UTC	Verify Call Failure
- Forensic Timeline:** A circular chart showing the distribution of result types over time.
- External Logs:** A terminal window showing raw log output.
- Result Types Legend:**
 - Pass (Green), Fail (Red), No Result (Grey), Verify Call Failure (Yellow), Verify Call Success (Light Green), Invalid Expected Value (Light Blue), Missing Expected Value (Light Purple), Invalid Object (Light Orange), Invalid Policy (Light Pink), Invalid Rule (Light Cyan), Invalid Session (Light Magenta), Invalid Value (Light Brown), Invalid Claim (Light Grey).
- Valid Claims/Errors:** A donut chart showing the ratio of valid claims to errors.
- Detailed Log Entry:**
 - ItemID: c722d493-91c8-49e9-b0a6-61e8963a133b
 - Opened: 2023-05-30 19:41:00.900015097 +0000 UTC
 - Closed: 2023-05-30 19:41:01.941912497 +0000 UTC
 - #Claims / #Results: 1 / 12
 - Message: Single invocation from WebUI at 2023-05-30 19:40:30.453805642 +0000 UTC



Attesting things with Jane (and Tarzan)





Digital Forensics

Timestamp	Type	ItemID	Information
2022-11-30_10:24:52	result	b0cc5561-36f9-46c6-bb59-453c1d7c4ced	Result value=0 for rule tpm2rules/TPM2QuoteStandardVerify and claim 4321359e-416f-4b3c-a8f9-14604438862f
2022-11-30_10:24:52	status	4321359e-416f-4b3c-a8f9-14604438862f	Contains: success
2022-11-30_10:24:52	change	old: f9af04b-82bd-472a-87b5-d9b0686a7634 new: 4321359e-416f-4b3c-a8f9-14604438862f	Reboot/powercycle count is now 620, was 619
2022-11-30_10:24:52	change	old: f9af04b-82bd-472a-87b5-d9b0686a7634 new: 4321359e-416f-4b3c-a8f9-14604438862f	Hibernation/Sleep count is now 3, was 1
2022-11-30_10:24:39	status	b52e673c-f114-4a31-bfa3-e5166d36e593	Contains: success
2022-11-30_10:24:39	change	old: f9af04b-82bd-472a-87b5-d9b0686a7634 new: 652e673c-f114-4a31-bfa3-e5166d36e593	
2022-11-29_13:33:35	result	2302b63d-32c3-43f5-a321-266f824bc0ab	Result value=0 for rule tpm2rules/TPM2QuoteStandardVerify and claim f9af04b-82bd-472a-87b5-d9b0686a7634
2022-11-29_13:33:35	status	f9af04b-82bd-472a-87b5-d9b0686a7634	Contains: success

action	PCR	New	Old
change	sha1.1	0x2d407d1df44e266449992e56838889ff8ea1214	0x0FA3E35EEB30;
change	sha1.10	0xB6A299E3E5429CE5F1F739743CCAS485599CF86	0xFCB9C5DA19
change	sha256.1	0x1EF720FCC908445AF91650B21871B25EBE76FE6017C7606605A8AC347621D3E	0xB853D270677E
change	sha256.10	0xA1058C867BC0831EF82F7881B541FD4FD8B1F7E0CD5CD11ESDD1239B2F9D1EA	0xBAS4C5233A8I

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

Email this comparison

```

0000018101810181010100000000000000000100001000101810181010100000000010001010000001800100100001010100010100000010
1000100000101010001038100000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

```

Edit texts ...

Switch texts

- 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
- Abstraction of attest and trust
- Supply-chain, run-time and life-cycle specifications



Grand Challenge: ORAN/NFV

