Attestation Results Framing

Laurence Lundblade, March 2022

Full range of security strengths

Certified HW with no SW at all (not a TPM, no measurement)

Simple uncertified SW

Everything in between (TPM, TEE's, Windows, RIOT, …)

Full range of system architectures

Pure HW — Purpose-built Attestation HW (not a TPM)

App-based — Attestation inside an Android app in Java, Swift, Python…

Everything in between (Full OS's, IoT Devices, TEEs, Network Equipment…)

JSON Encoding & others
TLS Security & others

JSON + TLS, widely used for B2B

Support JWT/CWT too

B2B data encoding and security is a solved problem, so this is not a focus of RATS

RATS standard for Device/Attester identity

Serial number, OEM, model, version

JSON and perhaps other encoding formats

Allow Passthrough Claims

Passed through from Evidence/Attester

Passed through from Endorser/Endorsement

Detail varies by use case

A base standard of simple pass/fail and/or error code — base standard must work for all architectures and security stengths

Device/Attester identity for some use cases

Machine learning risk engines want every scrap and detail