CoSERV Revisited

CONCISE SELECTOR FOR ENDORSEMENTS AND REFERENCE VALUES

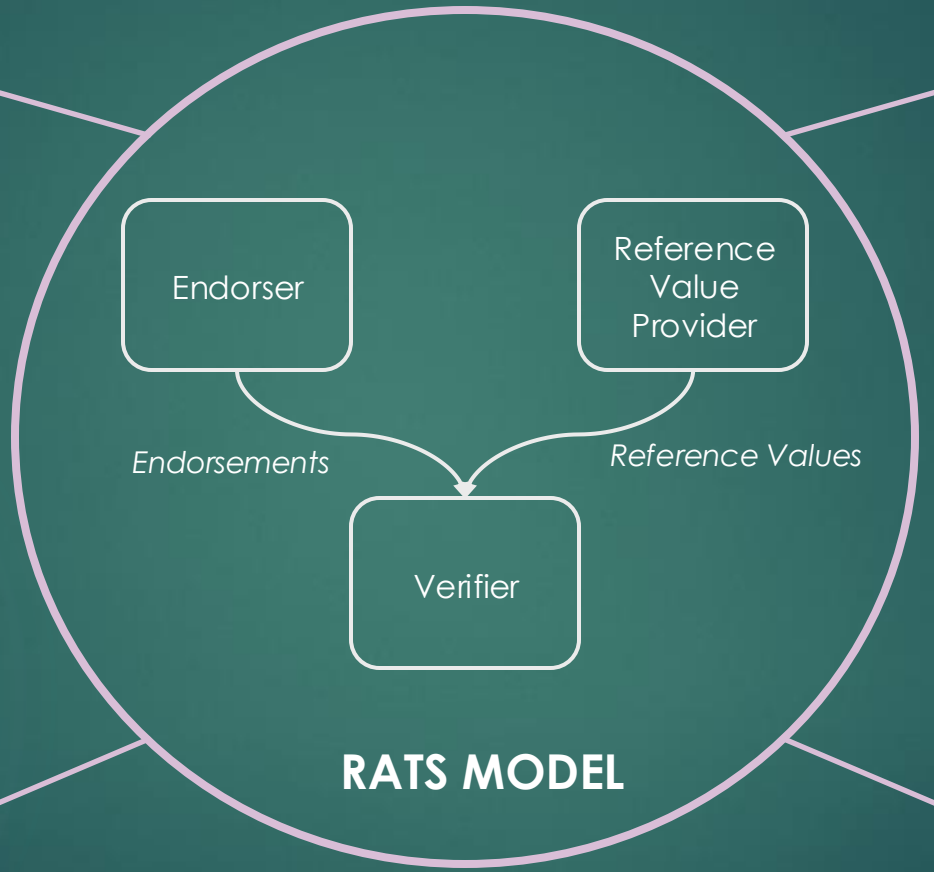
UPDATE AND DISCUSSION

CCC ATTESTATION SIG MEETING 2025-07-15

Background

Fragmentation
A growing number of vendor-specific APIs for verifiers to code against

Supply Chain Complexity
Levels of indirection between supply chain actors and verifiers



Verifier Diversity
Verifiers might be cloud services, or local application code - they might run on constrained devices

Interaction Models
Might be push or pull, or continuous synchronisation

The idealized RATS model hides some real-world challenges. How can we address these and help the industry to harmonize?

CoSERV Overview

A common query language for RATS artifacts, based on CBOR and CoRIM

Trust Anchors

Reference Values

Endorsed Values

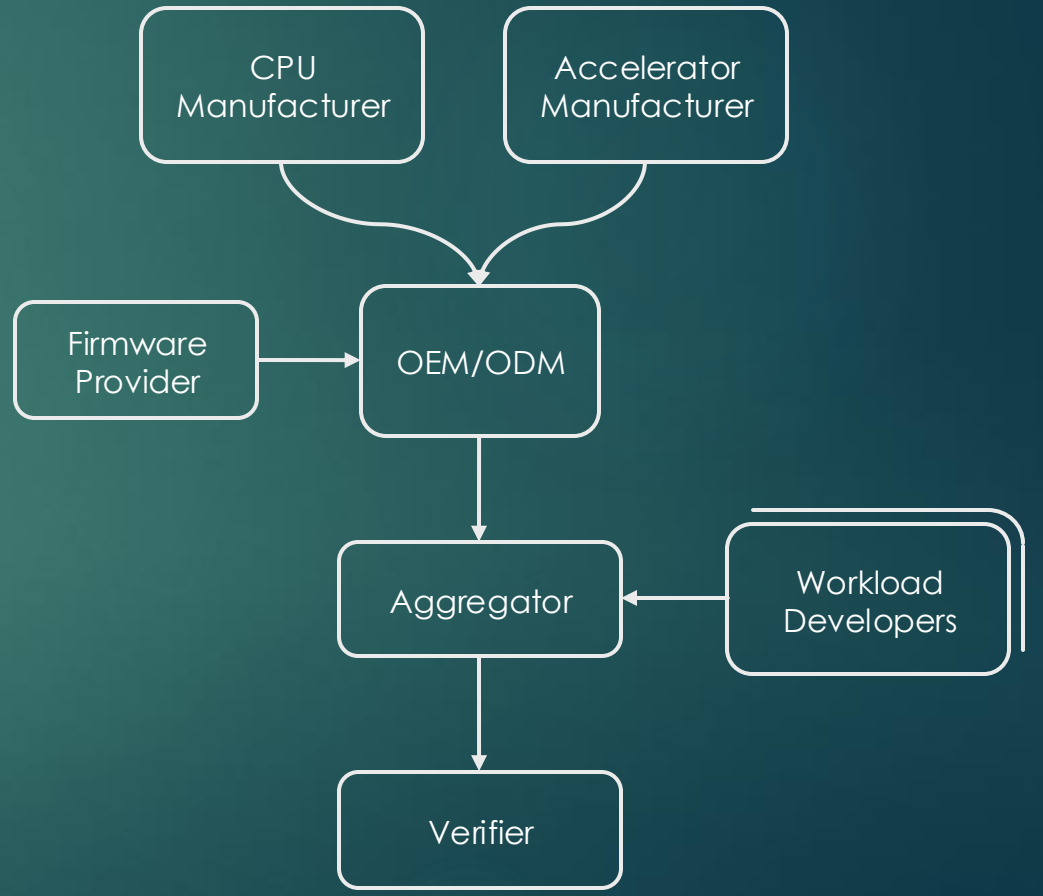
Supporting flexible interactions and transports

HTTP REST

CoAP

One-shot or pub/sub

Supporting real-world supply chain complexity



https://datatracker.ietf.org/doc/draft-howard-rats-coserv/

IETF Draft Updates

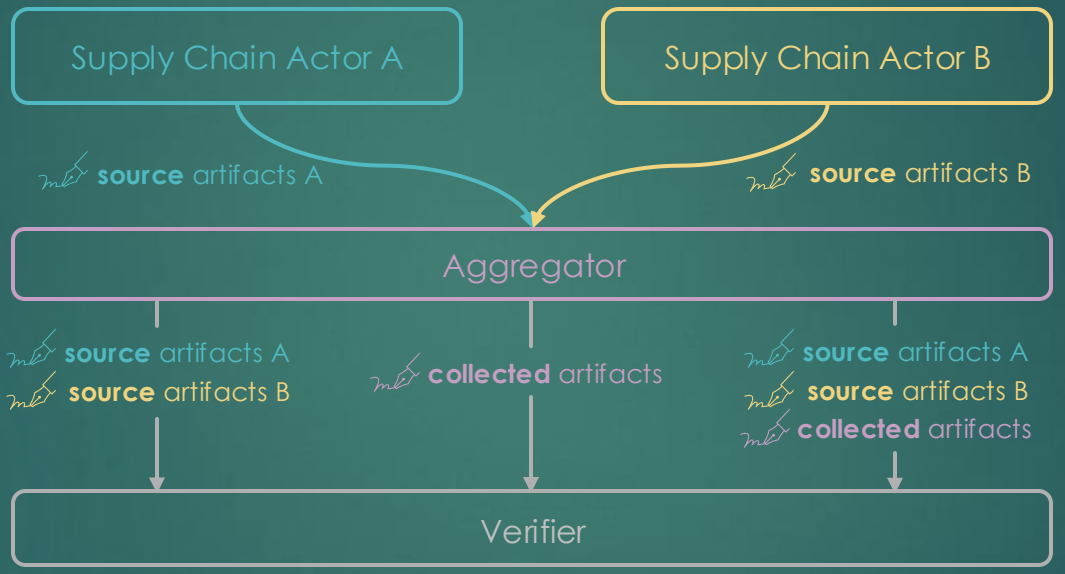
Welcome!

Shefali **Kamal**
FUJITSU

Henk **Birkholz**
FRAUNHOFER SIT

Joining as IETF draft co-authors

Trust Models



Broker Model
Pass-through of source artifacts with their signatures

Shallow Trust
Verifier trusts aggregator only

Deep Trust
Verifier trusts aggregator, but also needs to verify signed sources

Stateful Environments

Aspects of **attester state** can now be captured as **measurements** in a CoSERV query

Allows the provider to produce the correct artifacts **in respect of that state**

e.g. TCB versions needed to obtain AMD SEV-SNP certificate

Implementation Updates (Veraison)

- CoSERV CBOR data model implemented to latest specification in mainline corim library
- Veraison coserv branch supports endorsement distribution HTTP endpoint:

GET https://<*veraison-host*>:11443/endorsement-distribution/v1/coserv/<*base64-encoded-coserv-query*>

- Trust Anchors and Reference Values can be queried from Veraison's **internal data stores** via existing plug-in mechanism
- New "proxy" plug-ins allow artifacts to be retrieved from **external services**
- Proxy plug-ins implemented for **NVIDIA RIM service** and **AMD KDS**
- This will be presented as a hackathon project at IETF-123 in Madrid

Resources

- CoSERV presentation at IETF RATS Interim Meeting 2025-05-02
- CoSERV presentation at CCC Attestation SIG Meeting 2025-05-17
- Detailed slides
- CoSERV IETF draft
- IETF-123 hackathon project
- Veraison CoSERV development branch

Questions/Discussion