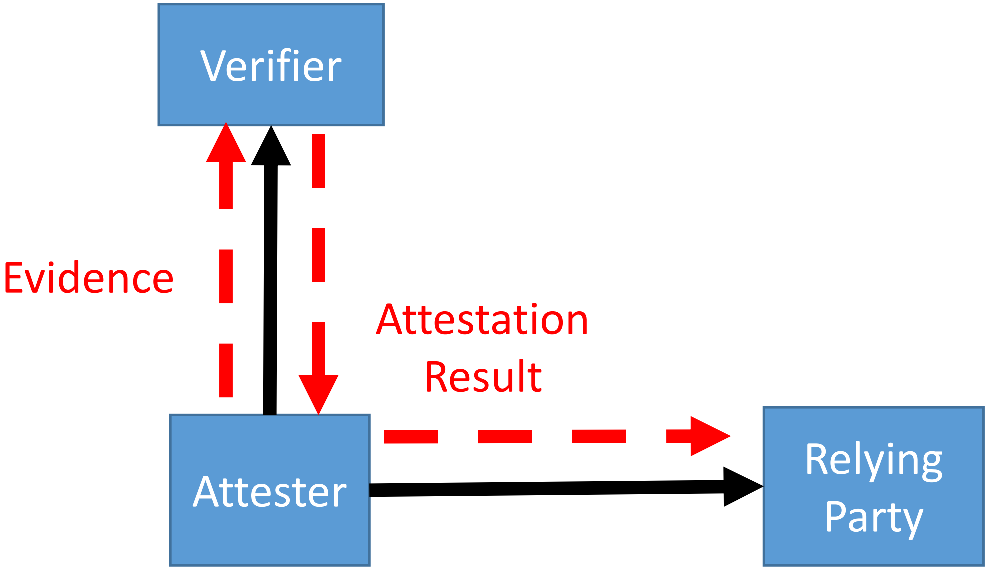
TEEP + RATS Alignment

Dave Thaler <dthaler@microsoft.com>

RATS models

“Passport” model:



Verifier

Evidence

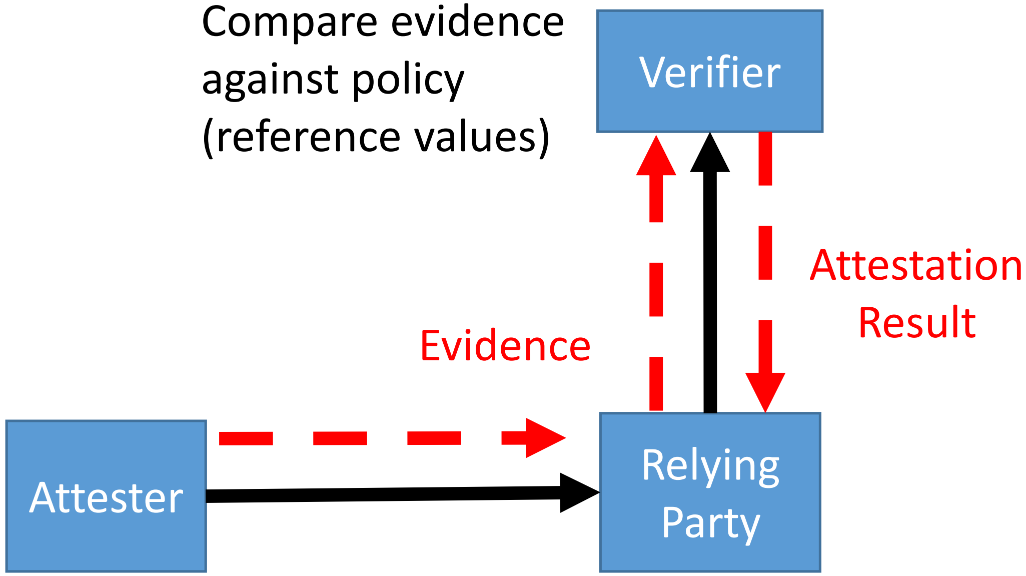
Attestation Result

Attester

Relying Party

Compare attestation result against policy

“Background check” model:



Compare evidence against policy (reference values)

Verifier

Attestation Result

Evidence

Attester

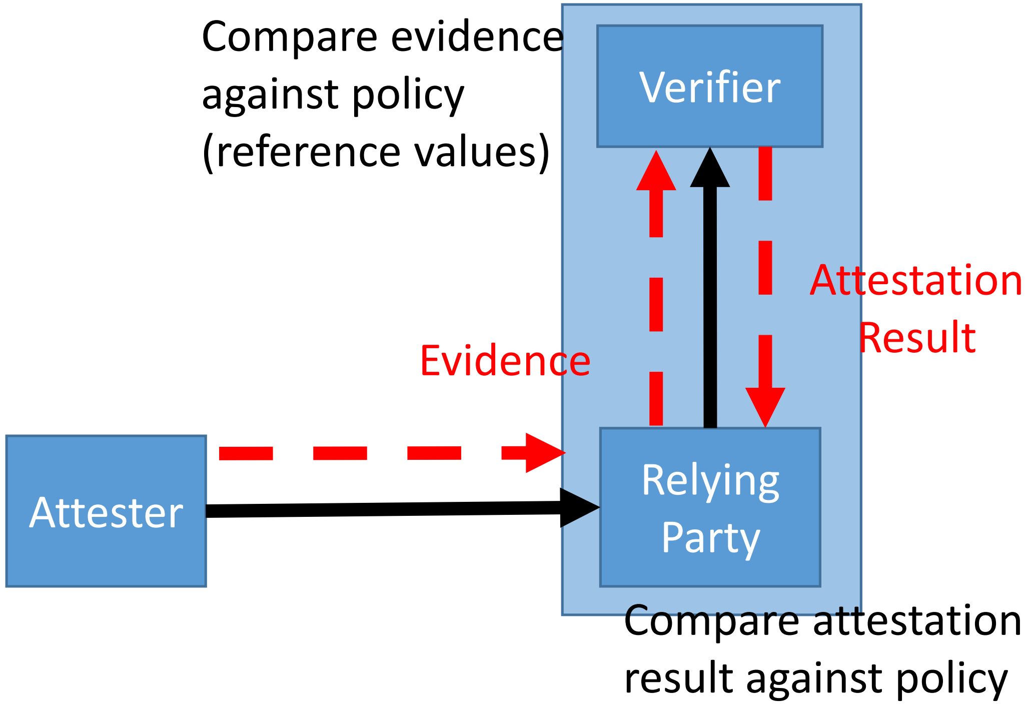
Relying Party

Compare attestation result against policy

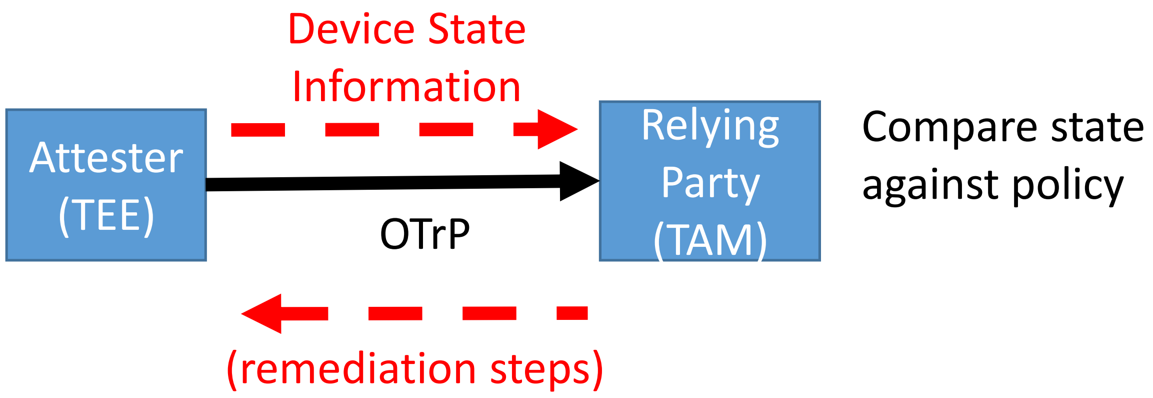
RATS models

Verifier could also be combined into same device Relying Party

“Verifying RP” model:


Compare evidence against policy (reference values)
Verifier
Attestation Result
Evidence
Attester
Relying Party
Compare attestation result against policy

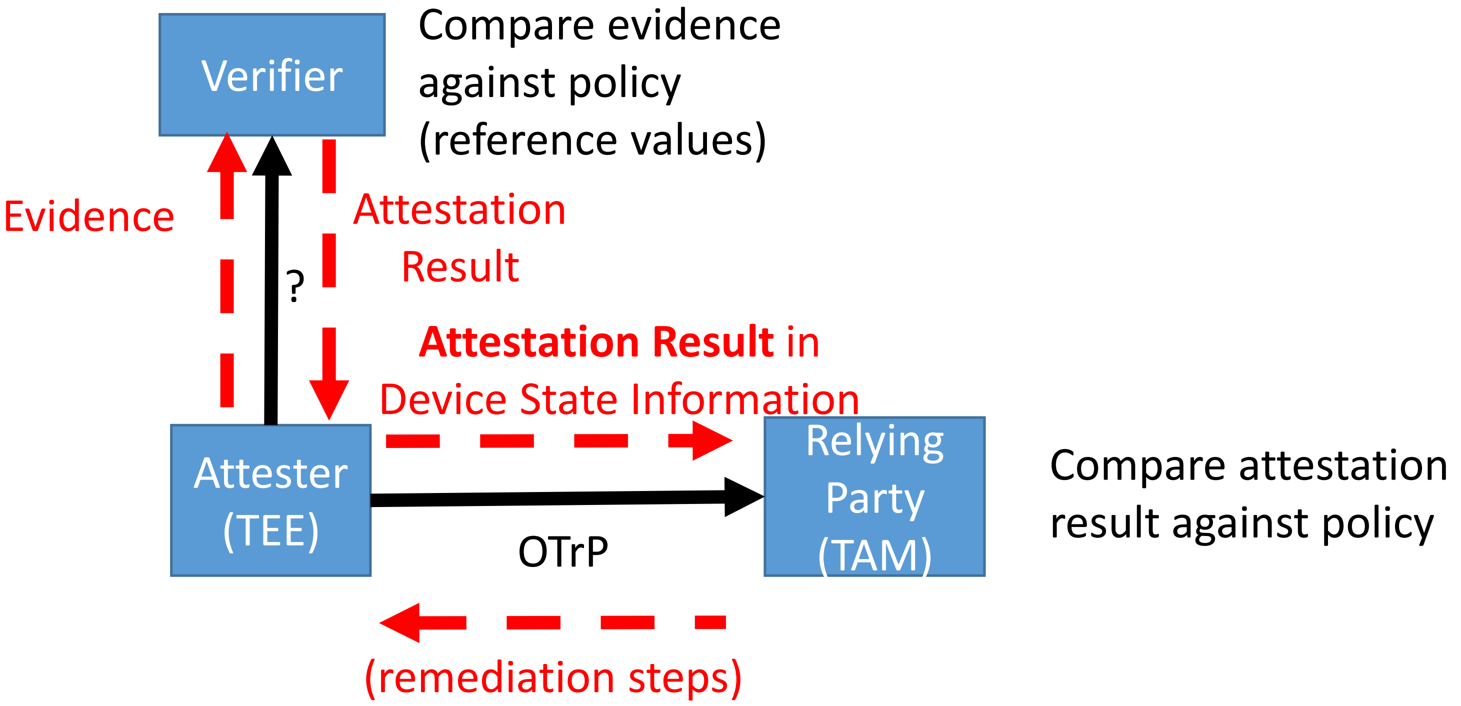
OTrP model for device state



There are at least 3 ways this *could* be combined with RATS models

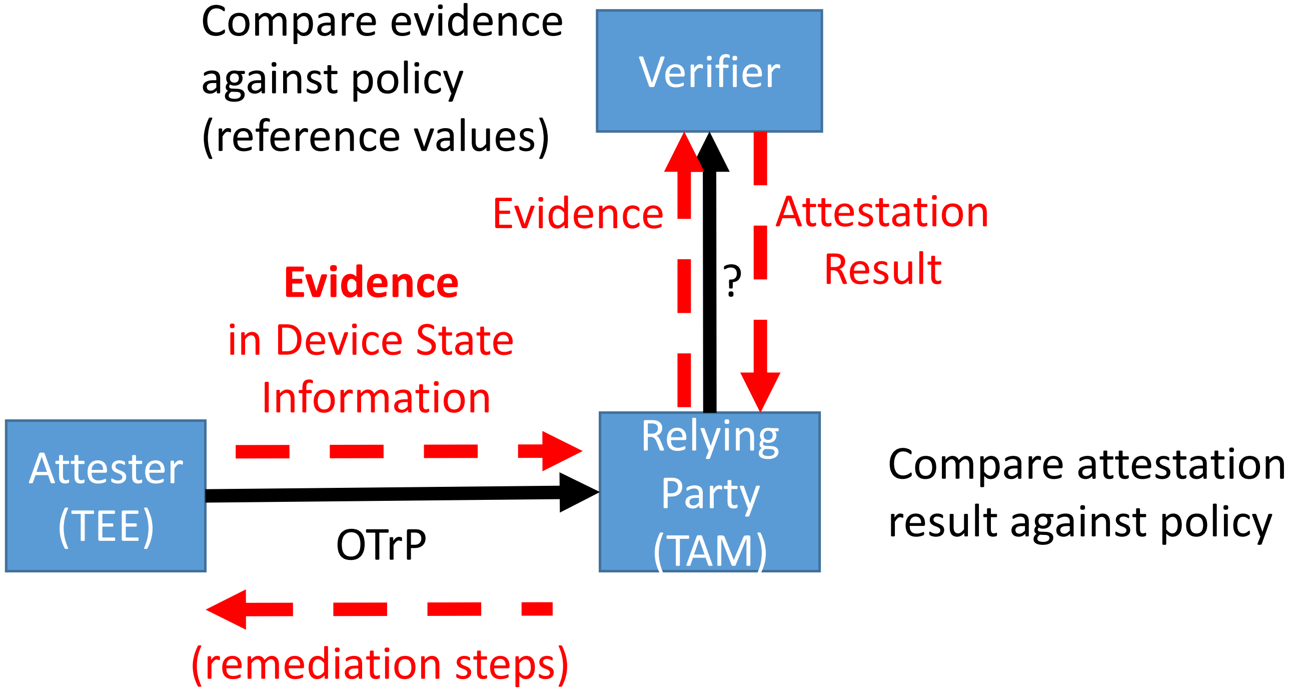
Option 1: Verifier and TAM used separately

Based on “Passport” model:


Verifier
Compare evidence against policy (reference values)
Evidence
?
Attestation Result
Attestation Result in Device State Information
Attester (TEE)
Relying Party (TAM)
OTrP
Compare attestation result against policy
(remediation steps)

Option 2: Chained roles

Based on “Background check” model:



Compare evidence against policy (reference values)

Verifier

Evidence

?

Attestation Result

Evidence in Device State Information

Attester (TEE)

OTrP

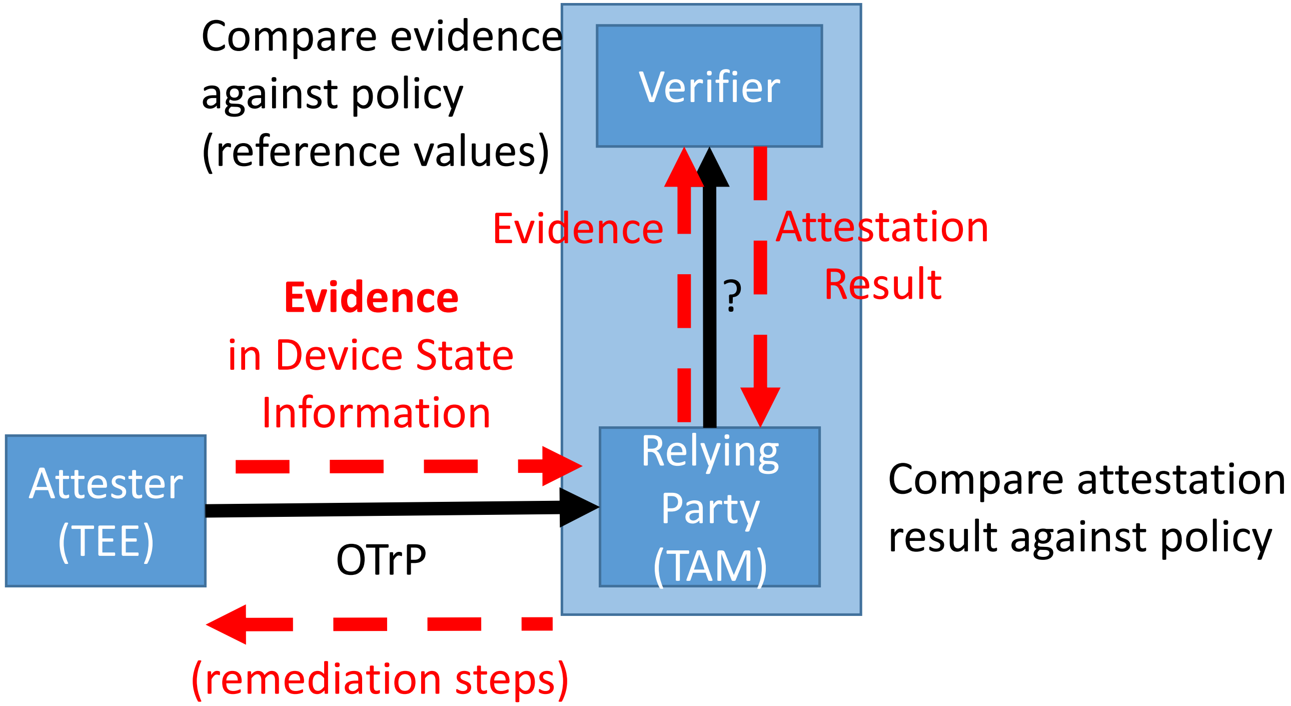
Relying Party (TAM)

Compare attestation result against policy

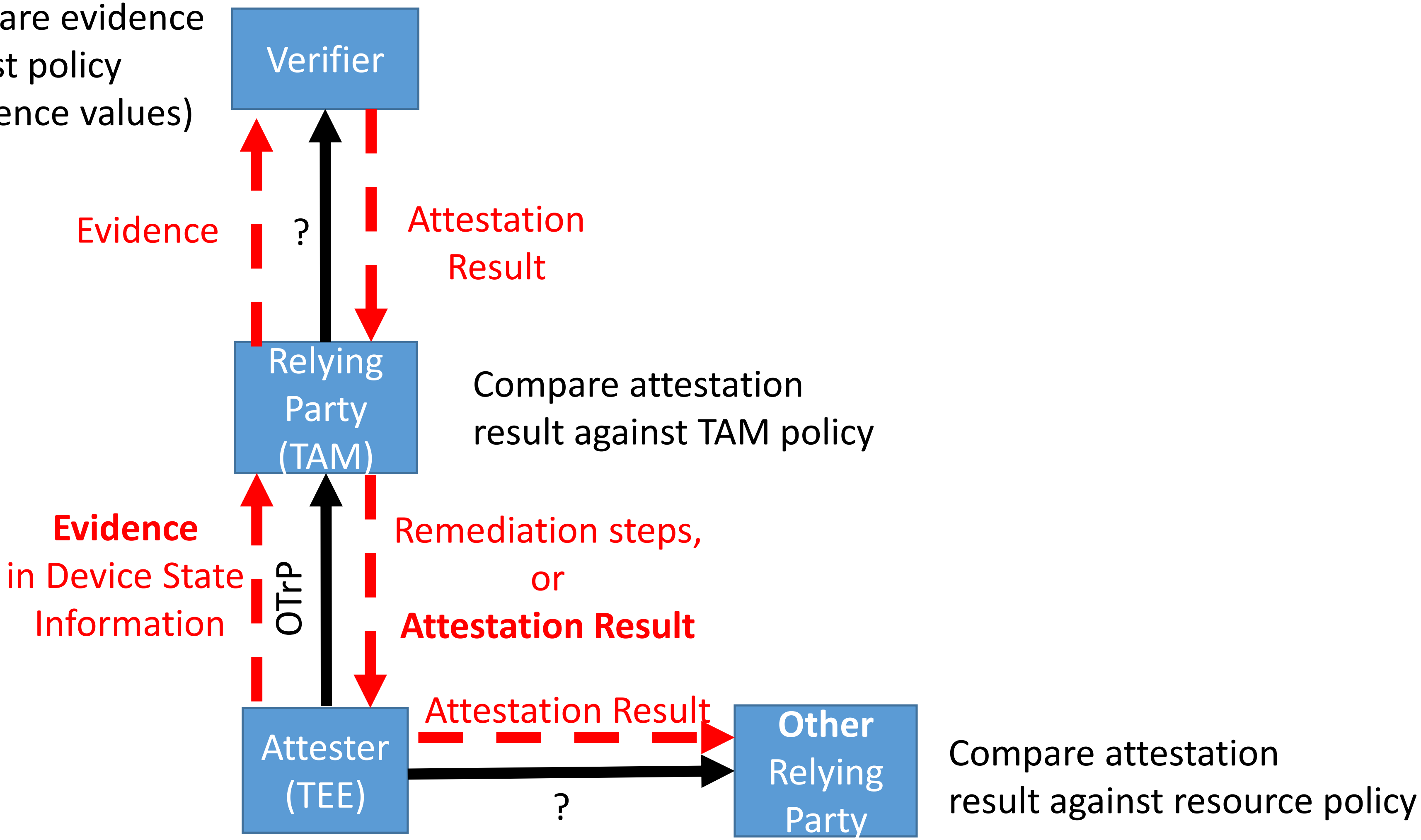
(remediation steps)

Option 3: Combined TAM/Verifier

Based on “Verifying RP” model:


Compare evidence against policy (reference values)
Verifier
Evidence
?
Attestation Result
Evidence in Device State Information
Attester (TEE)
Relying Party (TAM)
OTrP
Compare attestation result against policy
(remediation steps)

Advanced use of OTrP in “Passport model”



Compare evidence against policy (reference values)

Verifier

Evidence

?

Attestation Result

Relying Party (TAM)

Compare attestation result against TAM policy

Evidence in Device State Information

OTrP

Remediation steps, or **Attestation Result**

Attestation Result

Attester (TEE)

?

Other Relying Party

Compare attestation result against resource policy

Freshness

- RATS wants a nonce in a challenge ensure freshness of info
  - OTrPv1 has RID in GetDeviceStateRequest,
    and in signed GetDeviceState response,
    but not inside the encrypted DSI part of the response
  - OTrPv2 proposal has NONCE in QueryRequest,
    and inside EAT in QueryResponse
- Nonce alone does not ensure result is still valid at time of receipt
  - Policy might have changed since sending the attestation result
    - Covered in OTrP by accepting a time window for periodic policy change checks
  - Device might have rebooted since sending the evidence
    - Covered in OTrP by restarting TEEP Agent (Attester)<->TAM (RP) exchange

Claim sets for TEEP use

- draft-ietf-teep-architecture-03, section 7.3:
  - “it is expected that extensions to the attestation claims will be required as new TEEs and devices are created, the set of attestation claims required by TEEP SHALL be defined in an IANA registry. That registry SHALL be defined in the OTrP protocol with sufficient elements to address basic TEEP claims, expected new standard claims (for example from https://www.ietf.org/id/draft-mandyam-eat-01.txt), and proprietary claim sets.”

Questions/Discussion