Unendorsed Tokens

Giri Mandyam

John Hillan

Jeremy O’Donoghue

Background: Reference Architecture

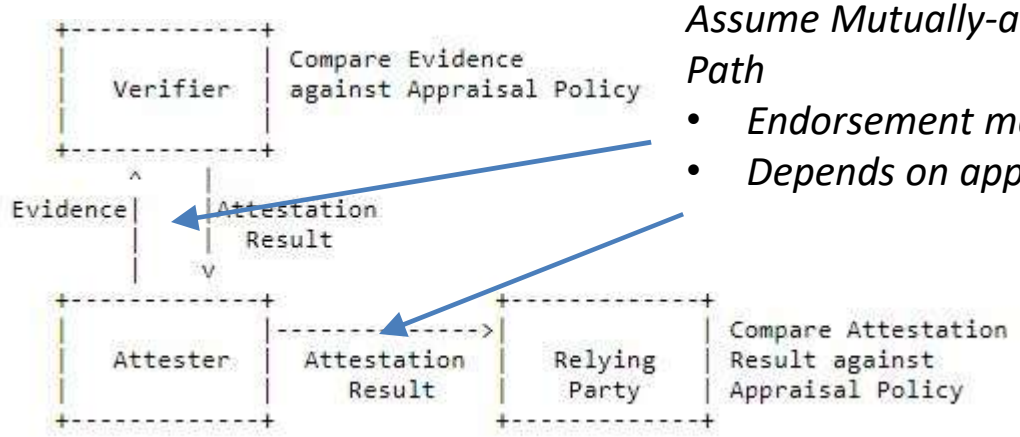
- https://tools.ietf.org/html/draft-ietf-rats-architecture-01
- Relevant terminology
  - Attestation Result: The evaluation results generated by a Verifier, typically including information about an Attester, where the Verifier vouches for the validity of the results.
  - Attester: An entity whose attributes must be evaluated in order to determine whether the entity is considered trustworthy, such as when deciding whether the entity is authorized to perform some operation.
  - Endorsement: A secure statement that some entity (typically a manufacturer) vouches for the integrity of an Attester's signing capability.
  - Endorser: An entity that creates Endorsements that can be used to help evaluate trustworthiness of Attesters.
  - Evidence: A set of information about an Attester that is to be evaluated by a Verifier.

Ref. Arch. (cont.)

- Sec. 8.3 (“Attestation Results”) states
  - “Finally, whereas Evidence *is signed* by the device (or indirectly by a manufacturer, if Endorsements are used), Attestation Results *are signed* by a Verifier, allowing a Relying Party to only need a trust relationship with one entity, rather than a larger set of entities, for purposes of its Appraisal Policy.”
- Lack of endorsements can also be considered in execution of appraisal policy – how can this be addressed in RAts specifications?

Ref. Arch. – Trusted Paths

- Passport model

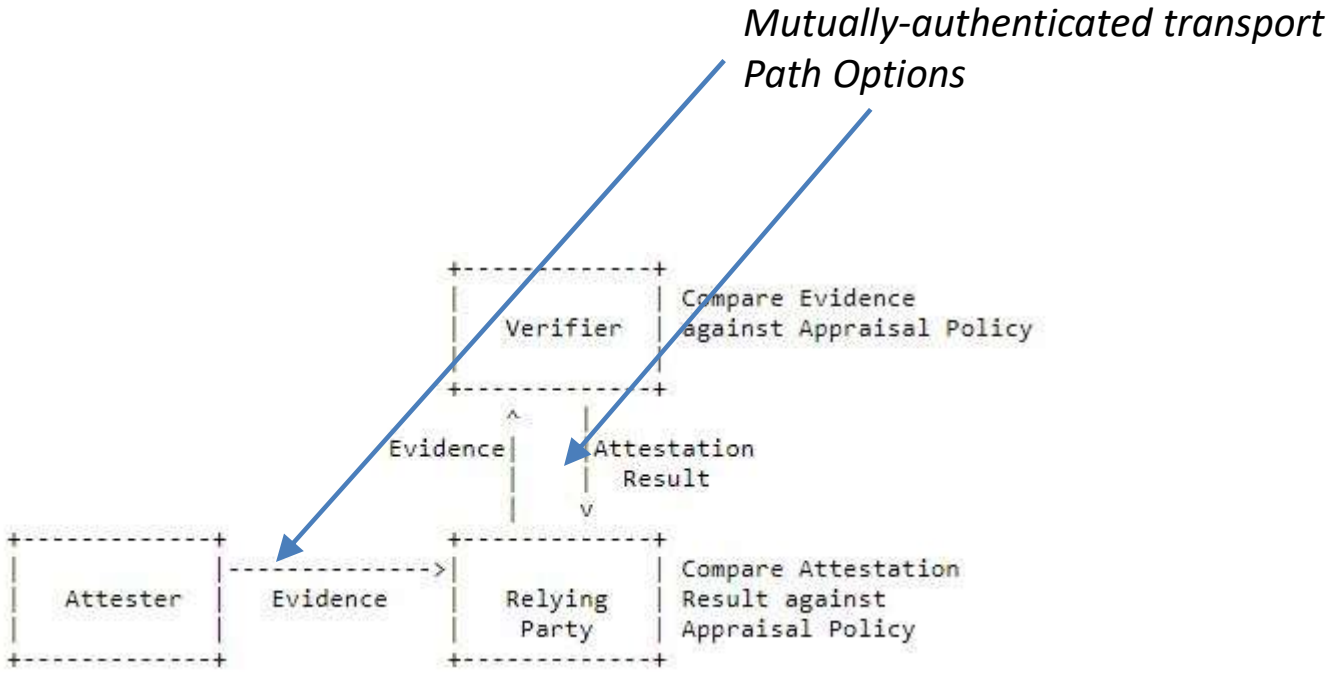


Assume Mutually-authenticated transport Path

- *Endorsement may not be required*
- *Depends on appraisal policy*

Trusted Paths (cont.)

- Background Check



Does CWT Allow for Unendorsed Tokens?

- RFC 8392 seems to allow it
  - "Depending upon whether the CWT is signed, MACed, or encrypted ..."
    - https://tools.ietf.org/html/rfc8392#section-7.1
- RFC 8392 also states
  - "If present, the CWT tag MUST prefix a tagged object using one of the COSE CBOR tags."
    - https://tools.ietf.org/html/rfc8392#section-6
- RFC 8152 (COSE spec) defines two constructs: the COSE object and COSE message type
  - https://tools.ietf.org/html/rfc8152#section-2
  - COSE object includes protected headers, unprotected headers, message content
  - Valid message types are: -sign, -sign1, -encrypt, -encrypt0, -mac, -mac0
    - Not clear what RFC 8152's recommendation is for unendorsed messages

Why Send and Unendorsed Token?
…even if the path is trusted

- Some resource-limited devices may want to avoid exercising their crypto engines when not absolutely required by appraisal policy
  - e.g. for power reasons
- Some transport paths may be trusted and throughput-limited
  - LTE Narrowband IoT for instance (~10's of kbps)
  - Crypto overhead can be costly

Why Solve this in rats?

- Would like an interoperable solution for unendorsed tokens
- Leverage existing standardized formats
  - EAT/CWT/COSE
- Avoid custom protocols based on attestation payload
  - e.g. sending EAT payload as CBOR object
    - How is it distinguished from other CBOR objects sent as part of a communications session betw. RP/Verifier and device?

Ways Forward

- Some options (not all are mutually exclusive)
  - Extend arch. spec. to address unendorsed tokens
  - Define new COSE msg. type
  - Define CBOR tag for attestation payload
  - Extend COSE algm. registry with mode that can be leveraged for unendorsed tokens
    - e.g. zero-length MAC/Hash
- Recommended solution
  - Work with COSE WG to determine best way forward for unendorsed COSE message
  - Architecture team defines recommended practices for unendorsed COSE tokens