Security Considerations

Current PR addresses the following:

a) Overall: will need to harmonize terminology with RAts architecture

b) Best practices on creation/transport of key material
   a) Manufacturer-created and –provisioned key material
   b) Creation of key material in an enclave (as defined in RFC 4949)
   c) Transport of key material (post-creation)
      a) Enclave-to-enclave: secure transport with key protection, encrypted storage, human courier

c) Transport security
   a) Leverage CWT/JWT transport security guidelines as much as possible
   b) Discussion on anti-replay
      a) Which actor creates the nonce
      b) Role of intermediaries
Security Considerations (cont.)

d) Multiple EAT “consumers”
   • Will need to replace “consumer” with architecture terminology
   • Discusses security considerations involving
     • Verifiers who are providing attestation results downstream
       • Verifiers may need to attest to their own security state
       • Verifiers for specific submods
     • Does this discussion belong in architecture doc?

e) What topics are missing?
Security Considerations (cont.)