Notetakers:
   Ned Smith

Chairs: Kathleen Moriarty, Nancy Cam-Winget, Ned Smith

Agenda bashing
- 5 min logistics
- 5 min hackathon report
- 10 min design team report
- 10 min EAT update
- 15 min Unendorsed tokens
- 10 min Trusted Path Routing
- 5 min AOB

Hannes - Hackathon reporting
- Presented slides at Securing the IoT Hackathon in Germany
- 45 participants, 3 topics: RATS,SUIT, TEEP
- https://siot-hackathon.github.io
- Impressions
- Tutorial day - was it useful?
- Nancy - Was there a tutorial for all three topics? (Yes)
- Some people were very experienced, others were not that experienced
- Dave Thaler - separate sequential tutorials were given.
- Code and documentation was updated - thought to be quite useful
- Some people haven't met before
- Found a couple of bugs
- It's difficult to make progress in 2 days unless familiar with it already
- a few people dropped out
- TPM attestation, QCBOR/t_cose, CHARRA <https://github.com/Fraunhofer-SIT/charra>code bases were worked on
- Nancy - take up topic on list to follow up on hackathon feedback and how to plan for future hackathons
- Michael - lot of logistics that can be leveraged in future hackathons (in particular, the mailing list that was created)

Design Team Report (Michael Richarson)
- Arch Design team - 9 people attending regularly
- Draft 02 plans:
- 6 use cases
- Reworked composite Attester -> Composite Device terminology resolved
- Many small wording changes
- Todo
- Introduction
- Terminology
- Need to get consensus on layered approach pull request
- Please review
- Meeting tommorrow: Last meeting before draft deadline
- Can discuss WGLC could start after IETF107
- Input now is better than after the draft deadline.

- Large objections better now vs. later
Laurence - should they be filed as issues?
Michael - Issues, email are all OK. (Michael will echo this on mailing list)

EAT Update (Laurence Lundblade)
- Closing out initial set of claims / issues
- Debug State claim
- What does it mean if no debug claim is provided?
- Could be unknown or provided in a proprietary claim
- EAT draft updated with explanation that there are no default values.
- Laurence wants to merge this into the EAT draft
- Would like to separate debug state from boot state.
- Everybody OK with merging splitting the debug state from boot state?
- Giri - As long as merge doesn't prevent vendors from doing debug and boot state in a proprietary way.
- Laurence - proprietary approaches diminish these claims. Is there a reason vendors can't use these claims?
- Nancy - Merge and ask for feedback.
- Make EAT and Update to RFC 8932 (CWT)
- Additional guidance on designing claims
- CWT fix: disallow floating point CBOR for dates (HW, SW and compilers don't support floating point)
- Michael - updating IANA considerations or more significant than this?
- Henk - JWT conflicts with OAuth list use of inherited(?) claims.
- GPU world would like unsigned tokens. Can't tag it with CBOR token in the right way if it is unsigned
- We've learned a few things since CWT was written, so it makes sense to update
- Dave Thaler - Agree with most of the slides; Propose splitting the document into two parts: A separate document would be updates to 8392; EAT should remain in RATS
- Laurence - OK. That makes sense.
- Henk - Clarification, tokens that are not signed are not tagged; CWT update document would clarify this.
- Laurence - looking for help on how to engage

Unendorsed Tokens (Giri Mandyam)
- Other people at Qualcomm provided input
- https://tools.ietf.org/html/draft-ietf-rats-architecture-01
- Relevant Terminology:
- Attestation Result:
- Attester:
- Dave Thaler: Endorser and Attester are separate roles. They may not be on the same device.
- Giri: These could be functional separations (but combined on the same entity)
- Henk: ??? (low microphone)
- Dave T: Endorser is whatever the manufacturer is

- Giri: Not sure that is reality
- (some discussion about what vendors implement and what the terminology means)
- Dave T: Endorsement is signed by a manufacturer's key.
- Giri: A Qualcomm device key isn't signed by a manufacturer.
- Dave T: Endorsement allows verifier to determine if device is/isn't a "knock off"
- Laurence: This was clarified at the hackathon (Endorsement semantics). Used to think endorsement was the verification key
- Giri: Talking about unsigned tokens today
- Evidence is signed by the device
- Attestation Results signed by Verifier
- Lack of "endorsments" (unsigned tokens)
- There are "trusted paths" in Passport Model
- If there is a trusted path that is anchored by mutually authenticated transport paths then there isn't a need for signed tokens
- Examples: Attester->Verifier:
- Dave T: It is implicitly signed because the transport provides signing
- Giri: Yes, that is a good way of thinking about it.
- Giri: Replace 'endorsed' with 'implicitly signed' in your
- Giri: Terminology to be updated to define implicitly signed
- RFC8392 seems to allow "it" - "Depending upon whether the CWT is signed, MACed, or encrypted..."
- RFC 81?? also unclear(?) - Defines COSE Object and COSE message type.
- Why send unendorsed Token?
- Some resource-limited devices may want to avoid exercising their crypto engines
- Why solve this in RATS?
- Interoperability
- Leverage EAT/CWT/COSE
- Avoid custom protocols based on attestation payload
- e.g. sending EAT payload as CBOR object
- Ways forward
- Some options are not mutually exclusive
- Extend arch to address unendorsed tokens
- Define new COSE msg type
- Define CBOR tag for attestation payload
- Extend COSE algm registry with mode that can leverage
- Rcommendation
- Work with COSE WG to determine best way forward
- Arch team to define recommended practices for implicitly trusted (unendorsed tokens)

Questions:
- Dave T: I wonder if this could be combined with the "update" to CWT RFC?
- Giri: OK
- Laurence: Should begin with an unsigned object

- Dave T: Does it make sense to combine (@Laurence)
- Laurence: Yes
- Nancy: Recommend continuing duscussion on email list

Eric Voit - Trusted Path Routing
- Includes reference to RIV draft on attestation for network equipment
- Looking for feedback to identify gaps (terminology, concepts, arch, etc)
- Slide showing a sample route traversing multiple router nodes but excluding an "untrusted" node
- Centralized model
- Verifier pushes "paths" to router nodes based on those that are trusted/untrusted
- Distributed model
- Passport is delivered to the routers and they supply passport to peer routers
- If passport is good then link is added to the topology
- Three modes
- Attestation event stream: YANG draft already captures this mode
- YANG notifications contain evidence of trust state
- Trusworthiness "levels"
- Trust can be nore than binary
- Draft Fedorka identifies what is in each PCR
- Is there a middle ground?
- Composite Evidence Passport
- Combines the results of a first verifier with additiona evidence taken moments later such that there is a time-based "history?" or sequence of Evidence and Results
- Laurence: Trustworthiness is in the "eye of the beholder": eg the Relying Party. Asking if it makes sense broadly. Maybe qualify as "trustworthiness for routers"
- Eric: OK.
- Laurence: Levels should be qualified as applying to routing domain
- Guy: Goal is to define common terminology - assuming there is agreement among the industry.
- Nancy: Can you present again at 107?

Nancy:
    - Anything else (30 seconds)
    - Let RATS chairs know agenda items for 107
    - Concerns about Mondy and Friday (split)
    - Guy: Will try to be there for both, but can topics be organized based on who is present for which days?
    - Nancy: Yes.
    - Kathleen: Many people will be remote (including Kathleen, Ned and maybe Nancy)
    - Kathleen: Should we plan for being remote and ways to substitute for hallway conversations? Chairs looking for suggestions
    - Hannes: Missed you at hackathon :-)
    - Hannes: Also look at remote hackathon participation?

- Kathleen: Yes, that is also a good idea.
- Hannes: Start email discussion on how to do remote hackathons
–Nancy: endedmeeting 8:04 PST