RATS agenda for Tuesday November 17, 2020

Jabber: xmpp:rats@jabber.ietf.org (mailto:xmpp:rats@jabber.ietf.org)?join
MeetEcho: https://www.meetecho.com/ietf109/rats (https://www.meetecho.com/ietf109/rats)
Notes <rel="self">: https://codimd.ietf.org/notes-ietf-109-rats (https://codimd.ietf.org/notes-ietf-109-rats)

Notes takers:

- Thomas Fossati (tf)
- Wei Pan (wp)
- Ned Smith (ns)

Agenda bash (5min)

- slides: https://datatracker.ietf.org/meeting/109/materials/slides-109-rats-sessb-chair-slides-00 (https://datatracker.ietf.org/meeting/109/materials/slides-109-rats-sessb-chair-slides-00)

Agenda bashing?

Henk Birkholz (hb)

hb: missing item: state of UCCS

Architecture Update

- document: https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/ (https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/)
- slides: <TBD>
- presenter: Michael Richardson (mcr)

Nancy Cam-Winget (ncw): authors: did you receive any feedback on the mailing list?
ncw: how many have read the latest arch draft? 11 yes, 13 no.
Eric Voit (ev): Has volunteered to read the draft
Dave Thaler (dt): anything we should do differently based on the IPR declaration?
ncw: echoed Dave's question.
km: There may not be an issue due to prior IPR. Affects the composite device section and attestation section. Does it matter if there is prior IPR?
ncw: we need to check with our respective corp: how does IPR filed in China impacts?
hb: plan to do an editorial pass for consistency (no technical change) after WGLC comments come in
ncw: I want at least three people to review other than the authors and say it's ready to go
Guy Fedorkow (gf): (having audio difficulties) Volunteered to read arch draft.
ncw: Guy, Thomas and Eric
km: Section 7 content is very different, so please focus reading here.

CHARRA Update

- document: https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/ (https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/)
- slides: https://datatracker.ietf.org/meeting/109/materials/slides-109-rats-sessb-charra-update-00 (https://datatracker.ietf.org/meeting/109/materials/slides-109-rats-sessb-charra-update-00)
- presenter: Eric Voit (ev)

`slide#2: purpose and scope`

ev: provide a YANG data modelfor network equipment: challenge-response protocol to retrieve PCR quotes using TPM v1.2 and v2.0 from the device
There is a YANG doctor review underway. Mahesh(?) is providing feedback currently to the authors.

`slide#3: relationship to other drafts`

ev: CHARRA is part of a bigger picture document roadmap, including architecture, interaction model. there are also dependent documents
There is a network device subscription draft that will also be added to the roadmap when it is furthur along. Other drafts are planned to be integrated into the YANG model.

`slide#4: issues addressed (from interim)`

ev: a number of issues were reviewed during the interim meeting.
A YANG model was added with all the TCG algorithm type definitions. Removed various redundancies, errors and grammar.

`slide#5: open issues`

ev: XPath expression review to validate some extra data integrity, needs YANG doctor review. after they are done we will be addressing their comments.

ev: maximise commonality between TPM v1.2 and v2.0 – we need a v1.2 expert to iron out the details. This reamains an open issue.

`slide#6: closed issues`

ev: tpm-name and node-id included in the RPCs
There is no objection to the minimized RPC option?

`slide#7: next steps`

ev: Next steps, once issues are done go for WGLC
ncw: Do you know anyone who could help with TPM validation?
ev: not really. there is also the option to remove 1.2 altogether but this is not ideal
gf: I will dig in TCG to find an expert that can help us out here
ev: That will be great. It could be a group meeting if they are not a YANG expert.

Interaction Models Update

- document: https://datatracker.ietf.org/doc/draft-birkholz-rats-reference-interaction-model/ (https://datatracker.ietf.org/doc/draft-birkholz-rats-reference-interaction-model/)
- slides: https://datatracker.ietf.org/meeting/109/materials/slides-109-rats-sessb-report-on-rats-reference-interaction-models-00 (https://datatracker.ietf.org/meeting/109/materials/slides-109-rats-sessb-report-on-rats-reference-interaction-models-00)
- presenter: Henk Birkholz (hb)

```
slide#2: interaction models
```

hb: some development: an emerging open-source on the verifier side (https://github.com/veraison (https://github.com/veraison))
This is a project highlited that focuses on implementation of the interaction model.

```
slide#3: recent activities
```

hb: draft adopted before last interim. No new content was suggested since the last interim.

```
slide#4: current activities
```

hb: review requested on two sections in particular: S6, which include *normative* language, and S7, which deals with generic information elements required for attester and verifier roles. Possibly there are confusing phrases etc... that would be nice feedback to get.

```
slide#?: track?
```

hb: is normative language compatible with informative status? or does this need standards track?
For now we'll leave it informational unless something changes.

Ira McDonald(im): (on chat) suggests it remain informational.

dt: leave it informational because implementations do not directly conform to the interaction model, just indirectly via a protocol spec

ncw: That's it.

EAT Update

- document: https://datatracker.ietf.org/doc/draft-ietf-rats-eat/ (https://datatracker.ietf.org/doc/draft-ietf-rats-eat/)
- slides: https://datatracker.ietf.org/meeting/109/materials/slides-109-rats-sessb-eat-status-00 (https://datatracker.ietf.org/meeting/109/materials/slides-109-rats-sessb-eat-status-00)
- presenter: Laurence Lundblade (ll)

```
slide#2: Proposed Contents of an EAT
```

Laurence Lundblade (ll): list of topics expected to be covered in EAT. only get to WGLC when all these topics are covered. question: is this the list?
Topics: HW Identification, SW Identification, Running State, Measurmeent of RS, Nonce/Timestamps, Identity of Verifier, Context, Purpose, Profile, Submodules, Nested EATs, Public Keys, GPS Location...

```
slide#3: Level of Completion in EAT Draft
```

ll: SW identification: there seems to be consensus on using CoSWID for SW identification, but still need to iron out details (see Issues on the SACM/CoSWID draft repo).

Security Characterization topic - There are pull requests, other comments and open issues.
Nonce and Timestamps - Pretty close to done, not planning to discuss today.
Identity and verifier input - The last couple presentations have been around this topic, some consensus and still more writing to do.
Giri has comments related to the profile discussion.
Submodules and nested EAT: PR close to be ready C implementation is in progress, the nesting has some complexities but appears to have consensus on how it fits together.
GPS location - a couple of outstanding comments to be addressed.

`slide#4: Other EAT Work`
ll: There are a few other topics not showing up on the previous slide.
We need more examples, align with the architecture document terminology
ll: (Going back to the previous slide.)
Q: are there comments: are these the claims we need to have before going to WGLC?
hb: I think the diagram is helpful. From the current 'go-with-the-flow' is there is a strong focus on the Attester comes with some form of IDs and Endorsement. Do you anticipate this being supplied by the Attester vs. the Endorser?
ll: My focus is just what is in EAT, not other places. I want to provide an identifier for endorsement with the possibility of including that id in the COSE header (so it's not really a claim), e.g., using x5u, x5bag, etc. AS-IS.
hb: So there are hints to the Verifier?
ll: Yes, the COSE headers allow for inclusion of these other elements.
hb: attester-centric, we should point that out early in the text.
ll: The next topic is EAT for Attestation Results.
dt: I am familiar with at least one open-source projects (open enclave SDK) that deals with implenenting TEEs. As far as the endorsement, we have demands on endorsements to be pre-cashed on the attester and supplied with the evidence to the verifier
Both are interesting and should be supported. It just happens to be incuded with the Evidence but is nevertheless considered as Endorsement.
ll: Yes, we plan to allow Endorsements to be included with the EAT.

hb: we need to do some planning here maybe?
Of course the EAT structure is very flexible and there is the notion of composite evidence, but personally recommend drawing a line that distinguishes between the

different types of content. Then there can be a composition construct that allows them to be packaged together. That allows complementary drafts that describe how the various types of information are combined/grouped rather than calling for merging / grouping them in the EAT draft.
ll: Interested in EAT being more comprehesive vs. lots of smaller drafts.
hb: the problem I see with “merging” is that it could take quite a while to finalise the document
ll: Focusing on Endorsements, the work will focus on identifiers of Endorsements rather than claims definitions.

`slide#5: Discussion: EAT use for Attestation Results`

ll: Several discussion points - we’ll likely use the rest of the time here. How far do we go with attestation results? Many EAT claims will pass through the Verifier and end up in attestation results. therefore, there is an interest to have pure pass-through (e.g., CoSWIDs, HW identification and version) without the need to rewrite at the Verifier. We don’t want to define new claims for Verifier in Attestation Results.

ll: For example, verification status claim, reference value checking result claims, certification status
and this is possibly a lot of work, maybe more than we want to take on for EAT.

dt: (from chat) Attestation Results are the main case I’m interested in using. The “pass through” shold be “pass through if policy says to do so”
dt: agree with almost everything on the slide other than one small amendment: what gets passed through depend on the appraisal policy – which I think is what you really mean
ll: yes it is
dt: I wouldn’t like to see them defined elsewhere as many claims will be passed through. I’m in favor of getting the new claims done sooner than later as it is unlikely implementations can go forward until all the claims are defined.
dt: Attestation results may have other claims added by the Verifier, that might use the layered or nested structure – which is already in place so there should be no extra work wrt that
km: The TPM log file is another way to provide evidence right?
ev: I love the idea of reuse. in the trustworthy path draft there are 10 claims that could be taken as a strawman for some of these attestation-result claims such as hardware

authenticated, …
ll: ok, I'll read the draft
hb: what Dave said is great, because it sort of removes my concerns.

ncw: Lets pause here and see if there are other topics for thursday that we may want to discuss now?
ll: Might be good to let Giri go now?
ncw: Is 39 minutes enough to cover the reamaining topics?

```
slide#6: Discussion: Work on Identifying Verifier Input
```

ll: key identification (COSE kid or the COSE x509 draft which is currently in the works). Unclear if it will be informational or standards track.
ll: Headers for identifying endorsements and
ll: reference values; and where to find reference values (URIs)

```
slide#7: Discussion: Public Key Inclusion
```

ll: have PK as a claim (e.g., FIDO does this, also FIDO IoT onboarding does it). FIDO user authentication WG is different from FIDO IoT.
there are a bunch of use cases for which Public Key(PK) inclusion as claim is critical. the problem is that the semantics of what the PK means varies a lot depending on use cases. e.g., It may not make sense to include FIDO semantics in EAT. FIDO auth binds PK to a triple (…); in IoT onboarding it's a CSR. But that isn't exactly the right concept. What I put in my PR is to suggest that when using a PK, the format to be used is one of COSE Key or JWK. Maybe we also should use RFC8747 (PoP, confermation claim, defined in CWT). Other claims to consider, security level claim. This seems to be common between FIDO and EAT, but this could be a can of worms. Another possibility is the intended use of a key as claims.
Any comments?

hb: Question: if you include a PK are you approving the possession of the corresponding private?
ll: Um, maybe? When you say PoP is it something like a CSR?
hb: Yes, there is a PoP draft in ACE or somewhere in IETF.
ll: 8747 is PoP draft.
Hannes Tschofenig (ht): Depends on which PK we are talking about here?

km: (from chat) The key about conveying identity of device or software - I guess that adds SPDX, SWID, and CoSWID.
ll: the semantics is higly dependent on use cases. so the PR actively avoids overlaying semantics, it just says use a certain format.
ht: you'd need a "profile" document that specifies the semantics
ll: yes
ht: ok, got it, makes sense.
ll: Looking for discussion on this topic. (silence) I guess everyone is OK with proposed text.
ll: Any interest in security level of key protection? (silence) I'll take that as a no.
tf: Can you repeat the questions?
ll: Can the security level claimis be used to describe the protection characteristics of the key?
tf: There is one use case that comes to mind that might make sense. Would like to discuss offline.
ll: Draft text will be added to capture results of this discussion.

```
slide#8: Discussion: Context, Purpose, Profile
```

ll: Less clear on where to go with this as it is relevant to ARM PSA.
dt: what does profile means? is EKU (extended key usage)?
tf: It is not in PSA claims, it has to do with the interrelation between the claims.
ll: The profiles define semantics of what claims are used and how they are used.
dt: Do you mean an RFC document?
tf: Yes, an informational RFC could be published containing profiles.
ht: (from chat) https://tools.ietf.org/html/draft-tschofenig-rats-psa-token-05 (https://tools.ietf.org/html/draft-tschofenig-rats-psa-token-05)
dt: (from chat) OK, so it isn't something that is passed over the wire?
gm: Yes, that is our intention.
hb: This sounds liike a policy (Appraisal Policy for Evidence) or (Appraisal Policy for Attestation Resuts)
ll: Yes, maybe that is a better way to characterize it.
tf: The policy isn't referenced by the profile. The profile isn't an identifier for the policy.
ll: Thanks for the input.
Giri Mandyam(gm): use case: a client certificate is requested for a TLS connection: the context claims would say that it's used for a CSR. There is a PR for this already.

ncw: There are people on the Q.
hb: How's that different from the audience claims that comes with web tokens?
gm: Yes, it is similar but does not have the same semantics.
hb: audience is used to identify the consumer, the context look same but semantically weaker. Using the Audience claim could make sense too.
gm: they can be used together but audience doesn't capture the semantics that is intended with the context claim. There may be a way to extend the Audience claim, but I don't know how.
hb: Food for thought, but probably already the same as the exiting claim.
ll: What if you have a PoP situation? Does it make sense if used with PoP?
gm: If the attestation evidence is received by an audience that doesn't expect it, then that would be part of the policy in decicing next steps. If the Verifier is only verifying PoP tokens, then there's nothing else for it to do if other claims are supplied.
ll: Do we need a registry of all possible contexts?
gm: Hoping the topic is comprehensive, but if not then we should try to make it comprehensive. If a future use case is defined then a profile would need to be defined.
ll: In FIDO there is a FIDO user verification, user registration context.
gm: The attestation would use 'client-data' to supply the requested credential. Attestation is most likely used out of context. Looks like a registration use case. No concept of runtime attestation.
ncw: time check?
gm: Context shouldn't be considered a blocker.

```
slide#9: Discussion: Measurement of Running State
```

ll: PR filed very recently re: measurement of the running state of a subsystem – TEE: periodicatlly measures the running OS and sends the measurement to the Verifier (e.g., Samsung TIMA).
ll: The TEE can claim success or failure or can send the measurements. This is more valuable than measurements once at boot, e.g., used to detect rooting and things like that before a high value transaction is started. I haven't seen this in CoSWID. Cross check with Linux IMA?
hb: "Evidence" tags can report measurements. Could be component scope of a composite device. It could report a snapshot at a single point in time.
ll: Example describing how a range of memory could be specified for snapshotting.

hb: The current schema may be underspecified.
ncw: Is there a way to close this thread?
ll: Will followup with hb offline.

FIDO and EAT dependencies

- slides: https://datatracker.ietf.org/meeting/109/materials/slides-109-rats-sessb-fido-updates-to-rats-00 (https://datatracker.ietf.org/meeting/109/materials/slides-109-rats-sessb-fido-updates-to-rats-00)
- presenter: Giri Mandyam (gm)

`slide#1: FIDO IoT and RATS/EAT`

gm: making this presentation not as an EAT co-author but as a representative of FIDO

`slide#2: Overview`

gm: FIDO is a standards and certification body mainly concerned with passwordless authentication. Interested in getting feedback from RATS members.

`slide#3: What does onboarding entail`

gm: (my definition of onboarding) - It's where OEM completes mfg and ships it. End user establiishes ownership relationship with the device. Transition between mfg ownership to a user's ownership. Goals include zero-touch (minimal intervention). Ownership is established via cloud service.

`slide#4: Attestation in onboarding`

gm: This for members who are not part of the FIDO alliance. Attestation is a critical part of the onboarding process.

`slide#5: FIDO IoT system architecture`

gm: FIDO IoT architecture. Device may/may not have connectivity. May require an intermediary to complete the connection to the target environment. A rendezvous service is needed to redirect to onboard owner.

`slide#6: Protocols`

gm: 4 protocols defined by the FIDO specification:
1) Device Init
2) Transfer Owner 0 (TO0)
3) Transfer Owner 1 (TO1)
4) Transfer Owner 2 (TO2)
TO1 - TO2 interfaces are attestable.

`slide#7: EAT dependencies`

gm: Can't complete protocol using EAT private space. Therefore, the registered claims are needed.

`slide#8: Request`

gm: EAT not ready, FIDO asks for registering claims (min set) that are crisp enough (i.e., they are not going to change in the time needed to shipping to IESG).
ll: Is it just the nonce and UEID claims?
gm: it's at least the claims needed for FIDO to go forward. There are other claims defined by FIDO that they'd like to move forward with registration.
ll: Interested in hearing other people wisdom, as there must be a precedent?
ht: can IANA just reserve the codepoint to avoid collisions? What if semantics changes between the different specs?
km: There is a process for doing this.
ncw: We need to create a structure for the IANA registry. It would be good if you could identify specific claims and priority for RATS WG to focus on.
gm: I can propose something to the mailing list.
ht: my understanding we're using the claims registry from CWT. Is this correct?
ncw: I thought we're using CWT, but not sure if we closed the notion of RATS defining out of a subset of the namespace.
ll: Thinks were using CWT namespace. No carve out for RATS AFAIK.
hb: There was a proposal to do a namespace carve out, but it wasn't resolved.

ncw: having completed the agenda I'll go ahead and cancel our Thursday meeting slot.

AOB