RATS Agenda – Session I – Status Updates

10:00 : 10:05 Agenda Bash & Logistics
   (5 min) Nancy Cam-Winget, Kathleen Moriarty, Ned Smith

10:05 : 10:10 CHARRA (draft-ietf-rats-yang-tpm-charra)
   (5 min) Eric Voit

10:10 : 10:13 AR4SI (draft-ietf-rats-ar4si)
   (3 min) Eric Voit

10:13 : 10:16 Device Subscription (draft-ietf-rats-network-device-subscription)
   (3 min) Eric Voit

10:16 : 10:21 Architecture (draft-ietf-rats-architecture)
   (5 min) Michael Richardson, Henk Birkholz

10:21 : 10:26 DAA (draft-ietf-rats-daa)
   (5 min) Henk Birkholz

   (5 min) Henk Birkholz

10:31 : 10:36 UCCS (draft-ietf-rats-uccs)
   (5 min) Henk Birkholz, Carsten Boreman

10:36 : 10:41 EAT (draft-ietf-rats-eat)
   (5 min) Laurence Lundblade

   (3 min) Guy Fedorkow
A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs

draft-ietf-rats-yang-tpm-charra-18

IETF 113, March 2022, RATS WG

H. Birkholz  S. Bhandari  E. Voit  L. Xia  T. Laffey  G. Fedorkow
M. Eckel  ThoughtSpot  B. Sulzen  Huawei  HPE  Juniper
Fraunhofer SIT
Relationship between drafts

**Full WG**
- **draft-ietf-rats-architecture**
  - Terminology
  - Topological models
  - Timing definitions

**draft-ietf-rats-reference-interaction-models**
- Terms
- Types of informational flows

**draft-ietf-rats-ar4si**
- Trustworthiness Claims
- Algorithm which enables Verifier to trust AR delivered via the Attester

**Routers / Switches**
- **draft-ietf-rats-tpm-based-network-device-attest**
  - Use case
  - Operational prerequisites
  - Evidence evaluation

**draft-ietf-rats-yang-tpm-charra**
- YANG definitions & RPCs
- TCG Algorithm registry

**draft-ietf-rats-network-device-subscription**
- Provably fresh events
- RFC-8639 based YANG subscriptions

**draft-voit-rats-trustworthy-path-routing**
- Specific objects and encodings for algorithm
- YANG model for provisioning

**Terms**

**Operational prerequisites**

**Evidence via Telemetry**

**WG adopted, progressing**

**Quote from TPM**

**WG adopted, progressing**

**simmering**
Status
One last IESG “Yes” or “No Objection” to pass

- Tweaks made during ongoing IESG review
  - Appendix describing IMA, as Linux Kernel could not be referred to as Normative.
  - YANG model references included
  - XPATH syntax tweaks suggested by requested XPATH experts. Proposal included in new v18.
- No scope / functionality changes
- Nothing seen at this time expected to block Ballot closure and document acceptance
Attestation Event Stream Subscription
draft-ietf-rats-network-device-subscription-01

IETF 113, March 2022, RATS WG

Henk Birkholz
Fraunhofer SIT
henk.birkholz@sit.fraunhofer.de

Eric Voit
Cisco
evoit@cisco.com

Wei Pan
Huawei
william.panwei@huawei.com
Purpose & Scope

• Defines how to subscribe to a stream of attestation related Evidence on TPM-based network devices.
  • When subscribed, a Telemetry stream of verifiably fresh YANG notifications are pushed to the subscriber.
  • Notifications are generated for the Evidence going into TPM PCRs, and when the PCRs are extended.

• Result
  • Verifier is pushed new verifiably fresh Evidence whenever PCRs change.
Status

• Stable as a direct combination of RFC-8639 & Charra
• Socialize Security Considerations section text (to be written)
• Then request WGLC
Attestation Results for Secure Interactions

draft-ietf-rats-ar4si-02

IETF 113, March 2022, RATS WG

Eric Voit
Cisco
evoit@cisco.com

Henk Birkholz
Fraunhofer SIT
henk.birkholz@sit.fraunhofer.de

Thomas Hardjono
MIT
hardjono@mit.edu

Thomas Fossati
Arm Limited
Thomas.Fossati@arm.com

Vincent Scarlata
Intel
vincent.r.scarlata@intel.com
Contents

• **Part 1**: Information Element definitions for Attestation Results (AR) generated by Verifier to support Secure Interactions between Attester and Relying Party

• **Part 2**: End-to-end implementation options: (a) Background check, (b) AR Augmented Evidence

• *Implementations:*
  • **Trusted Path Routing** (Proprietary – Cisco)
  • **Veraison** (Open Source, aspiration = Confidential Compute Consortium adoption)
Changes since IETF112

- WG Adoption
- Text clarifications on values of specific Trustworthiness Claims
- Mailing list comparison with EAT ‘security-level’
- Mailing list comparison with EAT ‘swresults’
- Continued alignment of instance draft: Awaiting meaningful market uptake before requesting WG adoption

Trusted Path Routing

draft-voit-rats-trustworthy-path-routing-05
IETF 113, March 2022, RATS WG

Eric Voit
Cisco
svoit@cisco.com

Chennakesava Raedy
Guddem
Cisco
gchaddam@cisco.com

Guyrocket
Juniper
grocket@juniper.net

Henk Brinkhorst
Fraunhofer FST
henk.brinkhorst@fsl.fraunhofer.de

Mailing Chen
China Mobile
chenmailing@chinamobile.com
Trustworthiness Claim Delivery
Based on draft-ietf-rats-architecture: Passport Model
## Section 2.3.1: AR Design Principles for Trustworthiness Claims

<table>
<thead>
<tr>
<th>Design Principle</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Expose a small number of Trustworthiness Claims</td>
<td>A plethora of similar Trustworthiness Claims will result in divergent choices made on which to support between different Verifiers. This would place a lot of complexity in the Relying Party as it would be up to the Relying Party (and its policy language) to enable normalization across rich but incompatible Verifier object definitions.</td>
</tr>
<tr>
<td>(2) Each Trustworthiness Claim enumerates only the specific states that could viably result in a different outcome after the Policy for Attestation Results has been applied</td>
<td>By explicitly disallowing the standardization of enumerated states which cannot easily be connected to a use case, we avoid forcing implementers from making incompatible guesses on what these states might mean.</td>
</tr>
<tr>
<td>(3) Verifier and RP developers need explicit definitions of each state</td>
<td>Without such guidance, the Verifier will append plenty of raw supporting info. This relieves the Verifier of making the hard decisions. Of course, this raw info will be mostly non-interpretable and therefore non-actionable by the Relying Party.</td>
</tr>
<tr>
<td>(4) Support standards and non-standard extensibility</td>
<td>Standard types of Verifier generated Trustworthiness Claims should be vetted by the full RATS working group, rather than being maintained in a repository which doesn’t follow the RFC process. This will keep a tight lid on extensions which must be considered by the Relying Party’s policy language. Because this process takes time, non-standard extensions will be needed for implementation speed and flexibility</td>
</tr>
</tbody>
</table>
## Comparing Trustworthiness Claims & swresults (undergoing tweaks in EAT)

<table>
<thead>
<tr>
<th></th>
<th>Trustworthiness Claim (AR4Si)</th>
<th>EAT Claim</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attestation target</strong></td>
<td>All runtime software/object loaded into Attester memory</td>
<td>A Verifier specified set of directories within the Attester file system</td>
</tr>
<tr>
<td><strong>Encodable states</strong></td>
<td>Seven</td>
<td>Five</td>
</tr>
<tr>
<td><strong>Vendor extensible</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Claim consistency</strong></td>
<td>Common claim generalizations across Verifier generated AR: (Affirming, Warning, Contraindicated, None)</td>
<td>No generalized claim abstractions across generated AR claims</td>
</tr>
<tr>
<td><strong>RP claim interpretation</strong></td>
<td>Claim always references the full attestation target</td>
<td>Claim references either attestation target or submodule(s). An RP parser must understand context within structured message.</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Only encodes information likely to be actioned by RP</td>
<td>Can encode both actionable information as well as supplementary information for debug logs</td>
</tr>
<tr>
<td><strong>Encodings/serialization</strong></td>
<td>Transport independent, example serialization in draft-voit-rats-trustworthy-path-routing</td>
<td>JSON, CBOR, could add more</td>
</tr>
<tr>
<td><strong>Information Model</strong></td>
<td>English prose</td>
<td>English prose &amp; CDDL</td>
</tr>
</tbody>
</table>
RATS Architecture Status
RATS WG
Report on Adopted I-Ds
Henk Birkholz <henk.birkholz@sit.fraunhofer.de>

IETF 113
22 March 2022
Vienna
RATS Architecture (I)

• When: Tuesdays 10am EST (+ a few Fridays/adhoc)
• Issues: 185 total (none remaining)
• Pull requests: 216 total (one remaining)
• No edits until the start of the next review phase
RATS Architecture (II)

• Latest Diff: https://www.ietf.org/rfcdiff?url1=draft-ietf-rats-architecture-12&url2=draft-ietf-rats-architecture-15

• 3.1 Added: Two Types of Environments of an Attester

• References added: DAA, PSA-Token, NIST-800-57p1, RFC8086, TCG-DICE-SIBDA

• Already had AD review, state is "Submitted to IESG for Publication"

• What is happening next?
DAA Status
Interaction Models Status
UCCS Status
RATS Direct Anonymous Attestation

- In the middle of multiple open issues
- Next steps:
  - Relate DAA Issuer flows to RATS Endorsements
  - Introduce the related TCG concept of "Privacy CA"
  - Explore relationships to TCG DICE and maybe add corresponding sections
  - Address issues of undermining anonymity by injecting re-identifiable information via CHARRA interaction models
RATS Reference Interaction Models


• 7.1.1. Added: Models and example sequences of Challenge/Response Remote Attestation
  • Background Check & Passport model based on emerging requirements coming from C2PA (LF project: Coalition of Content Provenance and Authenticity)
• Anything else then consistency polish, diagram maintenance and... is now the time to ask for dedicated area and dir review?
RATS Unprotected CWT Claims Sets

- Addressed early review comments from Thomas Fossati
- Recap: while UCCS is for all CWT an UCCS document must never be shipped with an application specific Security Consideration – RATS is the initial context
  - Follow-up I-Ds can reuse the core definitions of this document and introduce their own specific Sec-Con.
- Added a proposal that combines the CDDL .feature control with a generic type definition to allow for a choice between JSON & CBOR – potentially allowing for UJCS.
EAT Status
EAT Update

Laurence Lundblade

IETF 113 March 2022
Planned Contents of an EAT - The Claims

- **HW Identification**
  - OEM, model, version...
  - Unique device identification

- **SW Identification - CoSWID**
  - Author, package, version...
  - Measurement

- **Security Characterization**
  - High-level OS, TEE, secure element, TPM...

- **Running State**
  - Boot and debug state

- **Measurement of Running SW**
  - Runtime integrity check

- **Nonce and Timestamps**
  - Freshness, prevent replay

- **Identify Verifier Input**
  - Endorsements, key ID, reference values...

- **Context, Purpose, Profile**
  - Intended use cases, profile claim

- **GPS Location**
  - Public Keys
  - Attestation of private keys on the device (e.g., Android key store)

- **Submodules**
  - HW subsystems, TEE, SW process and apps...

- **Nested EATs**
  - One signed EAT inside another

- **Formal Device Certifications**
  - For example, Common Criteria certification; format is GP’s DLOA

- **Results Codes**
  - Overall Verification Results, Measurement Results
Level of Completion in EAT Draft

- HW Identification
  - OEM, model, version...
  - Unique device identification

- SW Identification - CoSWID
  - Author, package, version...
  - Measurement

- Security Characterization
  - High-level OS, TEE, secure element, TPM...

- Running State
  - Boot and debug state

- Measurement of Running SW
  - Runtime integrity check

- Nonce and Timestamps
  - Freshness, prevent replay

- Identify Verifier Input
  - Endorsements, key ID, reference values...

- Context, Purpose, Profile
  - Intended use cases, profile claim

- GPS Location

- Public Keys
  - Attestation of private keys on the device (e.g., Android key store)

- Submodules
  - HW subsystems, TEE, SW process and apps...

- Nested EATs
  - One EAT inside another, Detached Bundles

- Formal Device Certifications
  - For example, Common Criteria certification; format is GP’s DLOA

- Result Codes
  - Overall Verification Results, Measurement Results

- Progress & change since IETF 112. In draft -12
  - Ready for last call, no open issues
  - Near completion, reviewed
  - Draft text
  - Proposed, Interest in
Important changes in the -12 draft (since IETF 112)

- Use normative language consistently
- Better definition of “entity”
- Lots of wording improvements
- Added HW Model claim
- Added boot odometer claim
- Added privacy considerations for replay protection
- Make HW Version one claim instead of three (3 were for chip, circuit board and device)
- Fill in IANA section with descriptions of all claim registrations (both early allocation and standard allocation)
Improved grouping of claims (PR #171)

- Claims about the entity
  - Identity – HW OEM, Model, Version, UEID, SUEID
  - Running state – debug and boot status, uptime, boot odometer
  - Composite devices – submods and token nesting
  - SW Manifests
  - Measurements and measurement results
  - Certification
  - Attestation results code(s)

- Claims about the token
  - Profile
  - Intended use
  - Time stamp
  - Nonce and Freshness
  - Recommendations for including public keys
Work in the EAT queue

- Complete the CDDL
  - Use JC<> CDDL generic to ease definitions that vary between CBOR and JSON
  - A few bug fixes
- Rearrange sections to group claim definitions better
Topics Requiring Work Group Consensus

- Resolve relationship to UCCS (Separate Presentation)
- Resolve security-level claim
- Attestation Results
  - EAT’s role in AR
  - A separate profile document?
  - Add general result code?
  - Relation to ar4si
RIV Status
TPM-based Network Device Remote Integrity Verification
draft-ietf-rats-tpm-based-network-device-attest-13

IETF 113 RATS
22 Mar 2022

Guy Fedorkow - gfedorkow@juniper.net
Eric Voit - evoit@cisco.com
Jessica Fitzgerald-McKay - jmfitz2@nsa.gov
Objective

• Standardize operational model for today’s existing but proprietary TPM-based router/switch Remote Attestation solutions.
  • Enables switches/routers to be appraised by non-proprietary controllers/Verifiers.
  • Gives Network Operators needed stability for interfacing operational systems.
Nonce based Background Check Model

<table>
<thead>
<tr>
<th>Attester</th>
<th>TPM</th>
<th>Log '-----'</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Relying Party</td>
</tr>
<tr>
<td>----------</td>
<td>-----</td>
<td>-------------</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
\text{time}(VG) & \Rightarrow \text{valueGeneration}(\text{targetEnvironment}) \Rightarrow \text{claims} \\
\text{requestEvidence}(\text{nonce, PcrSelection}) & \Rightarrow \text{time}(NS) \\
\text{time}(EG) & \Rightarrow \text{evidenceGeneration}(\text{nonce, PcrSelection, collectedClaims}) \\
\text{SignedPcrEvidence}(\text{nonce, PcrSelection}) & \Rightarrow \text{LogEvidence} \Rightarrow \text{returnSignedPcrEvidence} \\
\text{returnLogEvidence} & \Rightarrow \text{time}(RG, RA) \\
\text{evidenceAppraisal}(\text{SignedPcrEvidence, eventLog, refClaims}) & \Rightarrow \text{attestationResult} \Rightarrow \text{time}(RX) \\
\text{Log Evidence hashed into TPM PCR} & \text{Attestation request received} \\
\text{TPM Quote Evidence is generated} & \text{Nonce generated} \\
\text{Log Evidence collected} & \text{Evidence Returned} \\
\text{Evidence Returned} & \text{Attestation Results generated} \\
\text{Attestation Results appraised} & \text{Attestation Results no longer fresh} \\
\text{Attestation Results no longer fresh} & \text{Evidence Returned} \\
\end{align*}
\]
Status of Draft-13

DISCUSS Comments are resolved

- The relevant TCG document is no longer draft status, and is now published
- Some more editorial comments have turned up
Next Steps

- Forward RIV for RFC-Editor review
Relationship to other WG drafts

Language

- draft-ietf-rats-architecture
  - Terminology
  - Topological models
  - Timing definitions

Profile

- draft-ietf-rats-tpm-based-network-device-attest
  - Use case
  - Prerequisites/simplifying assumptions which enable operation
    - TPM1.2/TPM2.0/equivalent needs
    - Pre-established Key Types
    - Pre-configured endorsements
  - RIV call flow
  - Evidence evaluation
    - PCR allocations for network devices
    - Relevance/viability of KGVs for a subset of PCRs
    - Appraisal Policy for Evidence
    - Attester log type formats supportable

Interface Specification

- Defines operational pre-requisites for
  - draft-ietf-rats-yang-tpm-charra
    - YANG definitions & RPCs for Attester
  - Attestation Evidence via Telemetry
    - draft-birkholz-rats-network-device-subscription
      - Provably fresh events
      - Subscribed YANG notifications

Peer Router Appraisal

- draft-voit-rats-trustworthy-path-routing
  - Trustworthiness Vector
  - Stamped Passport definition

Enables WG discussion via shared context
10:44–11:04 **RATS Charter**  
(20 min) WG Chairs

11:04–11:14 **RATS Milestones**  
(10 min) WG Chairs

11:14–11:44 **EAT Attestation Evidence / Results Taxonomy**  
(30 min) Laurence Lundblade

11:44–12:00 **Open MIC**  
(16 min)
Attestation Results Framing
Full range of security strengths

Certified HW with no SW at all (not a TPM, no measurement)

Simple uncertified SW

Everything in between (TPM, TEE’s, Windows, RIOT, …)
Full range of system architectures

Pure HW — Purpose-built Attestation HW (not a TPM)

App-based — Attestation inside an Android app in Java, Swift, Python…

Everything in between (Full OS’s, IoT Devices, TEEs, Network Equipment…)

JSON + TLS, widely used for B2B

Support JWT/CWT too

B2B data encoding and security is a solved problem, so this is not a focus of RATS
RATS standard for Device/Attester identity

Serial number, OEM, model, version

JSON and perhaps other encoding formats
Allow Passthrough Claims

Passed through from Evidence/Attester

Passed through from Endorser/Endorsement
Detail varies by use case

A base standard of simple pass/fail and/or error code — base standard must work for all architectures and security strengths

Device/Attester identity for some use cases

Machine learning risk engines want every scrap and detail
RATS Agenda – Session II

23 March 2022
Room: Grand Park Hall 3
Time zone: UTC+1, 1 hr

13:00 : 13:05 Agenda bash & logistics
(5 min) Nancy Cam-Winget, Kathleen Moriarty, Ned Smith

13:05 : 13:15 UCCS / UJCS and EAT
(10 min) Giri Mandyam

(10 min) Giri Mandyam

13:25 : 13:40 Concise Reference Integrity Manifest
(15 min) Henk Birkholz, Thomas Fossati (draft-birkholz-rats-corim)

13:40 : 14:00 Open MIC
(20 min)
EAT and UCCS
IETF 113
Currently there are two standards-track WG drafts for attestation tokens in RATS
- Entity Attestation Token (EAT)
- Unsigned CBOR Claim Set (UCCS)

Goal: establish relationship (incl. normative dependencies) between these documents

Assumption: unsigned JSON claim set (UJCS) should be supported
- For this presentation, the term ‘UCCS’ will cover both use cases
Premise: UCCS is Scoped to Attestation

- UCCS is not a generic method to send unsigned CWT claims in any and all contexts
- UCCS draft specifies this limitation in the intro: “This specification allocates a CBOR tag to mark Unprotected CWT Claims Sets (UCCS) as such and discusses conditions for its proper use in the scope of Remote ATtestation procedureS (RATS) and the conveyance of Evidence from an Attester to a Verifier”
Premise: UCCS does not always require a mutually authenticated secure transport

- UCCS document states in front matter “if a mutually Secured Channel is established between two remote peers, and if that Secure Channel provides the required properties ..., it is possible to omit the protection provided by COSE, creating a use case for unprotected CWT Claims Sets”
- This would make sense as a security consideration, but should not be a normative requirement
  - Example where UCCS may be acceptable (depending on RP security policy) is one-way authenticated TLS connection
EAT Relationship to UCCS

- EAT is the RATS standards-track method for conveying attestation evidence
- As per Sec. 1.2 of the EAT specification: "An EAT is a claims set about an entity based on one of the following:
  - CBOR Web Token (CWT)
  - Unprotected CWT Claims Set (UCCS)
  - JSON Web Token (JWT)
- Therefore EAT has a normative dependency on UCCS definition, which means stable CDDL description that is consistent with the rest of the EAT spec
EAT Relationship to UCCS (cont.)

- EAT is silent on normative requirements for underlying transport, and provides high level recommendations in security considerations section
  - This is because EAT is general-purpose; not all EAT transport can be guaranteed to be mutually-authenticated secure tunnels
- EAT document likely cannot properly cover security considerations regarding conveyance of unsigned claims
  - Would be better covered in a different dedicated draft
EAT Editors Recommendation

- EAT document provides the CDDL description for unsigned claim sets (both CWT and JWT, i.e. UCCS and UJCS)
- EAT document incorporates the request to IANA for the CBOR/JSON tag
- Current UCCS document re-focuses on only security considerations for unsigned claims
  - Can be informational track
Why this change?

- EAT document only requires stable CDDL description of UCCS, and editors are confident that exists today
- Security considerations for UCCS likely requires additional investigation
  - May not close very quickly
  - EAT implementors who require UCCS option may get held up
- EAT can go to RFC with a reference to UCCS I.-D. in its security considerations
  - Assuming current UCCS draft is redirected to focus only on security considerations
- UCCS document can more extensively cover all cases for transport security considerations. Examples include
  - When one-way auth. is sufficient
  - Role of root-of-trust in securing transport (e.g. SIM-based auth.)
Exportable Keys
IETF 113
Implementations of authentication technology such as FIDO/Webauthn are turning to cloud synchronization of private keys
- Private key synchronization can allow for less friction in end user management of credentials (e.g. device migration/upgrade)
Authenticator Restricted Operating Environment

- From https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-security-requirements-v1.4-fd-20201102.html
- AROE may include attester
RATS Architecture Relevance

- As per https://datatracker.ietf.org/doc/html/draft-ietf-rats-architecture#section-12.1.1, "It is assumed that an Attesting Environment is sufficiently isolated from the Target Environment it collects Claims about and that it signs the resulting Claims set with an attestation key, so that the Target Environment cannot forge Evidence about itself."
- Same section goes on to say: "In many cases the user or owner of a device that includes the role of Attester must not be able to modify or extract keys from the Attesting Environments, to prevent creating forged Evidence. Some common examples include the user of a mobile phone or FIDO authenticator."
Attestation Evidence for Extractable Auth Credentials

- FIDO authenticator may not have separation between attester and target
- Should attestation evidence specifically address whether private key material is extractable?
- If so, should this evidence be accompanied by evidence that attestation keys are not extractable?
  - Lack of such evidence could also be used in RP security assessment of authenticator
- Implicit evidence: example would be if RP determines whether authenticator allows extractable keys through endorsement
Potential Ways Forward

1. Define relevant evidentiary claims in EAT document
   - Assuming extractable keys are of more general interest than just authenticators
2. Leave issue to an EAT profile for FIDO compliant authenticators
   - Can define relevant evidentiary claims in profile
3. Do nothing
   - Let RP figure out appraisal process via implicit evidence or some other means
Concise RIMs

IETF 113 – Vienna
draft-birkholz-rats-corim-02
Goal

• One or more authorized supply chain actors (OEM, ODM, ISV, SiP, etc.) need to come together and “describe” an Attester to a Verifier

• “[...] standardize formats for endorsements and reference values”
  • Proposed charter
Information and Data Model

• Groups of triples (subj+verb+obj) describing an attester
• Sentences of the form:
  • Supply chain entity A says that:
    • Target environment has reference value X
    • Attesting environment has verification key Y
    • Target/Attesting environment has endorsed value Z
    • And more (the set of triples is extensible), e.g.: model relations in composite devices
• Encoded to CBOR
• Signed with COSE
Status Recap

• Info model
  • TCG, DICE WG, “DICE Endorsement Architecture”
    • V1.0 R0.37 successfully balloted for IP/Technical and Public Review

• Data model
  • https://github.com/ietf-rats/ietf-corim-cddl
    • CDDL, examples in CBOR diag notation, assembly & test infra
  • IETF I-D: https://datatracker.ietf.org/doc/draft-birkholz-rats-corim

• Running Code (golang library and CLI)
  • https://pkg.go.dev/github.com/veraison/corim
Questions

Adopt as soon as rechartering concludes?