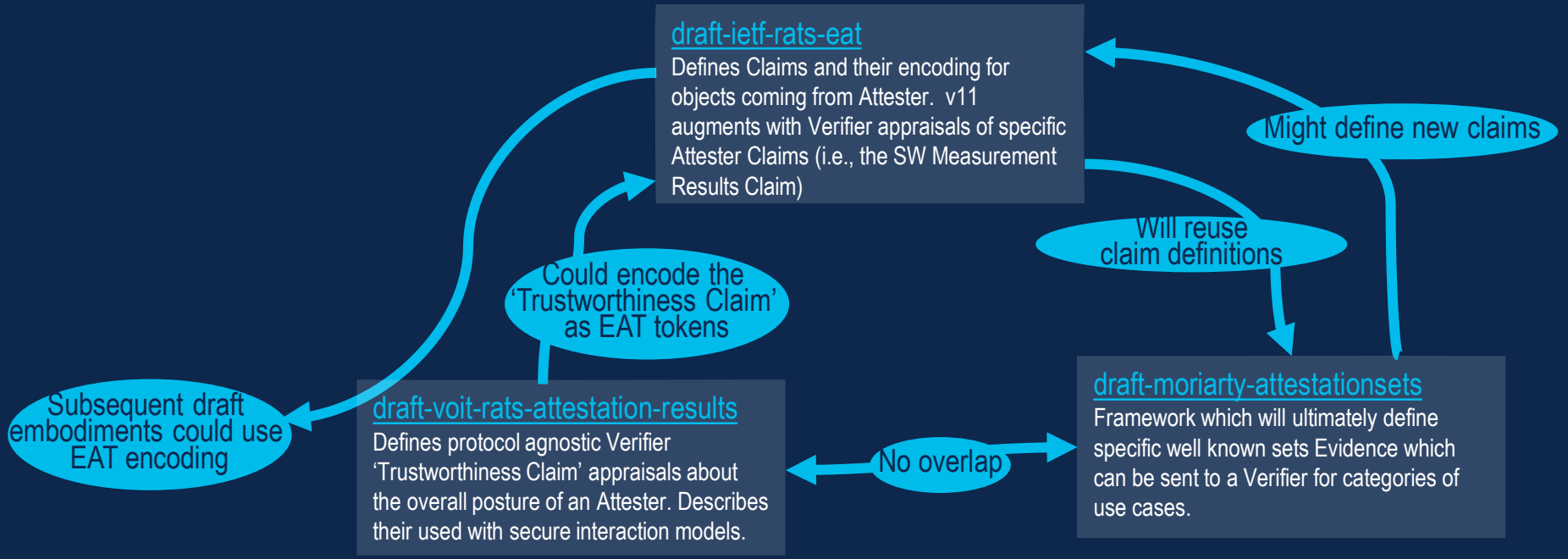
Normative Intersections



Attestation Results for Secure Interactions

draft-voit-rats-attestation-results-02

IETF 112, November 2021, 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

Summary

@ IETF 111 WG requested document content realignment

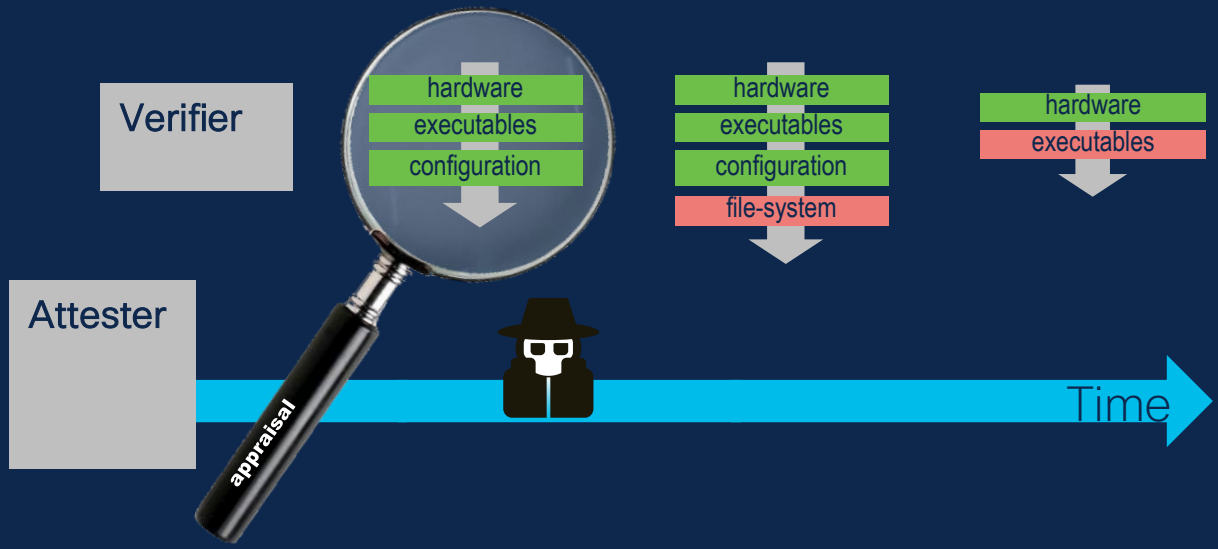
- Part 1: Information Element definitions for Attestation Results (AR) generated by Verifier to support Secure Interactions between Attester and Relying Party
- Part 2: End-to-end implementation options: (a) Background check, (b) AR Augmented Evidence
- Implementations:
  - Trusted Path Routing (Proprietary – Cisco)
  - Veraison (Open Source, aspiration = Confidential Compute Consortium adoption)
- Ask: WG Adoption after intersections discussed
  - draft-ietf-rats-eat
  - draft-voit-rats-attestation-results
  - draft-moriarty-attestationsets

Remote Attestation in a Heterogenous World

- Many types of Attesting Environments (AE)
- Relying Party cannot support ∞ language permutations
  - And a mix and match across L1 ↔ L7 platforms is coming if IETF RATS succeeds
- Relying Party needs shared definitions/structures for Verifier Appraisals
  - Will help scale and Interop
  - Reduce transcoding/mapping between sequentially bound sets of Attesters
  - Could be encoded in EAT, YANG, CDDL, etc...

Verifier Appraisal

- Zero to many Trustworthiness Claims assigned during an appraisal cycle.



Trustworthiness Claims, simplified since IETF 111

Identity	**instance-identity**	Recognition of Attester via a private key signature which could only have come from that instance of the Attesting Environment
Integrity	**hardware**	Recognition of expected hardware and firmware based on their code fingerprints
	executables	Recognition of runtime files, scripts, and other objects loaded into runtime memory
	sourced-data	Evaluation of the integrity of data objects loaded into memory
	file-system	Recognition of all file system objects which may be utilized
	configuration	Evaluation of the configuration, and conclusions on the exposure of known vulnerabilities
Confidentiality	**runtime-opaque**	Accessibility of Attester objects in memory from outside the Attester but within same physical host
	storage-opaque	Does Attester encrypt its persistent storage

Proposed Encodings of Trustworthiness Claims

Identity	**instance-identity**	Recognition of Attester via a private key signature which could only have come from that instance of the Attesting Environment	2: Recognized, affirmed 96: Not recognized, but should be 97: Recognized, contraindicated
Integrity	**hardware**	Recognition of expected hardware and firmware based on their code fingerprints	2: Only genuine/supported Authentic 32: Authentic, but known security bugs 96: Recognized, contraindicated 97: Not recognized, but should be
	executables	Recognition of runtime files, scripts, and other objects loaded into runtime memory	2: Recognized, only genuine/supported 32: Recognized, but known security gaps 33: Some objects loaded not recognized 96: Recognized, contraindicated
	sourced-data	Evaluation of the integrity of data objects loaded into memory	2: comes from affirmed Attesting sources 32: does not come from affirmed 96: Recognized, contraindicated
	file-system	Recognition of all file system objects which may be utilized	2: Recognized, affirmed 32: Some analyzed files not recognized 96: Recognized, contraindicated
	configuration	Evaluation of the configuration, and conclusions on the exposure of known vulnerabilities	2. Known and approved config 3. No known vulnerabilities exposed 32: Known security risk exposed 96: Unsupportable configuration
Confidentiality	**runtime-opaque**	Accessibility of Attester objects in memory from outside the Attester but within same physical host	2: TEE encryption, opaque to device root 32: Target inaccessible by peer Apps 96: Contraindicated or compromised
	storage-opaque	Does Attester encrypt its persistent storage	2: All objects needing privacy encrypted 32: Not all objects need privacy encrypted 96: Secrets are stored unencrypted

Encoded using signed 8-bit integer, intended to simplify RP based Policy evaluation

Affirming (Values 2 to 31): The Verifier affirms the Attester support for this aspect of trustworthiness

Warning (Values 32 to 95): The Verifier warns about this aspect of trustworthiness

Contraindicated (Values 96 to 127): The Verifier asserts the Attester is explicitly untrustworthy regarding this aspect. (99 is always signature verification error.)

None (Values 0, 1, & -1): The Verifier makes no assertions about this Trustworthiness Claim. (0 is no claim, 1 is wrong evidence delivered, -1 is processing error.)

Values under -1: vendor allocatable

Values -2 to -32

Values -33 to -96

Values -97 to -128

Normalizing Trustworthiness Claims (Informational /Appendix)

	Trustworthiness Claim	Protection Technologies		
		Process-based	VM-based	HSM-based
Identity	instance-identity	Optional	Optional	Optional
Integrity	hardware	Implicit	Chip dependent	If PCR check ok
	executables	Optional	Optional	If PCR check ok
	sourced-data	Optional	Optional	Optional
	file-system	Optional	Optional	Insufficient
	configuration	Optional	Optional	Optional
Confidentiality	runtime-opaque	Implicit	Implicit	Very limited support
	storage-opaque	Implicit	Chip dependent	Very minimal space

Normalized Trustworthiness Claims ≠ the same Relying Party policy disposition

- Even with Normalized Trustworthiness Claims, Attesters need not be treated equivalently by the Relying Party
  - Variance in underlying protections of SGX, TrustZone, SEV, TPM, etc. could mean different disposition via the Appraisal Policy for Attestation Results.
  - Each Verifier, or Verifier version, or Verifier appraisal of a specific type of Attester may be trusted differently for different claims

Attestation Results Augmented Evidence

- Evidence the Relying Party might Action bundled by Attester
- Signatures protect from manipulation

Verifiable Identity instance(s) + Trustworthiness Claims of the Verifier + Verifiable Freshness

Attester	chip vendor
	chip type
	target environment
	target developer
	instance
Verifier	verifier id
	verifier developer

- Categories defined in this draft
- Specific objects to be defined in other drafts

Identity	instance-identity
Integrity	hardware
	executables
	configuration
	file-system
	sourced-data
Confidentiality	runtime-opaque
	storage-opaque

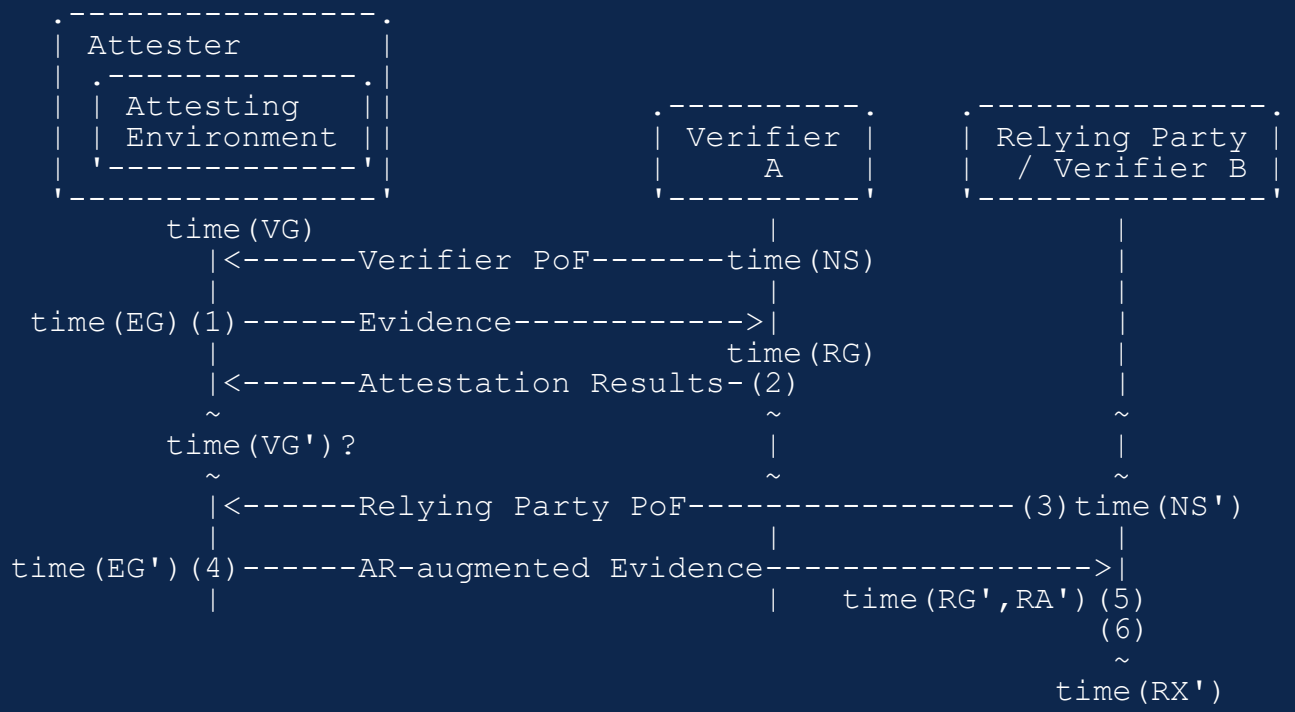
Defined in this draft

Random Number	nonce
Synchronized Clocks	timestamp
	tuda sync token
Epoch	epoch id

- Categories defined in draft-ietf-rats-architecture Section 10

Trustworthiness Claim Delivery

Based on draft-ietf-rats-architecture: Passport Model



Summary

@ IETF 111 WG requested document content realignment

- 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)
- Ask: WG Adoption after intersections discussed
  - draft-ietf-rats-eat
  - draft-voit-rats-attestation-results
  - draft-moriarty-attestationsets