Guidelines for Security Considerations of RATS (draft-rats-sardar-sec-cons)

Muhammad Usama Sardar

TU Dresden, Germany

November 6, 2025

Thanks to my travel sponsors!

Peg Jones GENXT CONFIDENTIAL COMPUTING CONSORTIUM Teleport

Motivation: We could definitely do better!

datatracker.ietf.org/wg/rats/documents/

IETF Datatracker Groups Documents Meetings Other muhammad_usama.sardar

Document	Pages	Date	Status
draft-ietf-rats-epoch-markers-02 **Epoch Markers**	20 pages	2025-10-09	I-D Exists In WG Last Call Nov 2025
draft-ietf-rats-daa-08 **Direct Anonymous Attestation for the Remote Attestation Procedures Architecture**	12 pages	2025-09-03	I-D Exists In WG Last Call Dec 2023, Dec 2025
draft-ietf-rats-endorsements-07 **RATS Endorsements**	12 pages	2025-08-25	I-D Exists In WG Last Call
draft-ietf-rats-ar4si-09 **Attestation Results for Secure Interactions**	39 pages	2025-08-15	I-D Exists In WG Last Call Nov 2023, Jan 2026

ietf.org/archive/id/draft-ietf-rats-epoch-markers-02.html

6. Security Considerations

TODO

ietf.org/archive/id/draft-ietf-rats-ar4si-09.html

5. Privacy Considerations

Privacy Considerations Text

6. Security Considerations

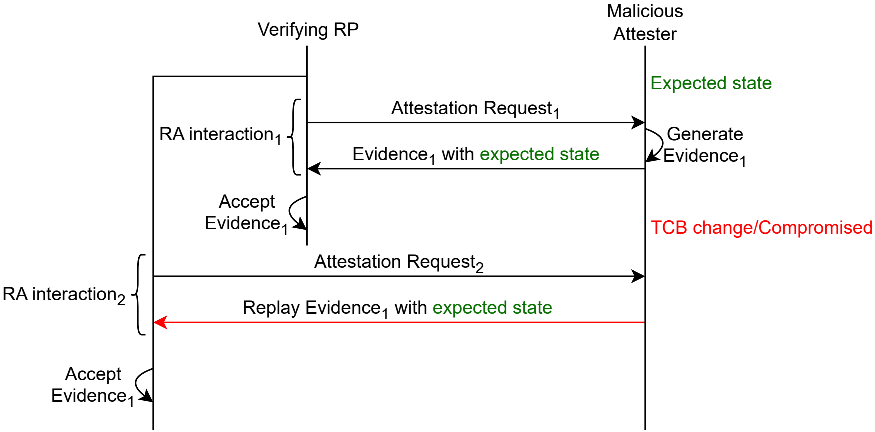
Security Considerations Text

(Snapshots as of 5th November, 2025)

Threat Modeling (What else would the WG find useful?)

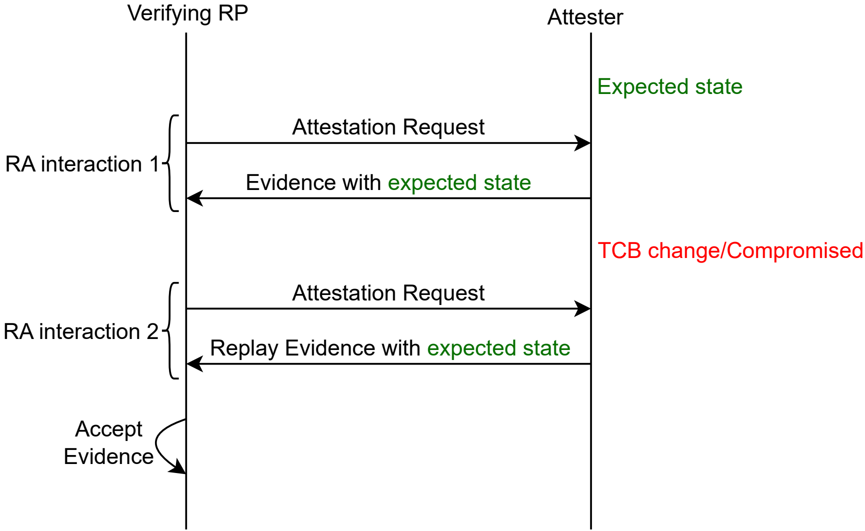
- Threat source
- Capabilities
- Threat action
- Threat impact

5.1a Replay of Stale Evidence Across Multiple Connections[1]



[1]Sardar, *Perspicuity of Attestation Mechanisms in Confidential Computing*, 2025.

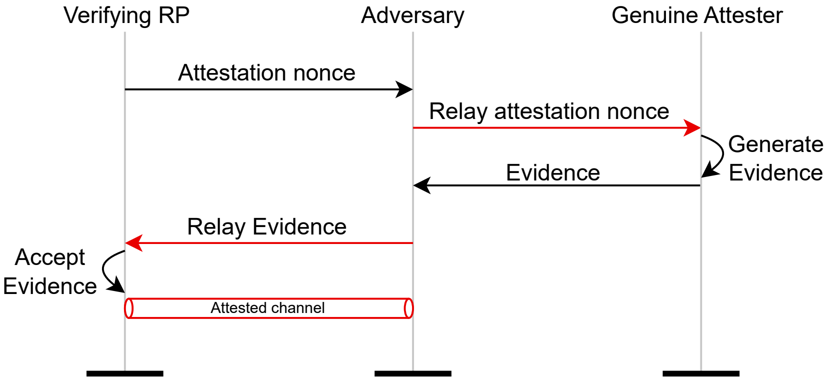
5.1b Replay of Stale Evidence Within the Same Connection[2]



[2] Sardar, *Perspicuity of Attestation Mechanisms in Confidential Computing*, 2025.

5.2 Relay Attacks[3]

- Privacy: Claims visible to passive adversaries
- Security: Relay attacks are possible.
  - Adversary tricks the Verifying RP to impersonate the genuine Attester.



[3] Sardar, *Perspicuity of Attestation Mechanisms in Confidential Computing*, 2025.

5.3 Diversion Attacks[4]

Definition

A network adversary – with Dolev-Yao[a] capabilities and access (e.g., via Foreshadow[b]) to attestation key of any machine in the world – can redirect a connection intended for a specific Infrastructure Provider to the compromised machine, potentially resulting in exposure of confidential data.

[a] Dolev and Yao, "On the security of public key protocols", 1983.

[b] Van Bulck, Minkin, Weisse, Genkin, Kasikci, Piessens, Silberstein, Wenisch, Yarom, and Strackx, "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution", 2018.

- Threat source: network adversary
- Capabilities: Dolev-Yao and privAK of any machine
- Threat action: redirect a connection
- Threat impact: exposure of confidential data

[4] Sardar, *Perspicuity of Attestation Mechanisms in Confidential Computing*, 2025.

Mitigations

- Some freshness criteria in Evidence
  - Attestation nonce
  - Timestamps
  - Epoch handle vs. epoch id vs. Epoch Markers[5]?
- Binding Evidence to connection
- Binding Evidence to Infrastructure Provider

[5] https://mailarchive.ietf.org/arch/msg/rats/CgvwdtLEEVxQj2Ab5y6RRugS8zk/

Key References

Dolev, D. and A. Yao. "On the security of public key protocols". In: *IEEE Transactions on Information Theory* 29.2 (Mar. 1983), pp. 198–208. ISSN: 1557-9654.

Sardar, Muhammad Usama. *Perspicuity of Attestation Mechanisms in Confidential Computing*. 2025.

Van Bulck, Jo, Marina Minkin, Ofir Weisse, Daniel Genkin, Baris Kasikci, Frank Piessens, Mark Silberstein, Thomas F. Wenisch, Yuval Yarom, and Raoul Strackx. "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution". In: *Proceedings of the 27th USENIX Security Symposium*. USENIX Association, Aug. 2018.

ACK

- Ira McDonald
- Inspiration from draft-irtf-cfrg-cryptography-specification-02
  - Nick Sullivan
  - Christopher A. Wood
- Simon Frost
- Jun Zhang
- Ivan Gudymenko

Thanks to my travel sponsors!

Peg Jones GENXT CONFIDENTIAL COMPUTING CONSORTIUM Teleport