Protecting the RATS Ecosystem from Critical-severity Vulnerabilities (draft-sardar-rats-sec-cons)

Muhammad Usama Sardar[1,2], Songbo Bu[3],
and Serhii Nikolaichuk[4]

(ACK: Bertrand Foing, Sammy Kerata Oina, Drasko Draskovic,
Markus Rudy, Rebekah Overdorf, and Tobias Pulls)

[1]TU Dresden, Germany

[2]Co-chair, Trusted Research Environment (TRE) Open Suite,
Global Alliance for Genomics and Health (GA4GH)

[3]Stevens Institute of Technology

[4]The Capital Index, Austin, Texas

September 14, 2026

Outline

1. The “Why” and “How”
2. Requesting Adoption

The "Why"[1]

[Rats] Re: Request for adoption of draft-sardar-rats-sec-cons-04.txt

toshiyuki sato <tomsato@myauberge.jp> | Mon, 13 July 2026 11:37 UTC | Show header

Hi Usama,

+1 to adoption from me, with a concrete data point rather than just a vote.

We built a Tier 1 checker -- structural, rule-derived, not formal verification -- directly from the guidelines in Sections 5 through 8 of your draft, and ran it against four of our own specifications (draft-sato-soos-kia-03, mjwt-02, gar-03, aep-02).

One of our drafts, KIA, was explicitly designed with CVE-2026-33697 in mind -- we built a structural defense against that relay-attack class before ever running this checker -- and the connection-binding checks derived from your Sections 5.3/6 passed cleanly against it, as expected.

[1] https://mailarchive.ietf.org/arch/msg/rats/kIP6rhvngA4mFYPoNhx9dDO8czg/

The "Why" (continued)[2]

But the same run on the same document still surfaced 2 ERROR-level findings and 3 WARNING-level findings elsewhere: a genuine cross-document identifier-ownership conflict we hadn't caught across several revisions, a missing privacy-considerations section, and gaps in explicit threat-model statement, authentication-level specificity, and an undefined term. So this isn't "the checker found nothing because we already got the headline case right" -- a document built with that specific CVE in mind still had other real gaps your guidelines caught, with nothing more sophisticated than pattern-matching against rules you've already written down.

Big Thank you!

Happy to share more detail off-list if it's useful for the adoption discussion.

Tom Sato
MyAuberge K.K.

[2] https://mailarchive.ietf.org/arch/msg/rats/kIP6rhvngA4mFYPoNhx9dDO8czg/

The "Why" (continued)[3]

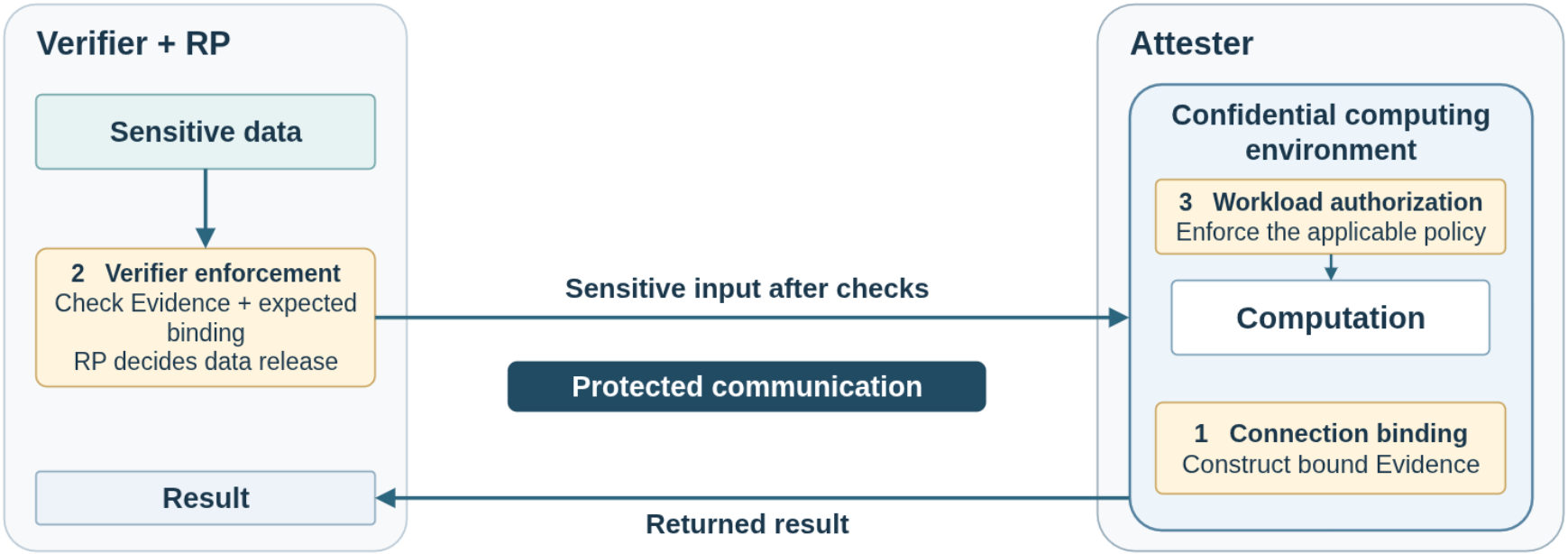
> 2. That binding is to a genuine TEE and to the freshness handle, not to the CAS channel. Since the CAS is an untrusted conduit (Section 7.2) and relay is not yet discussed, a relay can sit between the Attester and the Credential Authority while every check above still passes: binding a public key, with or without a nonce, does not correlate the Evidence with the session, per the public analysis of binder mechanisms (Identity Crisis in Confidential Computing, ASIA CCS 2026; Intra-handshake.fail, CVE-2026-33697). The remedy is cheap: also fold a value derived from the CAS transport's shared secret, the RFC 9266 TLS exporter, into the freshness field, and say so in Security Considerations.

- Note: written before being the author of draft-sardar-rats-sec-cons

[3] https://mailarchive.ietf.org/arch/msg/rats/yaGG4sVf4pCfJOHNPPRv3Xg0cG8/

Problem Statement: Secure Computation

- How to check the connection and remote environment before releasing sensitive data?
- Numbers in figure identify checks



How?

Illustrative Examples of Security Considerations and Implementation Guidance for RATS

1. **Connection Binding**: Bind Evidence to the current connection.

2. **Verifier Enforcement**: Enforce the expected value at the verifier API (fail closed when absent or mismatch)

3. **Workload Authorization**: Enforce the applicable workload policy on every accepting path.

Outline

1 The “Why” and “How”

2 Requesting Adoption

Scope (from authors' lens): A Shared Security Baseline

- Build on top of RFC3552 and RFC9334
- RATS charter from a security considerations perspective
  1. Formats
  2. Conveyance protocols
- Authors' proposal: cover security considerations baseline for both in this draft.
  - Pro: shared burden. Other drafts (TACRA, draft-richardson-rats-geographic-results[4], etc.) can reference the applicable checks and state their assumptions and remaining risks.
- Requesting WG adoption. Adoption is a starting point, not a finish line. Proposed corrections and security concerns in RATS drafts are illustrative and can be removed.

[4] See adoption call thread, e.g., `https://mailarchive.ietf.org/arch/msg/rats/nfrdr1T9Pdp6D_kj2Et3XZk-hOY/`