RATS Working Group
Internet-Draft
Updates: 9334 (if approved)
Intended status: Informational
Expires: 23 April 2026

M. U. Sardar
TU Dresden

20 October 2025

Guidelines for Security Considerations of RATS
draft-rats-sardar-sec-cons-00

Abstract

This document aims to provide guidelines and best practices for writing security considerations for technical specifications for RATS targeting the needs of implementers, researchers, and protocol designers.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://muhammad-usama-sardar.github.io/rats-sec-cons/draft-rats-sardar-sec-cons.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-rats-sardar-sec-cons/.

Source for this draft and an issue tracker can be found at https://github.com/muhammad-usama-sardar/rats-sec-cons.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 April 2026.

Table of Contents

1. Introduction

While [I-D.irtf-cfrg-cryptography-specification] provides excellent guidelines, remote attestation [RFC9334] has several distinguishing features which necessitate a separate document. One specific example of such feature is architectural complexity.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. General Hierarchy of Authentication

[Gen-Approach] proposes general hierarchy of one-way authentication, which can help precisely state the intended level of authentication (in decreasing order):

* One-way injective agreement
* One-way non-injective agreement
* Aliveness

Recentness can be added to each of these levels of authentication.

4. Attacks

Security considerations in RATS specifications need to clarify how the following attacks are avoided or mitigated:

* Diversion attacks [Meeting-122-TLS-Slides]
* Relay attacks
* Replay attacks

5. Examples of Specifications That Could Be Improved

5.1. RFC9334

5.1.1. Unprotected Evidence

Section 7.4 of [RFC9334] has:

> A conveyance protocol that provides authentication and integrity protection can be used to convey Evidence that is otherwise unprotected (e.g., not signed).

Using a conveyance protocol that provides authentication and integrity protection, such as TLS 1.3 [RFC8446], to convey Evidence that is otherwise unprotected (e.g., not signed) undermines all security of remote attestation. Essentially, this breaks the chain up to the trust anchor (such as hardware manufacturer) for remote attestation. Hence, remote attestation effectively provides no protection in this case and the security guarantees are limited to those of the conveyance protocol only. In order to benefit from remote attestation, Evidence MUST be protected using dedicated keys chaining back to the trust anchor for remote attestation.

5.1.2. Missing Roles and Conceptual Messages

* Identity Supplier and its corresponding conceptual message Identity are missing and need to be added to the architecture [Tech-Concepts].

* Attestation Challenge as conceptual message needs to be added to the architecture [Tech-Concepts].

6. Examples of Specifications That Are Detrimental for Security

We believe that the following drafts are detrimental for the RATS ecosystem:

* Multi-Verifiers [I-D.deshpande-rats-multi-verifier]: the design of multi-verifiers not only increase security risks in terms of increasing the Trusted Computing Base (TCB), but also increases the privacy risks, as potentially sensitive information is sent to multiple verifiers.

* Aggregator-based design [I-D.ietf-rats-coserv]: Aggregator is an explicit trust anchor and the addition of new trust anchor needs to have a strong justification.

7. Security Considerations

All of this document is about security considerations.

8. IANA Considerations

This document has no IANA actions.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, <https://www.rfc-editor.org/rfc/rfc9334>.

9.2. Informative References

[Gen-Approach]
Sardar, M. U., "Perspicuity of Attestation Mechanisms in Confidential Computing: General Approach", October 2025, <https://www.researchgate.net/publication/396593308_Perspicuity_of_Attestation_Mechanisms_in_Confidential_Computing_General_Approach>.

[I-D.deshpande-rats-multi-verifier]
Deshpande, Y., jun, Z., Labiod, H., and H. Birkholz, "Remote Attestation with Multiple Verifiers", Work in Progress, Internet-Draft, draft-deshpande-rats-multi-verifier-03, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-deshpande-rats-multi-verifier-03>.

[I-D.ietf-rats-coserv]
Howard, P., Fossati, T., Birkholz, H., Kamal, S., Mandyam, G., and D. Ma, "Concise Selector for Endorsements and Reference Values", Work in Progress, Internet-Draft, draft-ietf-rats-coserv-02, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-coserv-02>.

[I-D.irtf-cfrg-cryptography-specification]
Sullivan, N. and C. A. Wood, "Guidelines for Writing Cryptography Specifications", Work in Progress, Internet-Draft, draft-irtf-cfrg-cryptography-specification-02, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-cryptography-specification-02>.

[Meeting-122-TLS-Slides]
Sardar, M. U., Moustafa, M., and T. Aura, "Identity Crisis in Attested TLS for Confidential Computing", March 2025, <https://datatracker.ietf.org/meeting/122/materials/slides-122-tls-identity-crisis-00>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[Tech-Concepts]
Sardar, M. U., "Perspicuity of Attestation Mechanisms in Confidential Computing: Technical Concepts", October 2025, <https://www.researchgate.net/publication/396199290_Perspicuity_of_Attestation_Mechanisms_in_Confidential_Computing_Technical_Concepts>.

Acknowledgments

The author wishes to thank Ira McDonald for insightful discussion. The author also gratefully acknowledges the authors of [I-D.irtf-cfrg-cryptography-specification], which serves as the inspiration of this work.

Author’s Address

Muhammad Usama Sardar
TU Dresden
Email: muhammad_usama.sardar@tu-dresden.de