Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 6 June 2026

T. Madaras
P. Estis
GuardSuite, VXMSecure

3 December 2025

PRE-RCT: Pre-Execution Authorization Receipt Format draft-madaras-preauth-receipts-00

Abstract

This document defines PRE-RCT, the Pre-Execution Authorization Receipt, a cryptographically signed and attestation-aware receipt format used to record high-risk authorization events. PRE-RCT is intended for use with pre-execution authorization protocols such as GNA.

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 6 June 2026.

Table of Contents

1. Introduction

Pre-execution authorization systems require durable, verifiable records capturing action parameters, policy state, approver decisions, and attestation evidence at the moment of authorization. PRE-RCT defines a standard structure to support interoperability, auditing, compliance, and long-term integrity.

2. Requirements Language

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. Design Goals

PRE-RCT is intended to:

* Provide strong non-repudiation.

* Bind action parameters to policy state.

* Support HAE attestation evidence.

* Support N-of-M approvals.

* Be portable across authorization systems.

4. Receipt Structure

PRE-RCT defines a structured object with required fields and optional domain extensions. The receipt MUST be integrity protected and cryptographically signed.

5. Required Fields

The following fields MUST be present:

receipt_id

action_hash

policy_hash

approver_identities

approver_signatures

timestamp

execution_token

hae_masking_profile_id

hae_attestation_token

context_snapshot (OPTIONAL)

6. Verification

Verifiers SHOULD:

* Validate structural integrity.

* Verify all digital signatures.

* Recompute and compare action_hash and policy_hash.

* Validate attestation tokens if present.

* Enforce timestamp bounds and replay protection.

7. IANA Considerations

This document has no IANA actions.

8. Security Considerations

PRE-RCT improves auditability and tamper-evidence but does not prevent collusion, coercion, or compromise below the firmware root of trust. Implementations MUST protect receipt confidentiality and integrity.

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, 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, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

Authors' Addresses

Tom Madaras
GuardSuite, VXMSecure
Hollywood, FL
United States of America
Email: tom@vxmsecure.com

Pat Estis
GuardSuite, VXMSecure
Houston, TX
United States of America
Email: pat.estis@gmail.com