Network Working Group                                          T. Madaras
Internet-Draft                                                P. Estis
Intended status: Experimental          GuardSuite, a VXMSecure Company
Expires: 5 June 2026                                  2 December 2025

# GuardMail Protocol (GMP): Authenticated Messaging with Non-Repudiable Cryptographic Receipts
draft-madaras-guardmail-gmp-00

## Abstract

This document specifies the GuardMail Protocol (GMP), a framework for authenticated outbound messaging that provides cryptographic proof of origin, integrity, and policy compliance for email and file-based communications. GMP introduces GuardMail Receipts (GMRs), signed metadata structures bound to sender identity and message content that allow recipients to verify authenticity independent of transport mechanisms such as SPF, DKIM, and DMARC.

GMP provides a modern, interoperable method for organizations to protect against impersonation, deepfake-based fraud, unauthorized content changes, and spoofed internal communications in enterprise environments.

## 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 5 June 2026.

## Copyright Notice

Table of Contents



## 1. Introduction

Email and messaging systems commonly rely on SPF, DKIM, and DMARC to provide domain-level authentication and alignment. While these mechanisms help detect some forms of spoofing, they do not provide a sender-specific, action-bound, or content-bound non-repudiation mechanism. A message may appear to originate from a legitimate domain while still being malicious, manipulated, or unauthorized.

GuardMail Protocol (GMP) introduces GuardMail Receipts (GMRs), which are cryptographically signed metadata objects that bind a sender identity to a particular message instance and its canonical content representation. A recipient or automated verifier can use the GMR to determine whether a message is authentic and intact, regardless of the underlying transport.

GMP is designed to work with existing email infrastructure and can be deployed incrementally. It is intended to complement, not replace, mechanisms such as SPF, DKIM, and DMARC.

## 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. Terminology

The following terms are used throughout this document:

GMR (GuardMail Receipt) A cryptographically signed metadata structure associated with a specific outbound message instance, containing sender identity and content hashes.

GMP (GuardMail Protocol) The protocol described in this document, defining how GMRs are constructed, attached, and verified.

GMS (GuardMail Stamping Service) The service that creates and attaches GMRs to outbound messages on behalf of a sending domain or organization.

VERIFIER A service or component that validates GMRs on received messages.

MUA (Mail User Agent) Email client used by end-users.

MTA (Mail Transfer Agent) Server responsible for transmitting email between domains.

## 4. Architectural Overview

GMP assumes the following high-level architecture:

1. A sender composes a message using a MUA.

2. The message is submitted to a sending MTA, which forwards it to the GuardMail Stamping Service (GMS) or applies stamping locally.

3. The GMS computes content hashes, constructs a GMR, signs it, and attaches it to the message as a header and/or footer block.

4. The stamped message is delivered over existing SMTP infrastructure to the recipient’s MTA and MUA.

5. A VERIFIER (running as part of the MUA, a plugin, or a gateway) extracts the GMR, recomputes hashes, validates the signature, and presents a verification status.

GMP does not mandate where the GMS or VERIFIER reside; they MAY be implemented as standalone services, integrated gateways, MTA extensions, or client-side components.

## 5. GuardMail Receipt (GMR) Structure

A GMR is a structured metadata object that MUST contain at least the following fields:

* rid: A globally unique receipt identifier for this message.
* sender_id: A sender identity string representing the originator.
* org_id: An organization identifier for the sending domain or entity.
* hdr_hash: A SHA3-256 hash of the canonicalized header set.
* body_hash: A SHA3-256 hash of the canonicalized message body.
* att_hash: A SHA3-256 hash of the attachments, or the string "NONE" if there are no attachments.
* policy_id: An optional identifier referencing the policy or profile used when stamping this message.
* ts_issued: The timestamp at which the GMR was created.
* signature: A digital signature computed over the above fields using a key controlled by the GMS for the sending organization.
* verify_url: An HTTPS URL for independent verification.

The following header format is RECOMMENDED:

```
X-GuardMail-Stamp: rid=<ID>; sender_id=<sender>;
  org_id=<org>; hdr_hash=<hex>; body_hash=<hex>;
  att_hash=<hex-or-NONE>; ts=<ISO-8601>;
  sig_alg=<alg>; signature=<base64>; verify_url=<url>
```

A body footer MAY be added for human consumption:

```
----BEGIN GUARDMAIL RECEIPT----
Receipt-ID: <ID>
Sender-ID: <sender>
Org-ID: <org>
Issued-At: <timestamp>
Verification: https://verify.example.com/r/<ID>
----END GUARDMAIL RECEIPT----
```

The header representation is authoritative for automated verification; the footer is primarily cosmetic.

## 6. Outbound Stamping Process

The GuardMail Stamping Service (GMS) performs the following steps when stamping a message:

1. Canonicalize the headers and body.
2. Compute hdr_hash, body_hash, and att_hash.
3. Construct a GMR with the required fields.
4. Sign the GMR with an organizational key.
5. Insert the GMR into the message as an "X-GuardMail-Stamp" header and/or a footer block.
6. Deliver the stamped message to the next-hop MTA.

MUAs and intermediate MTAs SHOULD preserve the GMR header and any associated footer blocks.

## 7. Verification Process (Inbound)

A VERIFIER (or compatible component) MUST implement at least the following steps:

1. Extract the GMR from the "X-GuardMail-Stamp" header.
2. Canonicalize message headers and body using the same algorithm as the GMS.
3. Compute local hdr_hash, body_hash, and att_hash from the received message.
4. Compare the locally computed hashes with those contained in the GMR.

5. Validate the GMR signature using a trusted public key or certificate for the sending organization or GMS.

6. Optionally contact the verify_url endpoint for revocation checks, policy evaluation, or additional status information.

Based on these checks, the VERIFIER SHOULD produce one of:

* VALID

* TAMPERED

* UNTRUSTED

* NOT FOUND

## 8. Security Considerations

GMP is intended to raise the bar against impersonation, spoofing, and tampering by binding messages to both sender identity and content hashes through digital signatures. It does not replace the need for endpoint security, anti-malware, and user education.

Implementers MUST:

* Protect private keys used for GMR signing.

* Implement safe key rotation and revocation mechanisms.

* Address replay and downgrade attacks in the verification flow, including reuse of old GMRs with new messages or weaker policy profiles.

GMP does not protect against compromise of the sender’s device or account prior to GMR generation. If an attacker controls the sender’s environment, they MAY be able to send malicious but syntactically "valid" messages. Additional controls (for example, strong authentication, device posture checks, and anomaly detection) are REQUIRED to mitigate those threats.

GMP also does not replace the need for transport-level protections such as TLS or domain-based authentication mechanisms such as SPF, DKIM, and DMARC. Rather, it is intended to complement these mechanisms by providing cryptographic non-repudiation at the level of individual messages and senders.

## 9. IANA Considerations

This document requests the registration of a new email header field in the "Provisional Message Header Field Names" registry:

Header field name: X-GuardMail-Stamp

Applicable protocol: mail

Status: provisional

Author/Change controller: IESG

## 10. 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/info/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/info/rfc8174>.

## Authors' Addresses

Tom Madaras
GuardSuite, a VXMSecure Company
Hollywood, FL 33021
United States of America
Email: tom@vxmsecure.com

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