Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 26 June 2026

M. De Gennaro
Stalwart Labs

23 December 2025

MTA Hooks: An HTTP-Based Mail Processing Protocol
draft-degennaro-mta-hooks-00

Abstract

This document specifies MTA Hooks, an HTTP-based protocol enabling Mail Transfer Agents (MTAs) to delegate message processing decisions to external services. MTA Hooks provides a modern alternative to legacy mail filtering protocols by leveraging ubiquitous HTTP infrastructure, supporting both JSON and CBOR serialization, and offering fine-grained capability negotiation. The protocol supports both inbound message reception and outbound message delivery scenarios, allowing external scanners to inspect messages, modify content, and influence routing decisions at various stages of mail processing.

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 26 June 2026.

Copyright Notice

Table of Contents

1. Introduction

Mail Transfer Agents require extensible mechanisms to integrate with external services for spam filtering, virus scanning, policy enforcement, and compliance monitoring. While legacy protocols such as the Milter protocol have served this purpose, they present challenges in modern deployments including proprietary wire formats, limited tooling, and operational complexity.

MTA Hooks addresses these challenges by defining an HTTP-based protocol for mail processing delegation. The protocol leverages the widespread availability of HTTP client and server implementations, standard serialization formats, and established operational practices for HTTP services.

MTA Hooks achieves broad deployment compatibility by building upon standard HTTP semantics and methods, allowing implementers to leverage existing HTTP client and server libraries. The protocol supports both JSON and CBOR serialization to accommodate environments with different performance and parsing requirements. Capability negotiation during registration enables graceful feature discovery and forward compatibility as the protocol evolves. Mandatory transport encryption protects message content in transit, while the authentication mechanism remains pluggable to integrate with diverse deployment environments. The HTTP foundation ensures compatibility with existing operational infrastructure including load balancers, reverse proxies, and monitoring systems.

MTA Hooks supports two primary use cases: inbound processing during message reception from remote clients, and outbound processing during message delivery to remote servers. Both scenarios follow a consistent request-response pattern where the MTA invokes the registered hook endpoints at configured processing stages.

1.1. Notational Conventions

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.

1.2. Terminology

The following terms are used throughout this document:

* MTA (Mail Transfer Agent): A software component responsible for transferring electronic mail messages between hosts, as described in [RFC5321].

* Hook Endpoint: An HTTP server endpoint that receives hook invocations from an MTA and returns processing instructions.

* Scanner: A service that registers with an MTA to receive hook invocations. Scanners perform functions such as spam filtering, virus scanning, or policy enforcement. The terms "scanner" and "hook endpoint" are used interchangeably when referring to the service receiving hook requests.

* Registration: The process by which a scanner establishes a relationship with an MTA, including capability negotiation and callback URL configuration.

* Inbound Processing: Hook invocation during message reception, when the MTA accepts a message from a remote SMTP client.

* Outbound Processing: Hook invocation during message delivery, when the MTA transmits a message to a remote SMTP server.

* Stage: A specific point in mail processing at which the MTA invokes registered hooks. Different stages provide access to different message properties.

* Action: An instruction from a scanner indicating how the MTA should proceed with message processing.

* Modification: A change to message properties requested by a scanner, expressed as operations on the hook request object.

1.3. Data Types

This specification defines several object types used throughout the protocol. The following primitive types are used:

String
: A JSON string value.

Int
: An integer in the range -2^53+1 <= value <= 2^53-1.

UnsignedInt
: An integer in the range 0 <= value <= 2^53-1.

Boolean
: A JSON boolean value (true or false).

UTCDate
: A string in "date-time" format as defined in [RFC3339], where the time-offset component MUST be "Z" (UTC time). For example, "2024-12-21T15:30:00Z".

2. Protocol Overview

MTA Hooks defines a request-response protocol where the MTA acts as an HTTP client and scanners act as HTTP servers. During mail processing, the MTA constructs a request containing message properties and context information, transmits it to registered scanner endpoints, and processes the response to determine subsequent actions.

2.1. Architecture

The protocol architecture consists of three primary components:

1. The MTA, which initiates HTTP requests to scanner endpoints at configured processing stages.

2. Scanner services, which receive requests, perform analysis, and return responses containing actions and modifications.

3. A registration mechanism through which scanners declare their capabilities and subscribe to specific processing stages.

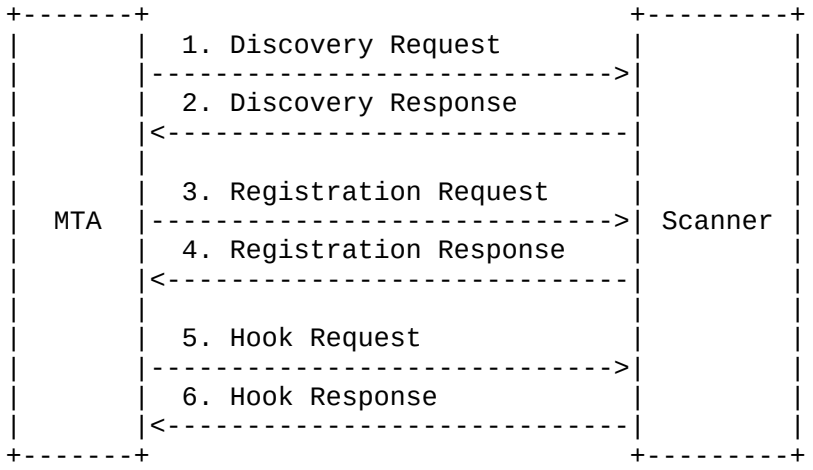

Figure 1: MTA Hooks Protocol Flow

The protocol flow proceeds as follows:

1. The MTA discovers scanner capabilities by requesting the well-known discovery endpoint.

2. The scanner returns a discovery document describing supported stages, actions, and configuration options.

3. The scanner submits a registration request specifying desired stages, properties, and callback configuration.

4. The MTA validates the request, optionally verifies the callback endpoint, and returns registration confirmation.

5. During mail processing, the MTA invokes the scanner’s callback URL with message properties and context.

6. The scanner returns a response containing an action and optional modifications.

2.2. Serialization

Requests and responses are serialized using either JSON [RFC8259] or CBOR [RFC8949]. The serialization format is negotiated during registration and indicated via HTTP Content-Type headers.

For JSON serialization, the Content-Type header MUST be "application/json". For CBOR serialization, the Content-Type header MUST be "application/cbor".

Binary data handling differs between formats. In JSON serialization, binary content such as message body parts MUST be encoded using Base64. In CBOR serialization, binary content SHOULD be transmitted as raw byte strings.

2.3. Processing Stages

MTA Hooks defines processing stages for both inbound and outbound message handling. Scanners subscribe to specific stages during registration and receive invocations only for subscribed stages.

2.3.1. Inbound Stages

Inbound stages correspond to SMTP protocol events during message reception:

* connect: Invoked when a remote client establishes a connection, before any SMTP commands are exchanged.

* ehlo: Invoked after the client sends EHLO or HELO command.

* mail: Invoked after each MAIL FROM command.

* rcpt: Invoked after each RCPT TO command. This stage may be invoked multiple times per transaction.

* data: Invoked after the complete message has been received, following the DATA command and message content.

2.3.2. Outbound Stages

Outbound stages correspond to delivery events during message transmission:

* delivery: Invoked after a delivery attempt completes for all recipients, regardless of success or failure.

* defer: Invoked only when at least one recipient delivery cannot be completed and requires retry.

* dsn: Invoked when the MTA generates a Delivery Status Notification of any type.

For outbound stages, the hook is invoked once after delivery attempts for all recipients in a given delivery batch have completed. The scanner receives the delivery status for each recipient and may modify per-recipient handling.

2.4. Inbound Message Processing

During inbound processing, the MTA invokes registered hooks as it receives messages from remote SMTP clients. This corresponds to traditional mail filtering scenarios where external services inspect incoming mail for spam, viruses, or policy violations.

The inbound flow proceeds through SMTP protocol stages:

1. A remote client connects to the MTA.

2. The MTA invokes hooks registered for the "connect" stage.

3. The client sends EHLO/HELO; the MTA invokes "ehlo" stage hooks.

4. The client sends MAIL FROM; the MTA invokes "mail" stage hooks.

5. The client sends one or more RCPT TO commands; the MTA invokes "rcpt" stage hooks for each.

6. The client sends DATA and message content; the MTA invokes "data" stage hooks.

At each stage, scanners may instruct the MTA to accept, reject, or modify the transaction.

2.4.1. Multiple Scanner Handling

When multiple scanners are registered for the same stage, the MTA invokes them sequentially in an implementation-defined order. Each scanner’s response affects the request seen by subsequent scanners.

The scanner chain terminates early when a scanner returns a terminal action:

* Inbound terminal actions: "reject", "discard", "disconnect"

* Outbound terminal actions: "cancel"

Non-terminal actions ("accept", "quarantine" for inbound; "continue" for outbound) allow the chain to proceed, and subsequent scanners may override these actions.

Implementations SHOULD provide configuration options for:

* Scanner invocation order (priority-based or explicit ordering)

* Whether to allow subsequent scanners to override "quarantine" decisions

* Logging of chain termination events for operational visibility

Example chain behavior:

1. Scanner A (spam filter) sets action to "accept" and adds X-Spam-Score header

2. Scanner B (virus scanner) receives modified request, detects malware, sets action to "reject"

3. Chain terminates; Scanner C is not invoked

4. MTA rejects the message

2.5. Outbound Message Processing

During outbound processing, the MTA invokes registered hooks as it delivers messages to remote SMTP servers. This supports use cases including delivery logging, compliance monitoring, and routing decisions.

The outbound flow proceeds as follows:

1. The MTA selects a queued message for delivery and identifies the recipients due for delivery at this time.

2. The MTA attempts delivery to all selected recipients.

3. After all attempts in this delivery job complete, the MTA invokes hooks registered for the "delivery" stage.

4. If any recipient requires retry, the MTA invokes "defer" stage hooks.

5. If the MTA generates a DSN, it invokes "dsn" stage hooks before sending.

A delivery job represents a single processing cycle where the MTA retrieves a message from the queue and attempts delivery to one or more recipients. The specific batching of recipients into delivery jobs is implementation-defined and may depend on factors such as destination domain, connection reuse, or queue configuration. The "delivery" stage hook is invoked once per delivery job after all recipient attempts within that job have completed.

Scanners may modify per-recipient delivery status, suppress DSN generation, or alter retry scheduling.

2.6. Modifications

Scanners communicate changes through modifications to the hook request object. Modifications are expressed as operations on JSON Pointers [RFC6901] referencing properties within the request structure.

Three modification operations are supported:

* Set: Replace the value at a specified path.

* Add: Insert a value at a specified path, including array element insertion.

* Delete: Remove the value at a specified path.

The MTA applies modifications in a defined order: set operations first, followed by add operations, and finally delete operations. Any modification that fails (for example, referencing a non-existent path for deletion) SHOULD be logged and included in failure statistics, but MUST NOT cause the entire response to be rejected.

If a scanner modifies both the "message" and "rawMessage" properties, the "rawMessage" modification takes precedence and "message" modifications are ignored.

3. Discovery

MTAs discover scanner capabilities through a well-known HTTP endpoint. Discovery is OPTIONAL; scanner endpoints MAY alternatively be configured manually.

3.1. Well-Known Endpoint

Scanners that support discovery MUST expose a discovery document at the path "/.well-known/mta-hooks". The MTA retrieves this document using an HTTP GET request.

The discovery endpoint MUST support JSON serialization. Support for CBOR serialization is OPTIONAL.

3.2. Discovery Document Format

The discovery document is a JSON or CBOR object containing the following fields:

version: String
The protocol version. This specification defines version "1.0".

endpoints: DiscoveryEndpoints
URLs for protocol operations.

serialization: String[]
Supported serialization formats. Valid values are "json" and "cbor".

capabilities: DiscoveryCapabilities
Supported protocol capabilities.

limits: DiscoveryLimits|null
Operational limits, or null if no specific limits are advertised.

extensions: String[]|null
Supported protocol extensions. Extension identifiers SHOULD use a reverse domain name prefix for vendor-specific extensions.

A *DiscoveryEndpoints* object has the following properties:

registration: String
URL path for submitting registration requests.

deregistration: String
URL path template for deregistration, with "{registration_id}" placeholder.

A *DiscoveryCapabilities* object has the following properties:

inbound: DirectionCapabilities|null Inbound processing
capabilities, or null if inbound processing is not supported.

outbound: DirectionCapabilities|null Outbound processing
capabilities, or null if outbound processing is not supported.

A *DirectionCapabilities* object has the following properties:

stages: String[]
Supported stages for this processing direction.

actions: String[]
Supported actions that scanners may request.

fetchProperties: String[]
JSON Pointers for properties the MTA can include in hook requests.

updateProperties: String[]
JSON Pointers for properties scanners may modify.

A *DiscoveryLimits* object has the following properties:

maxMessageSize: UnsignedInt|null Maximum message size in bytes the scanner accepts.

maxRegistrations: UnsignedInt|null Maximum concurrent registrations.

timeoutMs: UnsignedInt|null Default timeout in milliseconds for hook invocations.

The fetchProperties and updateProperties arrays contain JSON Pointers as defined in [RFC6901]. Each pointer identifies a property within the hook request structure that the MTA supports including or that scanners may modify. For example, "/envelope/from/address" refers to the sender’s email address within the envelope object.

3.2.1. Example Discovery Document

```
{
  "version": "1.0",

  "endpoints": {
    "registration": "/v1/hooks/register",
    "deregistration": "/v1/hooks/register/{registration_id}"
  },

  "serialization": ["json", "cbor"],

  "capabilities": {
    "inbound": {
      "stages": ["connect", "ehlo", "mail", "rcpt", "data"],
      "actions": ["accept", "reject", "discard",
                  "quarantine", "disconnect"],
      "fetchProperties": ["/envelope", "/message", "/rawMessage",
                          "/server", "/tls", "/auth", "/senderAuth",
                          "/client", "/stage", "/action",
                          "/timestamp","/response", "/protocol",
                          "/queue"],
      "updateProperties": ["/envelope", "/message", "/rawMessage",
                           "/action", "/response"]
    },
    "outbound": {
      "stages": ["delivery", "defer", "dsn"],
      "actions": ["continue", "cancel"],
      "fetchProperties": ["/envelope", "/message", "/rawMessage",
                          "/server", "/queue", "/stage", "/action",
                          "/timestamp", "/protocol"],
      "updateProperties": ["/envelope/to", "/action", "/message",
                           "/rawMessage"]
    }
  },

  "limits": {
    "maxMessageSize": 52428800,
    "maxRegistrations": 64,
    "timeoutMs": 30000
  },

  "extensions": ["x-vendor-feature"]
}
```

3.3. Manual Configuration

Discovery is OPTIONAL. Administrators MAY configure scanner endpoints manually, including capability restrictions and authentication credentials. Manual configuration may be necessary in environments where the well-known endpoint is not accessible or where policy requires explicit configuration.

4. Registration

Scanners register with MTAs to establish callback configuration and negotiate capabilities. Registration creates a persistent relationship that remains active until explicit deregistration or expiration.

4.1. Registration Request

Scanners submit registration requests via HTTP POST to the registration endpoint. The request body contains a JSON or CBOR object with the following fields:

name: String
: Human-readable name identifying the scanner.

version: String|null
: Scanner software version string.

callback: CallbackConfig
: Callback configuration.

expiresAt: UTCDate|null
: Requested registration expiration timestamp. The MTA MAY assign a different expiration based on policy.

serialization: String
: Requested serialization format for hook requests. MUST be a value from the MTA’s supported serialization list.

inbound: StageSubscription|null
: Inbound hook configuration. Omit or set to null if not subscribing to inbound stages.

outbound: StageSubscription|null
: Outbound hook configuration. Omit or set to null if not subscribing to outbound stages.

filter: FilterOperator|FilterCondition|null

Filter configuration to limit which messages trigger hooks. Uses filter syntax from Section 5.5 of [RFC8620].

metadata: String[String]|null
Arbitrary key-value pairs for scanner identification and operational metadata.

A *CallbackConfig* object has the following properties:

url: String
HTTPS URL where the MTA sends hook requests.

timeoutMs: UnsignedInt|null
Requested timeout in milliseconds. The MTA MAY ignore or cap this value.

A *StageSubscription* object has the following properties:

stages: String[]
Stages to subscribe to. MUST be a subset of the MTA's supported stages for this direction.

properties: String[]|null
JSON Pointers specifying message properties to receive. A value of null requests all supported properties.

At least one of "inbound" or "outbound" MUST be present and non-null in the registration request.

4.1.1. Filter Configuration

The filter field uses the FilterOperator and FilterCondition syntax defined in Section 5.5 of [RFC8620]. A FilterOperator combines multiple conditions using AND, OR, or NOT logic. A FilterCondition specifies criteria that a message must match.

Filter conditions follow Section 4.4.1 of [RFC8621] with the following restrictions on metadata conditions: only the "size" condition from Section 4.1.1 of [RFC8621] is permitted. All other metadata conditions are NOT supported as they depend on mailbox state or JMAP-specific concepts not applicable to MTA processing:

* inMailbox

* inMailboxOtherThan

* before

* after
* minSize
* maxSize
* allInThreadHaveKeyword
* someInThreadHaveKeyword
* noneInThreadHaveKeyword
* hasKeyword
* notKeyword

All other filter conditions defined in Section 4.4.1 of [RFC8621] are permitted by this specification, including text-matching conditions such as "from", "to", "cc", "bcc", "subject", "body", "header", and "text". However, support for specific conditions is determined by the MTA implementation. If a scanner specifies a filter condition that the MTA does not support, the registration MUST be rejected with an UNSUPPORTED_FILTER error.

The following additional conditions are defined for envelope filtering:

envelopeFrom: String
: Matches if the MAIL FROM address matches the given value. The value MAY include wildcards using the "*" character, which matches zero or more characters.

envelopeTo: String
: Matches if any RCPT TO address matches the given value. The value MAY include wildcards using the "*" character, which matches zero or more characters.

Filters apply only to the "data" stage for content-based conditions (those examining message headers or body). For the "mail" and "rcpt" stages, only envelopeFrom and envelopeTo conditions are evaluated; other conditions are ignored for these stages. Messages or envelope commands not matching the filter do not trigger hook invocations.

4.1.2. Example Registration Request

```
POST /v1/hooks/register HTTP/1.1
Host: mta.example.com
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJIUzI1NiIs...

{
  "name": "Acme Spam Filter",
  "version": "2.1.0",

  "callback": {
    "url": "https://scanner.example.com/hooks/scan",
    "timeoutMs": 25000
  },

  "expiresAt": "2025-12-21T15:30:00Z",

  "serialization": "json",

  "inbound": {
    "stages": ["data"],
    "properties": ["/message", "/envelope", "/senderAuth"]
  },

  "outbound": {
    "stages": ["delivery"],
    "properties": null
  },

  "filter": {
    "operator": "OR",
    "conditions": [
      {"from": "*@external.example.com"},
      {"envelopeFrom": "*@partner.example.org"}
    ]
  },

  "metadata": {
    "vendor": "acme-security",
    "environment": "production",
    "instance": "scanner-01"
  }
}
```

4.2. Callback Verification

Upon receiving a registration request, the MTA SHOULD verify that the callback URL is reachable and operated by the registering party. Verification proceeds as follows:

1. The MTA generates a unique verification token.

2. The MTA sends an HTTP POST request to the callback URL with Content-Type set to the serialization format requested in the registration request. The request body contains:

```
{
  "action": "verify",
  "token": "vrf_8f3a2b1c9d4e5f6a7b8c9d0e1f2a3b4c"
}
```

1. The scanner MUST respond with HTTP status 200 and a body containing the same token:

```
{
  "token": "vrf_8f3a2b1c9d4e5f6a7b8c9d0e1f2a3b4c"
}
```

1. The MTA confirms the response token matches the request token.

If verification fails, the MTA MUST reject the registration request:

* If the callback URL is unreachable or times out: HTTP 422 with error code CALLBACK_UNREACHABLE

* If the callback responds but the token does not match: HTTP 422 with error code CALLBACK_VERIFICATION_FAILED

* If the callback URL does not use HTTPS: HTTP 422 with error code TLS_REQUIRED

* If the callback URL's TLS certificate is invalid: HTTP 422 with error code TLS_CERTIFICATE_INVALID

4.3. Registration Response

Upon successful registration, the MTA returns HTTP status 201 Created with a response body containing:

registrationId: String
: Unique identifier for this registration. The identifier MUST consist of ASCII alphanumeric characters plus hyphen (-), underscore (_), and colon (:), with a maximum length of 255 characters.

status: String
: Registration status. Values are "active", "suspended", or "pending_verification".

createdAt: UTCDate
Timestamp of registration creation.

expiresAt: UTCDate|null
Timestamp when registration expires, or null if no expiration is set.

callback: CallbackConfig
Confirmed callback configuration, which may differ from the request if the MTA adjusted values.

negotiated: NegotiatedCapabilities
Final negotiated capabilities representing the intersection of scanner request and MTA support.

endpoints: RegistrationEndpoints
URLs for managing this registration.

A *NegotiatedCapabilities* object has the following properties:

serialization: String
Confirmed serialization format.

inbound: NegotiatedSubscription|null
Confirmed inbound configuration, or null if not registered for inbound processing.

outbound: NegotiatedSubscription|null
Confirmed outbound configuration, or null if not registered for outbound processing.

A *NegotiatedSubscription* object has the following properties:

stages: String[]
Confirmed stages.

properties: String[]
Confirmed property list.

A *RegistrationEndpoints* object has the following properties:

deregistration: String
URL for deregistration requests.

status: String
URL for status queries.

4.3.1. Example Registration Response

```
HTTP/1.1 201 Created
Content-Type: application/json
Location: /v1/hooks/register/reg_7a3b9c2e-4d5f-6a7b-8c9d-0e1f2a3b4c5d

{
  "registrationId": "reg_7a3b9c2e-4d5f-6a7b-8c9d-0e1f2a3b4c5d",
  "status": "active",
  "createdAt": "2024-12-21T15:30:00Z",
  "expiresAt": "2025-12-21T15:30:00Z",

  "callback": {
    "url": "https://scanner.example.com/hooks/scan",
    "timeoutMs": 25000
  },

  "negotiated": {
    "serialization": "json",
    "inbound": {
      "stages": ["data"],
      "properties": ["/message", "/envelope", "/senderAuth"]
    },
    "outbound": {
      "stages": ["delivery"],
      "properties": ["/message", "/envelope", "/queue", "/server"]
    }
  },

  "endpoints": {
    "deregistration": "/v1/hooks/register/reg_7a3b9c2e",
    "status": "/v1/hooks/register/reg_7a3b9c2e/status"
  }
}
```

4.4. Authentication

Authentication for registration requests is REQUIRED but the specific mechanism is out of scope for this specification. Implementations SHOULD support at least one of the following authentication methods:

* Bearer tokens via the HTTP Authorization header

* Mutual TLS with client certificate verification

* HMAC-based pre-shared key authentication

See Section 9 for deployment guidance on authentication.

4.5. Registration Lifecycle

4.5.1. Status Queries

Scanners MAY query their registration status via HTTP GET to the status endpoint returned during registration.

```
GET /v1/hooks/register/reg_7a3b9c2e/status HTTP/1.1
Host: mta.example.com
Authorization: Bearer eyJhbGciOiJIUzI1NiIs...
```

The response contains registration status and optional statistics:

registrationId: String
The registration identifier.

status: String
Current status: "active", "suspended", or "deregistered".

createdAt: UTCDate|null
Timestamp of creation.

expiresAt: UTCDate|null
Timestamp of expiration.

lastInvocation: UTCDate|null
Timestamp of most recent hook invocation.

statistics: RegistrationStatistics|null
Operational statistics.

health: HealthStatus|null
Health check status.

A *RegistrationStatistics* object has the following properties:

invocations: InvocationCounts
Invocation counts.

errors: InvocationCounts
Error counts with the same time period structure as invocations.

averageResponseMs: Number
Average response time in milliseconds.

An *InvocationCounts* object has the following properties:

total: UnsignedInt

Total count since registration.

last24h: UnsignedInt
Count in past 24 hours.

last7d: UnsignedInt
Count in past 7 days.

last30d: UnsignedInt
Count in past 30 days.

A *HealthStatus* object has the following properties:

status: String
Health status: "healthy", "degraded", or "unhealthy".

lastCheck: UTCDate
Timestamp of last health check.

consecutiveFailures: UnsignedInt
Count of consecutive failed health checks.

4.5.2. Example Status Response

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "registrationId": "reg_7a3b9c2e-4d5f-6a7b-8c9d-0e1f2a3b4c5d",
  "status": "active",
  "createdAt": "2024-12-21T15:30:00Z",
  "expiresAt": "2025-12-21T15:30:00Z",
  "lastInvocation": "2024-12-21T16:42:18Z",

  "statistics": {
    "invocations": {
      "total": 15482,
      "last24h": 3241,
      "last7d": 10234,
      "last30d": 43210
    },
    "errors": {
      "total": 32,
      "last24h": 5,
      "last7d": 12,
      "last30d": 28
    },
    "averageResponseMs": 45
  },

  "health": {
    "status": "healthy",
    "lastCheck": "2024-12-21T16:44:00Z",
    "consecutiveFailures": 0
  }
}
```

4.5.3. Registration Expiration and Renewal

Registrations MAY have an expiration time set by the MTA based on policy. Scanners MUST re-register before expiration to maintain continuous service. Re-registration follows the same process as initial registration and requires full capability renegotiation.

The MTA SHOULD provide advance notice of pending expiration through the status endpoint. Scanners SHOULD monitor their registration status and initiate re-registration before expiration.

4.6. Deregistration

Scanners deregister by sending an HTTP DELETE request to the deregistration endpoint.

```
DELETE /v1/hooks/register/reg_7a3b9c2e HTTP/1.1
Host: mta.example.com
Authorization: Bearer eyJhbGciOiJIUzI1NiIs...
```

Upon successful deregistration, the MTA returns HTTP status 200 with confirmation:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "registrationId": "reg_7a3b9c2e-4d5f-6a7b-8c9d-0e1f2a3b4c5d",
  "status": "deregistered",
  "deregisteredAt": "2024-12-21T16:45:00Z"
}
```

After deregistration, the MTA MUST NOT send further hook invocations to the scanner's callback URL.

4.6.1. In-Flight Requests

Hook invocations that are in-flight at the time of deregistration MAY complete normally. The MTA SHOULD accept and process responses from these in-flight invocations. Scanners SHOULD continue to respond to hook requests that arrive during or shortly after deregistration processing, as network latency may cause requests dispatched before deregistration to arrive afterward.

Once deregistration completes, the MTA MUST NOT initiate new hook invocations to the deregistered scanner's callback URL. The MTA SHOULD allow a brief grace period (implementation-defined, but typically a few seconds) for in-flight responses before considering the deregistration fully complete.

4.6.2. Automatic Deregistration

The MTA MAY automatically deregister scanners that become unreachable. Implementation-specific policies govern the threshold for automatic deregistration, such as consecutive failure counts or timeout periods. The MTA SHOULD log automatic deregistrations for operational visibility.

5. Hook Request

When processing reaches a stage for which scanners are registered, the MTA constructs a hook request and transmits it to each registered scanner's callback URL.

5.1. Request Structure

Hook requests are transmitted via HTTP POST to the scanner's callback URL. The Content-Type header indicates the serialization format negotiated during registration.

The MTA MAY include an X-MTA-Hooks-Registration header containing the registration identifier. This header is OPTIONAL but can assist scanners that handle multiple registrations at a single endpoint.

The request body contains a JSON or CBOR object with properties determined by the scanner's registration. The following sections describe available properties organized by category.

5.2. Common Properties

The following properties are available for both inbound and outbound processing:

stage: String
: The current processing stage.

action: String
: The action the MTA will perform if no scanner modifications occur. For inbound processing, values are "accept", "reject", "discard", "quarantine", or "disconnect". For outbound processing, values are "continue" or "cancel".

envelope: Envelope
: The message envelope containing sender and recipient information.

message: Object|null
: A structured representation of the email message based on the Email object defined in Section 4 of [RFC8621].

rawMessage: String|null
: The complete message in Internet Message Format as defined in [RFC5322]. In JSON serialization, the value is Base64-encoded. In CBOR serialization, the value is a raw byte string.

timestamp: UTCDate
: Timestamp when the current stage began.

protocol: ProtocolInfo|null
: Protocol information.

queue: QueueInfo|null
: Queue information.

server: ServerInfo|null
Information about the MTA.

5.3. Envelope Properties

An *Envelope* object has the following properties:

from: EnvelopeAddress
Sender information from MAIL FROM command.

to: EnvelopeAddress[]|DeliveryRecipient[]
Recipient information from RCPT TO commands. For inbound processing, this is an array of EnvelopeAddress objects. For outbound processing, this is an array of DeliveryRecipient objects.

An *EnvelopeAddress* object represents an address in the message envelope and has the following properties:

address: String|null The email address. For MAIL FROM, this MAY be null to represent the null reverse-path. For RCPT TO, this MUST NOT be null.

parameters: String[String] SMTP parameters associated with the address as key-value pairs. Common parameters include ORCPT, ENVID, and other DSN-related parameters defined in [RFC3461].

For outbound processing, recipient objects include additional delivery status fields described in Section 5.9.

5.4. Queue Properties

A *QueueInfo* object has the following properties:

id: String
Unique queue identifier for this message within this MTA. The identifier MUST be unique for the lifetime of the message in the queue and SHOULD remain stable across hook invocations for the same queued message.

5.5. Message Properties

5.5.1. Structured Message

The message property contains a structured representation of the email message based on the Email object defined in Section 4 of [RFC8621]. The following differences from the JMAP Email object apply:

* Metadata properties defined in Section 4.1.1 of [RFC8621] are not included, with the exception of the "size" property which MAY be present.

* The blobId property is replaced by a blob property containing the actual content. In JSON serialization, blob values are Base64-encoded strings. In CBOR serialization, blob values are raw byte strings.

Property availability depends on the processing stage and MTA capabilities. At early stages such as "connect" or "ehlo", message properties are not available.

5.5.2. Raw Message

The rawMessage property contains the complete message in Internet Message Format as defined in [RFC5322], including all MIME parts and attachments. In JSON serialization, the value is Base64-encoded. In CBOR serialization, the value is a raw byte string.

The rawMessage property represents the entire message as stored or received by the MTA. When present, it provides byte-exact access to the message content, which is necessary for operations such as cryptographic signature verification.

Scanners MAY request both message and rawMessage properties. If a scanner’s response modifies both properties, only rawMessage modifications are applied; message modifications are ignored.

The raw message content MUST NOT appear within the message property as a blob value. The message property contains only the structured parsed representation with individual body part contents available via bodyValues, while rawMessage contains the complete unparsed message.

5.5.3. Choosing Between Structured and Raw

The message property provides a structured, parsed representation suitable for:

* Header inspection and modification

* Recipient analysis

* Content-type aware body part processing

* Efficient access to specific message components

The rawMessage property provides the complete RFC 5322 message suitable for:

* Cryptographic verification (DKIM signature validation)

* Archival or compliance logging

* Processing that requires byte-exact message content

* Forwarding or re-injection without modification

Scanners that need both structured access and raw content SHOULD request both properties. When modifying messages, scanners SHOULD prefer structured modifications via the message property unless byte-exact control is required. Modifications to rawMessage require the scanner to produce a complete, valid RFC 5322 message.

5.6. Server Properties

A *ServerInfo* object has the following properties:

name: String
: Server hostname.

ip: String
: Server IP address.

port: UnsignedInt
: Server port number.

5.7. Protocol Properties

A *ProtocolInfo* object has the following properties:

version: String
: MTA Hooks protocol version.

5.8. Inbound Properties

The following properties are available only during inbound processing:

response: SmtpResponse|null The SMTP response the MTA would send if no scanner modifications occur.

client: ClientInfo|null Information about the connecting SMTP client.

senderAuth: SenderAuthentication|null Results of sender authentication checks.

auth: SmtpAuthentication|null SMTP authentication information, if the client authenticated.

tls: TlsInfo|null TLS connection information.

5.8.1. SMTP Response Properties

An *SmtpResponse* object represents an SMTP response and has the following properties:

code: UnsignedInt
The three-digit SMTP status code.

enhancedCode: String|null
The enhanced status code as defined in [RFC3461], if available.

message: String
The human-readable response text.

5.8.2. Client Properties

A *ClientInfo* object has the following properties:

ip: String
Client IP address.

port: UnsignedInt
Client port number.

ptr: String|null
PTR record for client IP, if available.

ehlo: String
EHLO or HELO string sent by client.

asn: UnsignedInt|null
Autonomous System Number for client IP, if available.

country: String|null
ISO 3166-1 alpha-2 country code for client IP, if available.

activeConnections: UnsignedInt|null
Number of concurrent connections from this client.

5.8.3. TLS Properties

A *TlsInfo* object has the following properties:

version: String
: TLS protocol version (e.g., "TLSv1.3").

cipher: String
: Cipher suite name.

cipherBits: UnsignedInt
: Cipher key length in bits.

certIssuer: String|null
: Client certificate issuer, if a client certificate was presented.

certSubject: String|null
: Client certificate subject, if a client certificate was presented.

5.8.4. Sender Authentication Properties

A *SenderAuthentication* object has the following properties:

spf-ehlo: String|null SPF result for EHLO identity as defined in [RFC7208].

spf-mail: String|null SPF result for MAIL FROM identity as defined in [RFC7208].

dkim: String|null DKIM verification result as defined in [RFC6376].

arc: String|null ARC verification result.

dmarc: String|null DMARC evaluation result as defined in [RFC7489].

Authentication result values follow the conventions established in the respective specifications.

5.8.5. SMTP Authentication Properties

An *SmtpAuthentication* object has the following properties:

login: String
: Authenticated username.

method: String

SASL mechanism used for authentication.

5.9. Outbound Properties

The following properties are available only during outbound processing.

5.9.1. Extended Queue Properties

For outbound processing, the queue property uses an *OutboundQueueInfo* object, which extends QueueInfo with additional fields:

id: String
: Unique queue identifier for this message.

expiresAt: UTCDate|null
: Timestamp when the queue entry expires.

attempts: UnsignedInt
: Total delivery attempts made so far.

5.9.2. Recipient Delivery Status

For outbound processing, each recipient in envelope.to is represented as a DeliveryRecipient object.

A *DeliveryRecipient* object extends EnvelopeAddress with delivery status information and has the following properties:

address: String
: The recipient email address.

parameters: String[String]
: SMTP parameters associated with the address as key-value pairs.

status: String
: The delivery status for this recipient. Values are "pending", "delivered", "deferred", "failed", or "failed-silent".

attempt: UnsignedInt
: The current delivery attempt number for this recipient.

lastResponse: SmtpResponse|null
: The last SMTP response received for this recipient, or null if no attempt has been made.

nextAttemptAt: UTCDate|null

The scheduled time for the next delivery attempt, or null if no retry is scheduled.

nextDsnAt: UTCDate|null
The scheduled time for the next DSN generation, or null if no DSN is scheduled.

queueName: String|null
The name of the outbound queue handling this recipient, if applicable.

For the "dsn" stage, the message and rawMessage properties contain the DSN message that the MTA is about to send. Scanners MAY modify or delete these properties to alter or suppress DSN generation.

5.10. Example Inbound Hook Request

```
POST /hooks/scan HTTP/1.1
Host: scanner.example.com
Content-Type: application/json
X-MTA-Hooks-Registration: reg_7a3b9c2e

{
  "stage": "data",
  "action": "accept",
  "timestamp": "2024-12-21T16:30:00Z",

  "response": {
    "code": 250,
    "enhancedCode": "2.0.0",
    "message": "OK"
  },

  "protocol": {
    "version": "1.0"
  },

  "queue": {
    "id": "queue_abc123"
  },

  "envelope": {
    "from": {
      "address": "sender@example.org",
      "parameters": {}
    },
    "to": [
      {
```

```
          "address": "recipient@example.com",
          "parameters": {}
        }
      ]
    },

    "message": {
      "size": 2048,
      "subject": "Meeting Tomorrow",
      "from": [
        {
          "name": "Sender Name",
          "email": "sender@example.org"
        }
      ],
      "to": [
        {
          "email": "recipient@example.com"
        }
      ],
      "sentAt": "2024-12-21T16:29:00Z",
      "messageId": ["<msg123@example.org>"],
      "headers": [
        {"name": "From", "value": "Sender Name <sender@example.org>"},
        {"name": "To", "value": "recipient@example.com"},
        {"name": "Subject", "value": "Meeting Tomorrow"},
        {"name": "Date", "value": "Sat, 21 Dec 2024 16:29:00 +0000"},
        {"name": "Message-ID", "value": "<msg123@example.org>"}
      ],
      "bodyStructure": {
        "type": "text/plain",
        "charset": "utf-8",
        "size": 28
      },
      "bodyValues": {
        "1": {
          "value": "Let's meet tomorrow at 10am.",
          "isEncodingProblem": false,
          "isTruncated": false
        }
      }
    },

    "client": {
      "ip": "192.0.2.100",
      "port": 54321,
      "ptr": "mail.example.org",
      "ehlo": "mail.example.org",
```

```
      "activeConnections": 3
    },

    "server": {
      "name": "mx1.example.com",
      "ip": "198.51.100.25",
      "port": 25
    },

    "tls": {
      "version": "TLSv1.3",
      "cipher": "TLS_AES_256_GCM_SHA384",
      "cipherBits": 256
    },

    "senderAuth": {
      "spf-mail": "pass",
      "dkim": "pass",
      "dmarc": "pass"
    }
  }
```

5.11. Example Outbound Hook Request

```
  POST /hooks/delivery HTTP/1.1
  Host: scanner.example.com
  Content-Type: application/json
  X-MTA-Hooks-Registration: reg_7a3b9c2e

  {
    "stage": "delivery",
    "action": "continue",
    "timestamp": "2024-12-21T17:00:00Z",

    "protocol": {
      "version": "1.0"
    },

    "queue": {
      "id": "queue_def456",
      "expiresAt": "2024-12-24T17:00:00Z",
      "attempts": 3
    },

    "envelope": {
      "from": {
        "address": "notifications@example.com",
        "parameters": {}
```

```
      },
      "to": [
        {
          "address": "user1@recipient.example",
          "parameters": {},
          "status": "delivered",
          "attempt": 1,
          "lastResponse": {
            "code": 250,
            "enhancedCode": "2.0.0",
            "message": "Message accepted"
          }
        },
        {
          "address": "user2@recipient.example",
          "parameters": {},
          "status": "deferred",
          "attempt": 3,
          "lastResponse": {
            "code": 451,
            "enhancedCode": "4.7.1",
            "message": "Try again later"
          },
          "nextAttemptAt": "2024-12-21T18:00:00Z",
          "nextDsnAt": "2024-12-22T17:00:00Z"
        }
      ]
    },

    "message": {
      "subject": "Your order has shipped",
      "from": [{"email": "notifications@example.com"}],
      "to": [
        {"email": "user1@recipient.example"},
        {"email": "user2@recipient.example"}
      ],
      "size": 4096
    },

    "server": {
      "name": "smtp-out.example.com",
      "ip": "198.51.100.50",
      "port": 25
    }
  }
```

6. Hook Response

Scanners respond to hook requests with modifications to the request object. These modifications instruct the MTA how to proceed with message processing.

6.1. Response Structure

Scanners respond with an HTTP 200 status code. The response body contains a JSON or CBOR object specifying modifications to apply to the hook request. The object has the following fields:

set: SetOperation[]|null An array of set operations to apply, or null if no set operations.

add: AddOperation[]|null An array of add operations to apply, or null if no add operations.

delete: DeleteOperation[]|null An array of delete operations to apply, or null if no delete operations.

A *SetOperation* object has the following properties:

path: String
JSON Pointer (per [RFC6901]) to the property to replace.

value: any
The new value for the property.

An *AddOperation* object has the following properties:

path: String
JSON Pointer to the location where the value should be added.

value: any
The value to add.

index: UnsignedInt|null
For array additions, the zero-based index at which to insert the value. If null or omitted, the value is appended to the array.

A *DeleteOperation* object has the following properties:

path: String
JSON Pointer to the property to remove.

6.2. Actions

Scanners change the MTA's action by including a set operation targeting the "/action" path. The following values are valid for inbound and outbound processing respectively.

The following action values are valid:

6.2.1. Inbound Actions

accept
: Accept the message for delivery to recipients. Non-terminal; chain continues.

reject
: Reject the message and return an error response to the sending client. Terminal; chain stops.

discard
: Accept the message from the client but do not deliver it. The client receives a success response. Terminal; chain stops.

quarantine
: Accept the message and place it in quarantine for administrative review. Quarantine location and handling are implementation-defined. Non-terminal; chain continues.

disconnect
: Terminate the SMTP connection immediately. Terminal; chain stops.

6.2.2. Outbound Actions

continue Proceed with normal processing. Non-terminal; chain continues.

cancel Cancel all pending deliveries for this message. Terminal; chain stops.

6.3. Modifications

Scanners communicate changes by specifying operations on the hook request object. The response contains JSON Pointer paths identifying properties to modify and the operations to perform. These modifications can alter any aspect of the transaction that the MTA permits, including:

* The action the MTA should take (accept, reject, quarantine, etc.)

* The SMTP response to send to the client or expect from the server

* Message headers and body content

* Envelope addresses (sender and recipients)

* Per-recipient delivery status for outbound processing

Three modification operations are supported:

set
Replace the value at a specified path with a new value.

add
Insert a value at a specified path. For objects, this adds a new property. For arrays, this inserts an element at the specified index or appends if no index is given.

delete
Remove the value at a specified path.

6.3.1. Set Operations

Set operations replace values at specified paths.

```
{
  "set": [
    {
      "path": "/action",
      "value": "reject"
    },
    {
      "path": "/response",
      "value": {
        "code": 550,
        "enhancedCode": "5.7.1",
        "message": "Message rejected due to policy"
      }
    }
  ]
}
```

6.3.2. Add Operations

Add operations insert new values. For arrays, an optional index specifies insertion position.

```
{
  "add": [
    {
      "path": "/message/headers",
      "value": {"name": "X-Spam-Score", "value": "5.2"},
      "index": 0
    },
    {
      "path": "/envelope/to",
      "value": {
        "address": "archive@example.com",
        "parameters": {}
      }
    }
  ]
}
```

6.3.3. Delete Operations

Delete operations remove values at specified paths. When deleting array elements, indices refer to positions in the array at the time each delete operation executes. Because delete operations execute sequentially and earlier deletions cause subsequent elements to shift to lower indices, scanners SHOULD order array deletions from highest to lowest index to avoid unexpected results.

For example, to delete elements originally at indices 1 and 3 from an array:

```
{
  "delete": [
    {"path": "/message/headers/3"},
    {"path": "/message/headers/1"}
  ]
}
```

Deleting index 3 first leaves the element originally at index 1 still at index 1. If the order were reversed, deleting index 1 first would shift the element originally at index 3 to index 2.

6.3.4. Modification Order

The MTA applies modifications in the following order:

1. Set operations

2. Add operations

3. Delete operations

This ordering allows predictable results when multiple operations affect related paths.

To change the action the MTA takes, the scanner sets the "/action" path to the desired value. To modify the SMTP response, the scanner can either set individual response fields (e.g., "/response/code", "/response/message") or replace the entire response object by setting "/response".

If a scanner modifies both the "message" and "rawMessage" properties, the "rawMessage" modification takes precedence and "message" modifications are ignored.

6.3.5. Conflicting Operations

If a response contains multiple operations targeting the same path or overlapping paths, the MTA applies them in the defined order (set, then add, then delete). The final state reflects all operations applied sequentially. For example, if a response sets "/message/subject" and also deletes "/message/subject", the subject will be deleted (delete operations execute last).

Implementations SHOULD NOT submit responses with conflicting operations targeting the same path, as the resulting behavior, while deterministic, may be confusing.

6.3.6. No Modification Response

If a scanner has no modifications to request, it MUST return either:

* An empty JSON/CBOR object: {}
* A response with empty or null modification arrays: {"set": null, "add": null, "delete": null}
* An HTTP 204 No Content response with no body

In all cases, the MTA proceeds with the action specified in the original request. The scanner chain continues to the next registered scanner unless the current action is terminal.

6.3.7. Size Limits

MTAs MAY impose limits on the size of modification values. If a modification would cause a header or message to exceed configured size limits, the MTA SHOULD reject that specific modification and log the failure.

6.3.8. Modification Errors

If a modification cannot be applied (for example, the path references a non-existent property for deletion, or the path is not in the permitted updateProperties list), the MTA SHOULD:

1. Log the error with sufficient detail for debugging

2. Increment modification failure statistics

3. Continue processing remaining modifications in the response

The MTA MUST NOT reject the entire response due to a single failed modification unless the failed modification is critical to interpreting the response (such as an invalid action value).

6.4. Example Hook Responses

6.4.1. Accept with Header Addition

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "add": [
    {
      "path": "/message/headers",
      "value": {"name": "X-Spam-Status", "value": "No"},
      "index": 0
    },
    {
      "path": "/message/headers",
      "value": {"name": "X-Spam-Score", "value": "1.2"},
      "index": 1
    }
  ]
}
```

6.4.2. Reject with Custom Response

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "set": [
    {
      "path": "/action",
      "value": "reject"
    },
    {
      "path": "/response",
      "value": {
        "code": 550,
        "enhancedCode": "5.7.1",
        "message": "Message rejected: virus detected"
      }
    }
  ]
}
```

6.4.3. Modify Subject and Add Recipient

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "set": [
    {
      "path": "/message/subject",
      "value": "[EXTERNAL] Original Subject"
    }
  ],
  "add": [
    {
      "path": "/envelope/to",
      "value": {
        "address": "compliance@example.com",
        "parameters": {}
      }
    }
  ]
}
```

6.4.4. Cancel Specific Recipient Delivery

For outbound processing, to cancel delivery for a specific recipient:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "set": [
    {
      "path": "/envelope/to/1/status",
      "value": "failed-silent"
    }
  ]
}
```

6.4.5. No Action Response

If a scanner has no changes to request, it returns an empty response body or a response with no action or modifications:

```
HTTP/1.1 200 OK
Content-Type: application/json

{}
```

The MTA proceeds with the default action specified in the request.

7. Transport

This section specifies HTTP transport requirements for MTA Hooks communications.

7.1. HTTP Version

Implementations MUST support HTTP/1.1 [RFC9112]. Implementations SHOULD support HTTP/2 [RFC9113] for improved performance through multiplexing. Implementations MAY support HTTP/3 [RFC9114].

When multiple HTTP versions are available, implementations SHOULD prefer newer versions for their performance benefits while maintaining fallback to HTTP/1.1.

7.2. TLS Requirements

All MTA Hooks communications MUST use TLS. Implementations MUST support TLS 1.2 [RFC5246] and SHOULD support TLS 1.3 [RFC8446].

Implementations MUST validate server certificates against trusted certificate authorities. Self-signed certificates SHOULD NOT be accepted in production deployments unless explicitly configured by administrators.

Cipher suite selection SHOULD follow current best practices. Implementations SHOULD disable cipher suites known to be weak or compromised.

7.3. Request Methods

The following HTTP methods are used:

* GET: Discovery document retrieval and status queries
* POST: Registration requests and hook invocations
* DELETE: Deregistration requests

7.4. Content Negotiation

For hook requests and responses, the Content-Type header MUST be set to "application/json" for JSON serialization or "application/cbor" for CBOR serialization.

The Accept header MAY be used during discovery to indicate preferred serialization format. If the scanner cannot provide the requested format, it SHOULD return the discovery document in JSON format.

7.5. Error Handling

7.5.1. HTTP Status Codes

MTAs SHOULD interpret HTTP status codes as follows:

* 2xx: Request successful. Process response body.
* 4xx: Client error. Do not retry; log error and proceed with default action.
* 5xx: Server error. May retry according to policy.

7.5.2. Timeout Handling

If a scanner does not respond within the configured timeout, the MTA SHOULD proceed with the default action. Timeout handling policy (fail-open vs. fail-closed) is implementation-defined and SHOULD be configurable.

7.5.3. Retry Policy

For transient errors (5xx status codes, network failures, timeouts), implementations SHOULD implement retry with exponential backoff. A recommended policy is:

* Maximum 3 retry attempts
* Initial delay: 100 milliseconds
* Backoff multiplier: 2
* Maximum delay: 5 seconds
* Add random jitter of 0-100 milliseconds

Implementations MAY provide configuration options to adjust retry parameters.

7.6. Connection Management

Implementations SHOULD use connection pooling to reduce latency for repeated requests to the same scanner endpoint. HTTP/2 multiplexing, where available, reduces the need for multiple connections.

Implementations SHOULD respect HTTP keep-alive semantics and connection limits advertised by scanners.

8. Implementation Considerations

8.1. MTA Considerations

8.1.1. Multiple Scanner Handling

When multiple scanners are registered for the same stage, the MTA invokes them sequentially in an implementation-defined order. Each scanner’s response affects the request seen by subsequent scanners.

Implementations SHOULD provide configuration options for:

* Scanner invocation order (priority-based or explicit ordering)
* Conflict resolution when scanners return conflicting actions
* Short-circuit behavior (whether to skip remaining scanners after certain actions)

8.1.2. Unavailable Scanners

When a scanner becomes unavailable (timeouts, errors, deregistration), the MTA must determine how to proceed. Common policies include:

* Fail-open: Proceed with default action as if scanner approved
* Fail-closed: Reject or defer message processing

The appropriate policy depends on deployment requirements. Security-focused deployments may prefer fail-closed, while availability-focused deployments may prefer fail-open. Implementations SHOULD make this policy configurable.

8.1.3. Performance Considerations

Synchronous hook invocation adds latency to mail processing. Implementations SHOULD consider:

* Connection pooling and keep-alive for scanner connections
* Parallel invocation of independent scanners where ordering is not required
* Timeout tuning based on scanner response time characteristics

8.2. Scanner Considerations

8.2.1. Idempotency

Scanners SHOULD design their processing to be idempotent. Network issues or MTA retries may result in duplicate invocations for the same message. Scanners SHOULD handle duplicate requests gracefully.

8.2.2. Response Time

Scanners operate in the critical path of mail delivery. Long response times delay message processing and may cause timeouts. Scanners SHOULD:

* Process requests promptly
* Implement internal timeouts shorter than MTA timeouts
* Consider asynchronous processing for expensive operations
* Return default responses when processing cannot complete in time

8.2.3. Stateless Design

Scanners SHOULD avoid relying on state from previous invocations. Each hook request contains complete context for processing decisions. Stateless design improves reliability and simplifies horizontal scaling.

8.3. Large Message Handling

Large messages present challenges for both MTAs and scanners. Implementations SHOULD consider:

* Message size limits advertised in discovery documents
* Truncation policies for oversized messages
* Memory management for large message bodies

Streaming or chunked delivery is not currently specified. For very large messages, implementations MAY arrange out-of-band content retrieval, though this is outside the scope of this specification.

8.4. High Availability

8.4.1. Scanner High Availability

For production deployments, scanners SHOULD be deployed with redundancy. Approaches include:

* Multiple scanner instances behind a load balancer
* Health checking with automatic failover
* Geographic distribution for disaster recovery

The MTA registers a single callback URL; load balancing occurs at the network layer.

8.4.2. Registration State

Registration state resides at the MTA. Scanner instances SHOULD NOT assume persistent local state. If scanner instances share a registration, they MUST coordinate to avoid conflicting operations (such as simultaneous deregistration).

9. Security Considerations

9.1. Authentication and Authorization

Authentication of registration requests is critical to prevent unauthorized scanners from receiving email content. Implementations MUST require authentication for registration operations.

Recommended authentication approaches:

* Bearer tokens: Simple to implement; tokens should be generated with sufficient entropy and rotated periodically.

* Mutual TLS: Provides strong authentication and binds identity to transport security.

* HMAC signatures: Allows authentication without transmitting secrets; requires secure key distribution.

Authorization policies SHOULD restrict which scanners may register and what capabilities they may request. Policies may be based on scanner identity, requested stages, or other criteria.

9.2. Transport Security

All MTA Hooks communications MUST use TLS to protect message content and authentication credentials in transit. Implementations MUST validate certificates to prevent man-in-the-middle attacks.

For internal network deployments, administrators may choose to use private certificate authorities. However, disabling certificate validation is NOT RECOMMENDED even for internal communications.

9.3. Message Confidentiality

Email messages frequently contain sensitive personal or business information. Scanners necessarily receive access to message content to perform their functions. Deployments SHOULD consider:

* Data handling policies for scanner operators

* Logging policies that avoid recording message content

* Data retention limits at scanner endpoints

* Regulatory requirements such as GDPR for personal data processing

9.4. Denial of Service

9.4.1. Registration Attacks

Attackers may attempt to exhaust MTA resources through excessive registration requests. Implementations SHOULD:

* Rate limit registration attempts per source
* Limit maximum concurrent registrations
* Require authentication before processing registrations
* Validate callback URLs before completing registration

9.4.2. Scanner Resource Exhaustion

Malicious or misconfigured MTAs could overwhelm scanners with requests. Scanners SHOULD:

* Implement rate limiting
* Set appropriate resource limits
* Monitor for unusual request patterns

9.4.3. Slow Scanner Attacks

Slow responses from scanners can exhaust MTA resources (connection limits, memory). MTAs SHOULD:

* Enforce strict timeouts
* Limit concurrent requests to any single scanner
* Implement circuit breaker patterns for repeatedly slow scanners

9.5. Injection Attacks

Scanner responses contain modifications applied to message processing. Implementations MUST validate all scanner-provided data:

* Header values MUST be validated to prevent header injection
* Recipient addresses MUST be validated against policy
* Body modifications MUST not introduce malformed content

9.6. Privacy Considerations

Email processing inherently involves access to personal communications. Implementations SHOULD minimize data exposure:

* Scanners SHOULD request only necessary properties
* MTAs SHOULD honor property restrictions from capability negotiation
* Logging SHOULD avoid recording message content or metadata
* Scanner operators SHOULD implement appropriate data protection measures

10. IANA Considerations

10.1. Well-Known URI Registration

This document registers the following well-known URI per [RFC8615]:

URI suffix: mta-hooks

Change controller: IETF

Specification document: This document

Status: permanent

Related information: N/A

10.2. MTA Hooks Serialization Format Registry

IANA is requested to create a new registry entitled "MTA Hooks Serialization Formats" with the following initial contents:

* Format: json
  - Description: JSON serialization per RFC 8259
  - Reference: This document
* Format: cbor
  - Description: CBOR serialization per RFC 8949
  - Reference: This document

New registrations require Specification Required per [RFC8126].

10.3. MTA Hooks Inbound Action Registry

IANA is requested to create a new registry entitled "MTA Hooks Inbound Actions" with the following initial contents:

* Action: accept
  - Description: Accept message for delivery
  - Reference: This document
* Action: reject
  - Description: Reject message with error response
  - Reference: This document
* Action: discard
  - Description: Accept but do not deliver message
  - Reference: This document
* Action: quarantine
  - Description: Place message in quarantine
  - Reference: This document
* Action: disconnect
  - Description: Terminate SMTP connection
  - Reference: This document

New registrations require Specification Required per [RFC8126].

10.4. MTA Hooks Outbound Action Registry

IANA is requested to create a new registry entitled "MTA Hooks Outbound Actions" with the following initial contents:

* Action: continue
  - Description: Proceed with normal delivery processing

- Reference: This document

* Action: cancel

- Description: Cancel pending deliveries

- Reference: This document

New registrations require Specification Required per [RFC8126].

10.5. MTA Hooks Inbound Stage Registry

IANA is requested to create a new registry entitled "MTA Hooks Inbound Stages" with the following initial contents:

* Stage: connect

- Description: Client connection established

- Reference: This document

* Stage: ehlo

- Description: EHLO/HELO command received

- Reference: This document

* Stage: mail

- Description: MAIL FROM command received

- Reference: This document

* Stage: rcpt

- Description: RCPT TO command received

- Reference: This document

* Stage: data

- Description: Message content received

- Reference: This document

New registrations require Specification Required per [RFC8126].

10.6. MTA Hooks Outbound Stage Registry

IANA is requested to create a new registry entitled "MTA Hooks Outbound Stages" with the following initial contents:

* Stage: delivery
  - Description: Delivery attempt completed
  - Reference: This document
* Stage: defer
  - Description: Delivery deferred for retry
  - Reference: This document
* Stage: dsn
  - Description: DSN generation pending
  - Reference: This document

New registrations require Specification Required per [RFC8126].

10.7. MTA Hooks Error Code Registry

IANA is requested to create a new registry entitled "MTA Hooks Error Codes" with the initial contents specified in Appendix A.

New registrations require Specification Required per [RFC8126].

11. References

11.1. 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>.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, <https://www.rfc-editor.org/rfc/rfc3339>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/rfc/rfc5246>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/rfc/rfc5321>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/rfc/rfc5322>.

[RFC6901] Bryan, P., Ed., Zyp, K., and M. Nottingham, Ed., "JavaScript Object Notation (JSON) Pointer", RFC 6901, DOI 10.17487/RFC6901, April 2013, <https://www.rfc-editor.org/rfc/rfc6901>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/rfc/rfc8126>.

[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>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/rfc/rfc8259>.

[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>.

[RFC8615] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019, <https://www.rfc-editor.org/rfc/rfc8615>.

[RFC8620] Jenkins, N. and C. Newman, "The JSON Meta Application Protocol (JMAP)", RFC 8620, DOI 10.17487/RFC8620, July 2019, <https://www.rfc-editor.org/rfc/rfc8620>.

[RFC8621] Jenkins, N. and C. Newman, "The JSON Meta Application Protocol (JMAP) for Mail", RFC 8621, DOI 10.17487/RFC8621, August 2019, <https://www.rfc-editor.org/rfc/rfc8621>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

[RFC9112] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP/1.1", STD 99, RFC 9112, DOI 10.17487/RFC9112, June 2022, <https://www.rfc-editor.org/rfc/rfc9112>.

[RFC9113] Thomson, M., Ed. and C. Benfield, Ed., "HTTP/2", RFC 9113, DOI 10.17487/RFC9113, June 2022, <https://www.rfc-editor.org/rfc/rfc9113>.

[RFC9114] Bishop, M., Ed., "HTTP/3", RFC 9114, DOI 10.17487/RFC9114, June 2022, <https://www.rfc-editor.org/rfc/rfc9114>.

11.2. Informative References

[RFC3461] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)", RFC 3461, DOI 10.17487/RFC3461, January 2003, <https://www.rfc-editor.org/rfc/rfc3461>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/rfc/rfc6376>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/rfc/rfc7208>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/rfc/rfc7489>.

Appendix A. Error Codes

This appendix defines error codes used in MTA Hooks error responses.

A.1. Error Response Structure

Error responses use the following structure:

```
{
  "error": {
    "code": "ERROR_CODE",
    "message": "Human-readable error description"
  }
}
```

A.2. HTTP 400 Bad Request

* INVALID_REQUEST: Malformed JSON/CBOR or missing required fields.
* INVALID_CALLBACK_URL: Callback URL is malformed or uses disallowed scheme.
* CAPABILITY_MISMATCH: Requested capability not supported by MTA.
* INVALID_STAGE: One or more requested stages are not valid.
* INVALID_ACTION: One or more requested actions are not valid.
* INVALID_MODIFICATION: One or more requested modifications are not valid.
* NO_STAGES_REQUESTED: Neither inbound nor outbound stages were specified.
* FILTER_INVALID: Filter configuration is syntactically invalid.

A.3. HTTP 401 Unauthorized

* AUTHENTICATION_REQUIRED: No authentication credentials provided.
* INVALID_CREDENTIALS: Provided credentials are invalid or expired.

A.4. HTTP 403 Forbidden

* REGISTRATION_DENIED: Valid credentials but not authorized to register.
* DOMAIN_NOT_ALLOWED: Scanner not authorized for requested domains.
* CALLBACK_NOT_ALLOWED: Callback URL not in allowlist.

A.5. HTTP 404 Not Found

* REGISTRATION_NOT_FOUND: No registration exists with the specified ID.

A.6. HTTP 409 Conflict

* ALREADY_REGISTERED: Scanner with same callback URL already registered.

* REGISTRATION_LIMIT_REACHED: Maximum number of registrations exceeded.

A.7. HTTP 422 Unprocessable Entity

* UNSUPPORTED_FILTER: The filter contains conditions that are not supported by this MTA.

* CALLBACK_UNREACHABLE: MTA could not reach callback URL for verification.

* CALLBACK_VERIFICATION_FAILED: Callback URL responded but verification failed.

* TLS_REQUIRED: Callback URL must use HTTPS.

* TLS_CERTIFICATE_INVALID: Callback URL TLS certificate is invalid or untrusted.

A.8. HTTP 429 Too Many Requests

* RATE_LIMITED: Too many registration attempts; retry after specified time.

A.9. HTTP 500 Internal Server Error

* INTERNAL_ERROR: Unexpected server error during processing.

A.10. HTTP 503 Service Unavailable

* REGISTRATION_DISABLED: Registration temporarily disabled by administrator.

Appendix B. Complete Example Flows

This appendix provides complete request and response examples for common scenarios.

B.1. Inbound Spam Filtering

This example shows a complete flow for spam filtering during inbound message reception.

B.1.1. Discovery

```
GET /.well-known/mta-hooks HTTP/1.1
Host: scanner.example.com
Accept: application/json
```

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "version": "1.0",
  "endpoints": {
    "registration": "/v1/hooks/register",
    "deregistration": "/v1/hooks/register/{registration_id}"
  },
  "serialization": ["json"],
  "capabilities": {
    "inbound": {
      "stages": ["data"],
      "actions": ["accept", "reject", "quarantine"],
      "fetchProperties": ["/message", "/envelope", "/senderAuth",
                          "/client"],
      "updateProperties": ["/message/headers", "/action", "/response"]
    }
  },
  "limits": {
    "maxMessageSize": 26214400,
    "timeoutMs": 30000
  }
}
```

B.1.2. Registration

```
POST /v1/hooks/register HTTP/1.1
Host: scanner.example.com
Content-Type: application/json
Authorization: Bearer sk_live_abc123

{
  "name": "SpamFilter Pro",
  "version": "3.0.1",
  "callback": {
    "url": "https://filter.example.net/hooks/spam",
    "timeoutMs": 20000
  },
  "serialization": "json",
  "inbound": {
    "stages": ["data"],
    "properties": ["/message", "/envelope", "/senderAuth", "/client"]
  },
  "metadata": {
    "customer": "acme-corp"
  }
}
```

B.1.3. Verification Callback

```
POST /hooks/spam HTTP/1.1
Host: filter.example.net
Content-Type: application/json

{
  "action": "verify",
  "token": "vrf_xyz789"
}

HTTP/1.1 200 OK
Content-Type: application/json

{
  "token": "vrf_xyz789"
}
```

B.1.4. Registration Response

```
HTTP/1.1 201 Created
Content-Type: application/json
Location: /v1/hooks/register/reg_spam_001

{
  "registrationId": "reg_spam_001",
  "status": "active",
  "createdAt": "2024-12-21T10:00:00Z",
  "expiresAt": "2025-01-21T10:00:00Z",
  "callback": {
    "url": "https://filter.example.net/hooks/spam",
    "timeoutMs": 20000
  },
  "negotiated": {
    "serialization": "json",
    "inbound": {
      "stages": ["data"],
      "properties": ["/message", "/envelope", "/senderAuth", "/client"]
    }
  },
  "endpoints": {
    "deregistration": "/v1/hooks/register/reg_spam_001",
    "status": "/v1/hooks/register/reg_spam_001/status"
  }
}
```

B.1.5. Hook Invocation - Clean Message

```
POST /hooks/spam HTTP/1.1
Host: filter.example.net
Content-Type: application/json
X-MTA-Hooks-Registration: reg_spam_001

{
  "stage": "data",
  "action": "accept",
  "timestamp": "2024-12-21T10:30:00Z",
  "response": {
    "code": 250,
    "enhancedCode": "2.0.0",
    "message": "OK"
  },
  "envelope": {
    "from": {"address": "alice@sender.example", "parameters": {}},
    "to": [{"address": "bob@recipient.example", "parameters": {}}]
  },
  "message": {
    "subject": "Quarterly Report",
    "from": [{"email": "alice@sender.example", "name": "Alice Smith"}],
    "to": [{"email": "bob@recipient.example"}],
    "size": 15360,
    "bodyValues": {
      "1": {
        "value": "Please find attached the Q4 report...",
        "isEncodingProblem": false,
        "isTruncated": false
      }
    }
  },
  "senderAuth": {
    "spf-mail": "pass",
    "dkim": "pass",
    "dmarc": "pass"
  },
  "client": {
    "ip": "192.0.2.50",
    "ehlo": "mail.sender.example"
  }
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "add": [
    {
      "path": "/message/headers",
      "value": {"name": "X-Spam-Status", "value": "No, score=0.5"},
      "index": 0
    }
  ]
}
```

B.1.6. Hook Invocation - Spam Detected

```
POST /hooks/spam HTTP/1.1
Host: filter.example.net
Content-Type: application/json
X-MTA-Hooks-Registration: reg_spam_001

{
  "stage": "data",
  "action": "accept",
  "timestamp": "2024-12-21T10:35:00Z",
  "response": {
    "code": 250,
    "enhancedCode": "2.0.0",
    "message": "OK"
  },
  "envelope": {
    "from": {"address": "promo@spammer.invalid", "parameters": {}},
    "to": [{"address": "bob@recipient.example", "parameters": {}}]
  },
  "message": {
    "subject": "YOU HAVE WON $1,000,000!!!",
    "from": [{"email": "winner@lottery.invalid"}],
    "to": [{"email": "bob@recipient.example"}],
    "size": 8192
  },
  "senderAuth": {
    "spf-mail": "fail",
    "dkim": "none",
    "dmarc": "fail"
  },
  "client": {
    "ip": "203.0.113.99",
    "ehlo": "totally-legit.invalid"
  }
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "set": [
    {
      "path": "/action",
      "value": "reject"
    },
    {
      "path": "/response",
      "value": {
        "code": 550,
        "enhancedCode": "5.7.1",
        "message": "Message rejected due to spam content"
      }
    }
  ]
}
```

B.2. Outbound Delivery Logging

This example shows outbound hook usage for delivery status logging and compliance.

B.2.1. Registration

```
POST /v1/hooks/register HTTP/1.1
Host: mta.example.com
Content-Type: application/json
Authorization: Bearer sk_live_def456

{
  "name": "Delivery Logger",
  "version": "1.0.0",
  "callback": {
    "url": "https://logger.example.net/hooks/delivery",
    "timeoutMs": 5000
  },
  "serialization": "json",
  "outbound": {
    "stages": ["delivery", "dsn"],
    "actions": ["continue"],
    "properties": null
  }
}
```

```
HTTP/1.1 201 Created
Content-Type: application/json

{
  "registrationId": "reg_logger_001",
  "status": "active",
  "createdAt": "2024-12-21T11:00:00Z",
  "negotiated": {
    "serialization": "json",
    "outbound": {
      "stages": ["delivery", "dsn"],
      "actions": ["continue"],
      "properties": ["/envelope", "/message", "/queue", "/context"]
    }
  },
  "endpoints": {
    "deregistration": "/v1/hooks/register/reg_logger_001",
    "status": "/v1/hooks/register/reg_logger_001/status"
  }
}
```

B.2.2. Hook Invocation - Partial Delivery

```
POST /hooks/delivery HTTP/1.1
Host: logger.example.net
Content-Type: application/json
X-MTA-Hooks-Registration: reg_logger_001

{
  "stage": "delivery",
  "action": "continue",
  "timestamp": "2024-12-21T12:00:00Z",
  "queue": {
    "id": "q_msg_12345",
    "expiresAt": "2024-12-24T12:00:00Z",
    "attempts": 1
  },
  "envelope": {
    "from": {"address": "notify@example.com", "parameters": {}},
    "to": [
      {
        "address": "user1@active.example",
        "parameters": {},
        "status": "delivered",
        "attempt": 1,
        "lastResponse": {
          "code": 250,
          "enhancedCode": "2.0.0",
```

```
            "message": "Delivered"
          }
        },
        {
          "address": "user2@slow.example",
          "parameters": {},
          "status": "deferred",
          "attempt": 1,
          "lastResponse": {
            "code": 451,
            "enhancedCode": "4.7.1",
            "message": "Greylisted, try again"
          },
          "nextAttemptAt": "2024-12-21T12:15:00Z"
        },
        {
          "address": "user3@invalid.example",
          "parameters": {},
          "status": "failed",
          "attempt": 1,
          "lastResponse": {
            "code": 550,
            "enhancedCode": "5.1.1",
            "message": "User unknown"
          }
        }
      ]
    },
    "message": {
      "subject": "System Notification",
      "messageId": "<notify-12345@example.com>",
      "size": 2048
    }
  }

  HTTP/1.1 200 OK
  Content-Type: application/json

  {
    "action": "continue"
  }
```

B.3. Deregistration

```
  DELETE /v1/hooks/register/reg_spam_001 HTTP/1.1
  Host: scanner.example.com
  Authorization: Bearer sk_live_abc123
```

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "registrationId": "reg_spam_001",
  "status": "deregistered",
  "deregisteredAt": "2024-12-21T18:00:00Z"
}
```

Appendix C. Acknowledgments

The authors thank the developers and operators of existing mail filtering systems whose experience informed this design.

Appendix D. Changes

[[This section to be removed by RFC Editor]]

draft-degennaro-mta-hooks-00

* Initial version

Author’s Address

Mauro De Gennaro
Stalwart Labs LLC
1309 Coffeen Avenue, Suite 1200
Sheridan, WY 82801
United States of America
Email: mauro@stalw.art
URI: https://stalw.art