Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 31, 2026

R. Haddad
Inventor

November 27, 2025

Mail Pre-Flight Template Discovery Protocol (MPTDP)
draft-haddad-mptdp-00

Abstract

This document specifies the Mail Pre-Flight Template Discovery Protocol (MPTDP). This mechanism allows a Mail User Agent (MUA) to proactively discover and retrieve a structured message template based on the recipient's public email address, prior to message composition. It utilizes a well-known URI structure and provides a security manifest to prevent address enumeration.

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 May 31, 2026.

1. Introduction

Current email composition relies heavily on unstructured text or reactive mechanisms (auto-responders). There is no standard way for a recipient domain to dictate the structure of an incoming message before the sender begins typing. This leads to incomplete correspondence, operational inefficiencies, and poor user experience.

MPTDP solves this by introducing a "Pre-Flight" check via HTTP, leveraging the existing web infrastructure of the recipient domain.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described

in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Protocol Overview

The protocol operates in a sequence triggered by the MUA upon entry of a valid email address string.

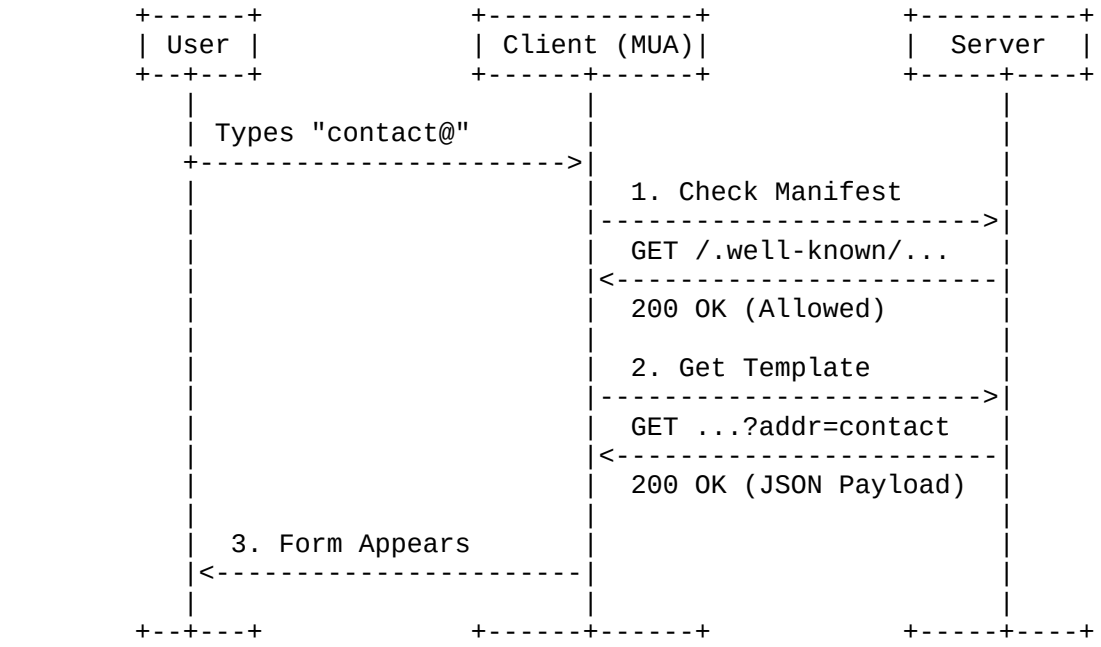

Figure 1: MPTDP Communication Sequence

4. Discovery Mechanism

4.1. The Manifest (Security Layer)

To prevent email enumeration (privacy attacks), a domain MUST publish a manifest listing authorized public endpoints.

- URI: https://{domain}/.well-known/mptdp-manifest.json
- Format: JSON

Example:

```
{
  "version": "1.0",
  "public_endpoints": ["support", "sales", "jobs"],
  "wildcard": false
}
```

The MUA MUST NOT issue a specific template request for an address local-part not listed in this manifest.

4.2. Template Retrieval

If authorized by the manifest, the MUA issues the retrieval request.

- URI: https://{domain}/.well-known/mptdp
- Method: GET
- Parameters:
  - address (REQUIRED): The local-part of the email.
  - lang (OPTIONAL): ISO 639-1 language code.

5. Response Format

The server responds with a JSON object defining the message structure.

Example Payload:

```
{
  "status": "success",
  "content": {
    "subject_template": "Claim [REF] - Assistance",
    "body_structure": [
      { "type": "text", "value": "Hello Support," },
      { "type": "input", "label": "Contract ID", "required": true }
    ]
  },
  "security": {
    "signature": "sha256:7f83b165..."
  }
}
```

6. Security Considerations

6.1. Privacy

The Manifest mechanism (Section 4.1) is critical. Implementers MUST ensure that private addresses (e.g., individual employees) are not exposed via this protocol unless explicitly intended.

6.2. Phishing and Integrity

MUAs SHOULD verify the "security.signature" field against the domain’s public keys (DKIM or specific DNS TXT record) to ensure the template has not been tampered with during transit. HTTPS is MANDATORY.

7. IANA Considerations

This document requests the registration of the URI suffix "mptdp" in the "Well-Known URIs" registry as defined by RFC 8615.

8. References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017.

[RFC8615] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, May 2019.

Author’s Address

Rachid Haddad
Email: haddad.rachid2006@gmail.com