Making the Internet work better

Email Processing Services

A Request for Proposals issued on 2023-07-18

IETF Executive Director
exec-director@ietf.org

About the IETF

The Internet Engineering Task Force (IETF) is the premiere Internet standards body creating open protocols to ensure that the global Internet is built on the highest-quality technical standards. These standards, shaped by rough consensus and informed by running code, are developed by a large volunteer community of leading engineering and technical experts from around the world. IETF processes are open and transparent, and IETF standards are freely available to anyone.

Standards and protocols developed at the IETF provide a core framework for today's online world. Everything from video conferencing, to email, to cloud storage is built on standards developed in the IETF community. In short, our work makes the Internet work.

Overview

Email processing is critical to the operation of the IETF as most of the work of the IETF takes place on mailing lists due to the globally distributed nature of IETF participants. There are multiple software components, both custom and off-the-shelf, in a complex mail processing chain.

This RFP is for a service provider with expert knowledge of mail processing, to migrate our current mail processing systems to new cloud infrastructure and manage these services with an extremely high level of reliability.

Timeline

18 July 2023	RFP Issued
8 August 2023	Questions and Inquiries deadline
15 August 2023	Answers to questions issued and RFP updated if required
5 September 2023	**Bids due**
19 September 2023	Preferred bidder selected and negotiations begin
6 October 2023	Contract execution and work begins

RFP Process

The process for the RFP is as follows:

1. The RFP is publicly issued, posted to our website[1] and announced to the RFP Announcement mailing list[2], which anyone can subscribe to.

2. Potential bidders have until 8 August 2023 to submit any questions by email to ietf-rfps@ietf.org. Questions will be treated as anonymous but not private, as explained below. If you do not receive confirmation that your questions have been received within 24 hours then resend until you do.

3. A written response to all questions is provided on or before 15 August 2023, direct to those parties that sent questions, by email to the RFP Announcement Mailing List and posted on our website[3]. The response will include the questions asked and the answers, but will not identify the

[1] https://www.ietf.org/about/administration/rfps-and-contracts/
[2] https://www.ietf.org/mailman/listinfo/rfp-announce
[3] https://www.ietf.org/about/administration/rfps-and-contracts/

company asking the question. If required, the RFP may be updated to correct or clarify any issues identified.

4. Bids are due by **5 September 2023** by email to ietf-rfps@ietf.org. If you do not receive confirmation that your bid has been received within 24 hours then please resend until you do. The bid should include the following information:

    a. Executive summary

    b. Standard approach to infrastructure management and infrastructure project management including any assumptions.

    c. Proposed new mail processing architecture and service components..

    d. Project plan and schedule for all the deliverables that must include when the work will begin and end, and any other milestones, as well as any dependencies that may delay delivery.

    e. Statement confirming that you can deliver the deliverables and meet all the listed requirements, along with any additional information needed to substantiate this.

    f. Key personnel experience and projected availability for the expected lifetime of the contract.

    g. Fee and payment schedule. Fixed priced bids are preferred but if that is not possible then a maximum fee must be specified.

    h. A warranty including a proposal for fee reduction or refund due to late- or non-delivery.

5. The IETF Administration LLC and designated contractors and volunteers will select a preferred bid and notify the bidder by 19 September 2023. The selection process may include questions by email and/or conference call.

6. The IETF Administration LLC then enters into contract negotiation with the preferred bidder, based on its standard contract and using the relevant sections of the Statement of Work below. If contract negotiation fails then a different preferred bidder may be chosen.

    a. For contracts of this nature, the standard proposed terms are an initial term of two years followed by two renewals by mutual agreement, each for a further two years, giving a possible total of six years.

7. Contract negotiation is anticipated to complete by 6 October 2023 and result in the award of the contract. All RFP contract awards are posted on our website and announced to the RFP Announcement mailing list. The terms of

the contract are later posted publicly on our website, with the fee information and signatures (where possible) redacted. In addition any Conflict of Interest declarations required of the preferred bidder are also posted publicly on our website. This transparency is non-negotiable.

8. Work generally begins immediately after award of the contract, unless specified otherwise in the Statement of Work or negotiated contract.

Jay Daley
IETF Executive Director
IETF Administration LLC

Statement of Work: Email Processing Services

Deliverables

The service provider will be contracted to deliver the following:

Part 1 - Pre-transition planning

The service provider must deliver the following within six weeks of the start of the contract:

1. A full architecture for the new mail processing services, agreed with the IETF, including:
    - Details of each component and how that will be operate including:
        - Where it will be deployed
        - What product/application will be used
        - How it will be managed and maintained
    - Details of how the architecture will ensure service availability and data integrity in the event of a range of failures.
2. A detailed plan for the upgrade of Mailman from v2 to v3. The plan must include:
    - Timetable
    - Tasks and schedule for IETF developers to upgrade integrations
    - Downtime requirements
    - Process for engaging with the existing service provider(s) and resolving any issues during the upgrade.
    - Test plan
    - Risk analysis with mitigation for key risks
3. A detailed plan for transition, agreed with the IETF. The plan must include:
    - Timetable for the transition
    - Individual technical transition plan for each service
    - Downtime requirements for each service
    - Process for engaging with the existing service provider(s) and resolving any issues during the transition.
    - Test plan for assuring a successful transition
    - Risk analysis with mitigations for key risks
4. Full cost estimate, including:
    - Service provider fees for the transition, unless already agreed on a fixed price basis.

- Any third party costs for infrastructure provision

Part 2 - Upgrade of Mailman

The service provider must complete a successful upgrade in line with the plan by 22 December 2023 (subject to the IETF being able to carry out its agreed tasks) including:

1. Successful upgrade
2. Timetable met
3. Agreed downtime not exceeded
4. All tests pass

Part 3 - Transition of existing services

The service provider must complete a successful transition in line with the architecture, transition plan and cost estimates, by 31 March 2024, including:

1. All services successfully transitioned
2. Timetable met
3. Agreed downtime not exceeded
4. All tests pass

Part 4 - Managed infrastructure

From the time the first service transitions, the service provider must deliver a managed Email Processing Services that meets the requirements, on an ongoing basis.

Requirements

Part 1 - Service provider requirements

Nature of service

The IETF requires a service provider with key personnel identified to work with the IETF who have extensive experience of managing mail processing.

This extensive experience must include at least the following: Internet Message Format (RFC 5322[4]), MIME and MIME extensions, SMTP, POP, IMAP and IMAP

[4] https://www.rfc-editor.org/rfc/rfc5322.html

extensions, SPF, DKIM and DMARC. Knowledge of ARC (RFC 8617[5]) and JMAP (RFC 8620[6]) would be an advantage.

The Service Provider is also required to have a good working knowledge of email reputation organizations and their methods, RBL providers and anti-spam solutions.

Scope of responsibility

Service provider will be responsible for the Email Processing Services and the delivery of the goals, including:

1. Email processing components as detailed in this RFP.
2. Management and operation of these components, including:
    a. Resource allocation
    b. Configuration and upgrades
    c. Change control
    d. Instrumentation
3. Management of any third party services, including
    a. All of 2 above
    b. Billing
4. Outcomes for the Email Processing Services, including:
    a. Availability
    b. Performance
    c. Security
    d. Visibility (i.e. of data collected by instrumentation)
    e. Value for money

Behaviors

IETF requires the service provider to actively practice the following behaviors:

- Open and communicative, particularly in pre-emptive communications
- Flexible attitude, particularly when it comes to the lines of responsibility when needed
- Always looking for ways to improve the services
- Aware of and continually aiming to adopt and further industry best practices, particularly automation

[5] https://www.rfc-editor.org/rfc/rfc8617.html
[6] https://www.rfc-editor.org/rfc/rfc8620.html

Part 2 - Goals and associated requirements

Email Processing Services must be operated to meet the following goals and associated requirements, each of which is described in more depth in the sections below. It is recognised that some of these goals overlap or are interdependent.

1. **Fit-for-purpose service availability**
2. **Fit-for-purpose service performance**
3. **Automated, transparent and accessible infrastructure management**
4. **Secure and enduring services and data**
5. **Comprehensive service monitoring**

Fit-for-purpose service availability

The IETF requires its Email Processing Services to support a fit-for-purpose service availability, which means:

- Minimal unplanned downtime.
- Designed to eliminate planned downtime (i.e. eliminating planned downtime required for routine upgrades).
- Planned downtime only needed for
    - Application deployment where required by the applications, recognising that the IETF aims to re-architect its own applications to remove this need
    - Transition of services
    - Major projects
- Where planned downtime is required, then:
    - It must not be during or during the preparation phase of IETF meetings or other key events..
    - Should be able to be scheduled for any day of the week at any time, to meet IETF operational requirements.

Fit-for-purpose service performance

The IETF requires its Email Processing Services to provide a fit-for-purpose service performance, which means:

- Excellent performance.
- All relevant and potentially relevant performance/utilization data collected.
- An architecture that scales to match load, particularly during key events, with minimal manual intervention.
- An architecture designed to support the global nature of the IETF and ensures excellent performance to all end users.
- An evidence based approach used in setting all resource limits.

- A strategy for rapidly addressing performance bottlenecks.

Automated, transparent and accessible infrastructure management

The IETF requires the management of its Email Processing Services to be automated, transparent and accessible, which means:

- All build and configuration managed through an automated configuration management and deployment platform (e.g. Ansible).
- Automation scripts in a public GitHub repository.
- Credentials and other secret information used in automation scripts / deployments to be properly protected in our HashiCorp Vault instance.
- A full test environment with the expectation that wherever possible, deployment involves first deploying to test, validating efficacy of changes, and then deploy to production.
- Where reasonable, it should be possible for any member of the IETF community to build a replica of any IETF service, with placeholder information available to replace any confidential information.

Secure and enduring services and data

The IETF requires its services and data to be secure and enduring, which means:

- An embedded risk-aware culture, with regular peer review and external audit of all strategies, processes and systems.
- Security-first network/service design and network/service management.
- A formal access control model with centralized observability.
- Clear compartmentalisation of confidential information.
- A patch management process that minimizes the threat from unpatched systems.
- A backup and restore strategy that provides strong assurance of data integrity and high confidence of system rebuild.
- Active management of nuisance traffic.

Comprehensive service monitoring

The IETF requires comprehensive, standards-based service monitoring, which means:

- Every part of the Email Processing Services is instrumented.
- Centralized collection of monitoring data to enable cross-service analysis.
- Controlled publication of monitoring data that maintains operational security while providing maximum access to the IETF community.

- Where possible, standards based data collection and distribution, and where proprietary APIs need to be used then these must be open and documented APIs.

Part 3 - Detailed operational requirements

Service hosting

The service provider can propose any of the following service hosting options for each component of the Email Processing Services:

- Use a SaaS offering
- Operate the component on the IETF cloud infrastructure
- Operate the component on third party cloud infrastructure.

The new IETF cloud infrastructure is the subject of a separate RFP. The service provider will need to coordinate the service provider for that infrastructure.

If the service provider proposes third-party cloud infrastructure, then it must meet the following requirements:

- At least two regions in the continental US, one to be the primary region for the Email Processing Services and one the secondary. Additionally, at least one region in Europe and one in Asia for possible future expansion.
- Open and transparent pricing model enabling high quality cost estimates to be made.
- Proven track record of stability and reliability.
- Full range of features necessary to meet IETF requirements.
- Support for orchestration (preferably Kubernetes), including automated deployment, scaling and management, except where the application itself cannot support this.

All services proposed to operate on a cloud infrastructure are subject to the following requirements:

- All services to be containerised (and managed via orchestration) so that they are entirely separated at the filesystem/package level and any one can have any supporting package upgraded without any other service being affected.
- Any service can be customized, upgraded and migrated to another platform / cloud provider with either no dependency or only entirely unavoidable dependency, on any other service or component of any other service. (no vendor lock-in when possible)
- As appropriate, all services to support operation behind Cloudflare Web Application Firewalls, Content Delivery Networks and other front end services.

Covered services and components

The service provider will be responsible for the operation and management of the following mail processing services:

- IETF mailing lists. The IETF operates hundreds of mailing lists, across multiple domain names, with a wide set of configurations and list owners, including public and private lists. The total number of subscribers across all lists exceeds 50,000[7] and the number of messages per month is approximately 10,000[8]. Some of the management of Mailman is automated by use of APIs and this is expected to grow significantly.
- Email integration. The IETF has a number of apps, both internally developed and third-party, that send mail through the IETF mail infrastructure.
- Direct mail. The IETF maintains an extensive and highly dynamic set of aliases for third party mailboxes to which it forwards mail. In addition there are a number of subdomains of ietf.org that have separate mail infrastructures (not covered in this RFP) which it regularly exchanges mail with, including through aliases.
- Mail stores. Transparency and access to historical information are critical to the IETF standards process and so makes mail publicly available in a number of ways - web archive, direct IMAP, and by pulling files from a filesystem.

The components that currently deliver these services, and which the service provider will be responsible for, are as follows:

- Off-the-shelf components.
    - Postfix. A standard MTA.
    - Mailman. Used for mailing lists.
    - ISODE IMAP. A commercial IMAP server, for which the IETF receives a donated license.
    - Amavis. Used for spam control.
- Internally developed components. The service provider will be responsible for the management of these components but not the software development, which will continue to be the responsibility of the IETF.
    - Postconfirm[9]. An internally developed and maintained application that provides a number of key features:
        - Challenge/response for first time posters to an IETF mailing list
        - DMARC rewriting on inbound and outbound messages
        - Maintenance of a global list of allowed posters to mailing lists.

[7] https://mailarchive.ietf.org/arch/reports/subscribers/
[8] https://mailarchive.ietf.org/arch/reports/messages/
[9] https://github.com/ietf-tools/postconfirm

    - Mailarchive[10] [11]. An internally developed open-source mail archiving tool that acts as a drop-in replacement for the standard Mailman archiving tool.

For each of these components, the service provider is free to propose an alternative to that currently in use, with the following additional requirements if this is the case:

- Any proposed alternatives must deliver all the currently used functionality.
- If the proposal is to replace a component, including internally developed components, with an alternative that requires developer resources, then the service provider will be solely responsible for sourcing those.

If the service provider proposes to continue with any of the existing internally developed components, then:

- The IETF will continue to develop and maintain these components and to assist/manage new deployment.
- The IETF will provide support to the service provider for these components.

Mailman upgrade and ongoing maintenance

The IETF currently uses Mailman v2 and the service provider is required to upgrade this to v3 as set out in the deliverables. Mailman is currently integrated into Postconfirm, Mailarchive and Datatracker (see below) using both APIs and command line invocations. The IETF will be responsible for upgrading these integrations as part of the upgrade to v3.

After the upgrade, the service provider is required to manage the Mailman service even if it has not yet transitioned to the new infrastructure.

Email standards

The IETF is the standards development organization where email standards originate. The IETF will be an early adopter of new email standards and/or experimental features and the Service Provider will be required to fully support this.

Nuisance traffic

As noted above, the service provider is required to actively manage nuisance traffic, which is expected to include blocking of individual addresses, domains, IP addresses and possibly more. All such blocking must be:

- Coordinated with the IETF and the operator of the IETF infrastructure, if any services run on that.

[10] https://github.com/ietf-tools/mailarch
[11] https://mailarchive.ietf.org/arch/

- In compliance with the policy set by the IETF Community on blocking.

Incident resolution

Service provider will be responsible for the resolution of all incidents that originate in the Email Processing Services, unless the service provider can demonstrate it is the fault of an IETF developed component that it cannot work around, or the fault of the IETF infrastructure if that is what the service is running on. For all other incidents, service provider responsibility is to support the IETF, as needed, for the IETF to resolve the incident.

Service provider incident resolution must meet the timescales set out below:

	Condition	**Resolution**
1	Service(s) is unusable[2], during an IETF meeting. (From morning of Saturday the meeting starts until afternoon of the following Friday, all in local meeting timezone).	Full service restoration within 30 minutes.
2	Service(s) is unusable[2], in the week before the IETF meeting. (From Monday morning ET timezone until the meeting starts).	Resolution within 2 hours, with extension of an additional 1 hour for exceptional circumstances.[3]
3	Service(s) is unusable[2], any time except during the periods in 1 and 2 above.	Resolution within 4 hours, with extension of an additional 4 hours in exceptional circumstances.[3]
4	Service(s) is usable but operating incorrectly, any time except during the periods in 1 and 2 above.	Triage within 12 hours. Resolution within 24 hours, with extension of an additional 24 hours in exceptional circumstances.[3]
5	Individual[4] mail processing issue.	Triage within 12 hours. Resolution within 48 hours, with extension of an additional 48 hours in exceptional circumstances.

NOTES:

[1] Services in this category will have been subject to a change freeze, except for emergency fixes, for at least one week before the meeting.

[2] Unusable means that the service is unavailable, or its performance is unacceptable, or it is operating incorrectly with the risk of data corruption or the risk of any other serious problem.

[3] Service provider is free to make this determination on a case-by-case basis. All such determinations to be recorded and discussed with IETF at scheduled review meetings.

[4] Explained further in the Troubleshooting section below.

Troubleshooting

Service Provider is required to troubleshoot individual issues with mail processing as requested by the IETF, where individual means that a specific group of users are affected, which may be small (e.g. one individual running their own MTA) or large (e.g. all Gmail users). These include, but are not limited to: lost, undeliverable or misdirected mail; problems accessing mail stores; issues with blocking, reputation scores, RBL listings.

Managing reputation

Service Provider is required to monitor important email reputation services and RBL providers and proactively mitigate any issues with the IETF reputation that adversely affect email delivery.

Cost management

It is expected (though not a requirement) that the IETF will be directly recharged by the Service Provider for the cost of any third-party cloud services. The IETF needs to keep these costs within budget and so requires the Service provider to:

- Provide reasonably accurate cost estimates on a quarterly basis
- Continually monitor incurred costs and alert the IETF of any significant deviations from previously supplied estimates.
- Aim to keep third-party costs within the agreed budget limits

As the Service Provider is required to continuously monitor the performance of the Email Processing Services and rapidly adjust resources as necessary to maintain an acceptable level of performance, it is recognised that this may lead to costs exceeding budget and that the priority may be for these adjustments to be made without prior estimation of the impact on costs.

Community engagement

The IETF is a community-led organization and regular communication with the community is key to the success of this contract. Service provider will be required to engage with the community as follows:

- Participate in regular community calls.
- Monitor key community mailing lists and respond as required.
- Monitor and respond to issues or PRs raised against GitHub repositories that service provider manages.

Part 4 - Transition specific

Current installations and separation of services

All Email Processing Services currently run on server IETFA, with a warm backup maintained via database replication and rsync at IETFC. Each server has 32 logical CPUs and 128Gb of RAM. The OS for each instance is OpenSuse, installed in a virtual server using Xenserver.

Applications on these servers are installed directly by the current service provider using a custom directory plan to provide some degree of application separation. A few applications are installed in Docker containers.

The IETF requires each application to be transitioned to its own containerised environment in order to achieve the goals outlined above.

Additional Details

The following sections are provided for information only and are not requirements or any form of commitment by the IETF. They are not intended to form part of any contract.

Datatracker

The IETF has developed a public facing document and workflow management tool called Datatracker[12] which is used extensively to track and progress IETF work. This is developed in Python on Django and is the main database powered application in use. The source code is open source, and available in a public GitHub repository[13].

[12] https://datatracker.ietf.org/
[13] https://github.com/ietf-tools/datatracker

Demand for services

The IETF is a global community with an uneven geographic spread, and the community uses the Email Processing Services 24x7x365. During IETF meetings, both the triannual plenaries and the many interim meetings, demand on services is high and uninterrupted availability is expected. At other times, the activities are not so time critical that they cannot tolerate a delay of a few hours if planned and sufficient warning is given.

Also, mail storage services are intended for users to pull large amounts of data (1-10 GB) in order to maintain local copies of large datasets.

Community participation in the development and operation of IT services

The IETF is a community-led organization and there are several mechanisms for the community to participate in the development and operation of IETF IT services. These may change over time:

- Monthly open Tools Team call of 1-1.5 hours.
- Participation on the Tools-discuss[14] mailing list. This is a low volume mailing list with occasional spurts of high volume. However, it should be noted that the community may raise relevant matters on other lists, including the general IETF list and the admin-discuss list.
- Formal consultations with the community on aspects of our IT strategy. These are rare, possibly twice a year, lasting for a few weeks, with community feedback provided by email.
- Occasional workshops or special meetings to discuss specific issues or plans.
- Contributing via public GitHub repositories. All IETF software is open source and available this way.

Developers and developer support

The IETF has a core set of staff developers and long-term development contractors (fewer than 10 in total) who write the bulk of our software. Our infrastructure includes a substantial set of development/testing environments and automated build chains.

There is also a strong set of community developers, some of whom develop adjacent tools for community use and some of whom contribute code to IETF tools. These developers are active throughout the year and particularly at ‘codesprint’ sessions, held at each IETF meeting, where 10+ community developers meet and work on the IETF applications for a day.

[14] https://www.ietf.org/mailman/listinfo/Tools-discuss

The IETF supports these community developers with pre-built development environments for them to run locally, and live integrations to development instances running on IETF infrastructure.

IETF Meetings and the IETF Network

The IETF meets three times a year on a global rotation. Each meeting will have 1000+ onsite participants and 400+ remote participants. These meetings are crucial to the operation of the IETF and therefore the expectation for IETF IT systems is that they are highly available both during the meetings and in the preparatory periods.

The IETF provides its own network in the IETF Meeting venues, which is installed and managed by the NOC team, a combination of contractors and volunteers. This network, its equipment and its management are out of scope for this contract.

The IETF utilizes a highly specialized remote participation tool during its meetings, with an onsite team managing this throughout the meeting. This operates on AWS under the management of the remote participation tool provider. This tool requires Datatracker to be functioning as its authentication provider.

The IETF uses a third party registration system for its meetings, which is integrated with both Datatracker and Salesforce.

Additionally, the IETF hosts interim meetings of individual Working Groups, using one of a number of remote participation options. The IETF generally avoids scheduling any application downtime or major upgrades near the time of an interim meeting.

Specialist providers

The IETF is supported by a number of specialist providers in the following areas: UI/UX research and design, Database management, Security auditing.

Threat model

The IETF is vulnerable to the same threats as any other organization and needs to mitigate those at many levels. The threat model for the IETF is unusual with more of an emphasis on data integrity and preserving the accuracy and availability of historical data, than on protecting confidential information. Where the IETF does collect highly confidential information, such as for the NomCom process, every effort is made to compartmentalize that. Additionally, the IETF receives significant nuisance traffic (as a proportion of overall traffic).

ENDS