EMAILCORE
Internet-Draft
Intended status: Standards Track
Expires: 12 March 2026

J.C. Klensin, Ed.

K. Murchison, Ed.
Fastmail

8 September 2025

Applicability Statement for IETF Core Email Protocols
draft-ietf-emailcore-as-23

Abstract

Electronic mail is one of the oldest Internet applications that is still in very active use. While the basic protocols and formats for mail transport and message formats have evolved slowly over the years, events and thinking in more recent years have supplemented those core protocols with additional features and suggestions for their use. This Applicability Statement describes the relationship among many of those protocols and provides guidance and makes recommendations for the use of features of the core protocols.

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 12 March 2026.

Copyright Notice

Table of Contents

1. Introduction

This document is an Applicability Statement [RFC2026], Section 3.2 that provides guidance in the use of the Internet's core email specifications, the Simple Mail Transfer Protocol (SMTP) [I-D.ietf-emailcore-rfc5321bis] and the Internet Message Format (IMF) [I-D.ietf-emailcore-rfc5322bis], and some extensions and other protocols that have been built on them. In order to promote interoperability amongst senders, receivers, and intermediaries, it includes discussions and recommendations about selected features of SMTP, IMF, and certain extensions to them that are required,

recommended, or to be avoided except in special cases. Furthermore, this document discusses some common mechanisms for confidentiality and authentication in electronic mail.

1.1. Conventions Used in This Document

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.

2. Applicability of Some SMTP Provisions

Over the years since [RFC5321] was published in October 2008, usage of SMTP has evolved, machines and network speeds have increased, and the frequency with which most SMTP senders and receivers have to be prepared to deal with systems that are disconnected from the Internet for long periods or that require many hops to reach has decreased. During the same period, the IETF has become much more sensitive to privacy and security issues and the need to be more resistant or robust against spam and other attacks. In addition SMTP (and Message Format) extensions have been introduced that are expected to evolve the Internet’s mail system to better accommodate environments in which Basic Latin Script is not the norm.

This section describes configuration options and other considerations about SMTP that may be appropriate under various circumstances and discusses the applicability of other protocols that represent newer work or that are intended to deal with relatively newer issues.

2.1. Handling of the Domain Argument to the EHLO Command

If the Domain argument to the EHLO command does not have an address record in the DNS that matches the IP address of the client, the SMTP server may refuse any mail from the client as part of established anti-abuse practice. Operational experience has demonstrated that the lack of a matching address record for the the domain name argument is at best an indication of a poorly-configured MTA, and at worst that of an abusive host.

2.2. Use of Address Literals

The address-literal ABNF non-terminal is used in various places in [I-D.ietf-emailcore-rfc5321bis] grammar. However, for SMTP connections over the public internet, an address-literal as the argument to the EHLO command or the Domain part of the Mailbox argument to the MAIL FROM command is quite likely to result in the message being rejected as a matter of policy at many sites, since they are deemed to be signs of at best a misconfigured server, and at worst either a compromised host or a server that’s intentionally configured to hide its identity.

2.3. Use of Addresses in Top-Level Domains

While addresses in top-level domains (TLDs) (i.e., single-label domains) are syntactically valid, mail to these addresses has never worked reliably. A handful of country code TLDs have top level MX records but they have never been widely used nor well supported. In 2013 [RFC7085] found 18 TLDs with MX records, which dropped to 17 in 2021 and to 11 in 2025 despite many new TLDs having been added.

Mail sent to addresses with single label domains has typically expected the address to be an abbreviation to be completed by a search list, so mail to bob@sales would be completed to bob@sales.example.com. This shortcut has led to unfortunate consequences; in one famous case, in 1991 when the .CS domain was added to the root, mail in computer science departments started to fail as mail to bob@cs was now treated as mail to Czechoslovakia. Hence, for reliable service, mail SHOULD NOT use addresses that contain single label domains.

2.4. Use of SMTP Extensions

As SMTP has evolved over the years, several extensions have become ubiquitous. As a result, the following extensions MUST be supported by SMTP senders and receivers:

* Secure SMTP over Transport Layer Security [RFC3207] (Cf. discussion in Section 6.1.)

* 8-bit MIME [RFC6152]

Similarly, the following extensions SHOULD be supported by SMTP senders and receivers:

* Command Pipelining [RFC2920]

* Internationalized Email [SMTPUTF8]

Delivery Status Notifications [RFC3461] requests, while recommended and useful if supported, have not been widely implemented and deployed. Mail systems that send such requests should be prepared for systems that receive them to not recognize or support them. Note that this extension for notification requests is distinct from the format of notifications defined in [RFC3464] and [RFC6533] and, the special media type defined in [RFC6522]. All of those SHOULD be supported.

Furthermore, while Enhanced Mail System Status Codes ([RFC3463], [RFC5248]) are widely supported, they are not ubiquitous. Nevertheless, they have been found to be useful to SMTP senders in determining the exact reason for a transmission failure in a machine-readable, language-independent manner, thus allowing them to present more detailed and language-specific error messages to users. Given the usefulness of these enhanced codes, SMTP receivers are RECOMMENDED to implement the SMTP Service Extension for Returning Enhanced Error Codes [RFC2034] utilizing the codes registered in [RFC5248].

3. Applicability of Message Format Provisions

This section describes considerations about the Internet Message Format that may be appropriate under various circumstances.

3.1. Use of Empty Quoted Strings

The quoted-string ABNF non-terminal is used in various places in [I-D.ietf-emailcore-rfc5322bis] grammar. While it allows for empty quoted string, such construct is going to cause interoperability issues when used in certain header fields. In particular, use of empty quoted strings is discouraged in "received-token" (a component of a Received header field) and "local-part" (left hand side of email addresses). For example, all of the following email header fields are non-interoperable:

```
Received: from node.example by x.y.test "" foo; 21 Nov 1997
10:01:22 -0600

From: "".bar@example.com

To: foo.""@example.net

Cc: ""@example.com
```

Use of empty quoted strings is fine in "display-name". For example, the following email header field is interoperable:

To: "" <test@example.com>

3.2. Use of Received Header Fields

3.2.1. Generation

Email addresses are commonly classified as Personally Identifiable Information (PII). Improper application of the FOR clause in Received header fields can result in disclosure of PII. As such, the FOR clause SHOULD NOT be generated if the message copy is associated with multiple recipients from multiple SMTP RCPT commands. Otherwise, the value of the FOR clause MUST contain the RCPT address that caused the message to be routed to the recipient of the given copy of the message.

Note however, that if a mail system generates a FOR clause when there is only a single recipient, and doesn’t generate one when there are multiple recipients, the absence of the field is an indication that there is another recipient, which may allow someone to infer that a "blind" copy is involved.

3.2.2. Consumption

Received header fields support analysis of handling and delivery problems, as well as aiding evaluation of a message with suspicious content or attributes. The fields are easily created and have no direct security or privacy protections, and the fields can contain personally sensitive information.

Therefore, the fields do not warrant automatic trust and do warrant careful consideration before disclosing to others. They should be used with care, for whatever information is deemed valuable, and especially when syntax or values occur that are not defined by the specifications [I-D.ietf-emailcore-rfc5321bis] [I-D.ietf-emailcore-rfc5322bis].

3.3. Reuse of Existing Messages

Many mail user agents (MUAs) have functions which use an existing email message as a template for editing a new message. These functions are different from traditional forwarding functions. Those generally preserve the original message as a body part or just the message body as quoted text. For example, an MUA may take an existing message, allow the user to replace the originator and destinations, edit parts of the body, and send it on to the new recipients. When performing such functions, the MUA SHOULD:

* Remove all header fields unknown to the MUA

* Remove any header fields that are only pertinent to the transport of the original message, such as trace header fields (see Section 3.6.7 of [I-D.ietf-emailcore-rfc5322bis])

4. Use of Email Addresses

4.1. Case-Sensitivity, Delimiters, and Mailbox Equivalency

SMTP specifies that the local-part of an email address is case-sensitive (see Section 2.4 of [I-D.ietf-emailcore-rfc5321bis]):

> The local-part of a mailbox MUST BE treated as case sensitive. Therefore, SMTP implementations MUST take care to preserve the case of mailbox local-parts. In particular, for some hosts, the user "smith" is different from the user "Smith". However, exploiting the case sensitivity of mailbox local-parts impedes interoperability and is discouraged.

While case-sensitivity is specified as an absolute requirement, it is important to stress that most implementations do not make case distinctions in local parts (most treat "smith", "Smith", and "SMITH" as the same), and most implementations do preserve the case that is received (from SMTP or HTTP, from address books, or from user input). Maximum interoperability will be achieved by keeping local-parts unchanged (and especially making no attempt to change their case in any way) and by assuming that local-parts that differ only in their case probably refer to the same mailbox. This is particularly important for software that validates user-input fields, where case changes are tempting, but must be avoided.

It is also important to note, as we encounter non-ASCII local-parts over time, that case changes are both character-set dependent and language dependent, and attempts to change case without having the full context necessary are likely to be wrong often enough to matter.

Additionally, final delivery systems vary in how they interpret the use of delimiters such as ’+’ and ’.’ in local-parts. Some systems make distinctions between local-parts such as "smith" and "smith+foo", or "jane.doe" and "janedoe", while others treat them as referring to the same mailboxes respectively. Since only the final delivery system can properly interpret the local-part of an address, originating and transit/relay mail systems are discouraged from making any assumptions as to address equivalence or from making any changes to local-parts containing such delimiters.

4.2. Use of non-ASCII Characters

Proper generation and transmission of email addresses containing non-ASCII characters is discussed in the SMTPUTF8 documents [SMTPUTF8] with more details for the domain-part in the specifications for Internationalized Domain Names [IDNA2008]. Section 9 of [RFC6530] says: "a downgrade mechanism that transforms the local part of an email address cannot be utilized in transit." This is actually just a special case of a principle, discussed in Section 2.3.11 of [I-D.ietf-emailcore-rfc5321bis] and elsewhere, that nothing other than the final delivery system should attempt to interpret or alter the local-part of an address. In particular, they MUST NOT:

* use web URI percent encoding (see Section 2.1 of [RFC3986]) in either the local-part or the domain-part of an address

* perform Internationalized Domain Names for Applications (IDNA) Punycode Conversion (see Section 4.4 of [RFC5891]) on the local-part of an address

Neither of these encodings will produce an address that is guaranteed to be treated as equivalent to the original one.

In some cases, servers or clients may be able to use local knowledge to substitute ASCII addresses for specific non-ASCII addresses, but that is beyond the scope of this memo. See Section 8 of [RFC6530] for further discussion.

4.3. Use and Validation of Email Address Syntax

Email addresses are frequently used as input to, or validated by, forms managed by various libraries, some tied to Versions of HyperText Markup Language (HTML) or other specs and others to client-side libraries developed in Javascript or other languages. In some cases, those who define or supply those systems may have found and corrected errors long ago, but old versions or interpretations are still in use. The allowed grammar for email addresses as incorporated in those tools, and hence in various applications, may be inconsistent with that allowed by the grammar for a "Mailbox" in Section 4.1.2 of [I-D.ietf-emailcore-rfc5321bis], the grammars for use of non-ASCII email addresses specified in the SMTPUTF8 specifications [SMTPUTF8], and common practices on the network. Specifically, the following differences from the standards mentioned above have been observed frequently enough that implementers should be aware of them. In no particular order, the important ones are:

* Absence of support for quoted strings.

* Even when restricted to the ASCII charset, some systems have a restricted character repertoire as compared to the applicable standards. For domain names, only a limited set of characters other than letters and digits are allowed. As a particularly important example for the local-part, the character "+", which is heavily used in some email contexts, is sometimes not permitted, as are characters that historically had special meanings in some gateway contexts such as "%" and "/".

* Some systems allow leading, trailing, or consecutive unquoted dots ('.') in the local-part of email addresses, although few mail systems support their use in that context. Taking advantage of that flexibility is NOT RECOMMENDED.

* As of the time this document was written, many systems still do not allow non-ASCII characters (as discussed in Section 4.2 above) in either the local-part or the domain-part of an email address.

* Additionally, some mail systems allow a trailing dot ('.') in the domain part of email addresses (as allowed as a notation by the basic Domain Names specification [RFC1035] but prohibited by [I-D.ietf-emailcore-rfc5321bis]), and is hence not interoperable with all systems. Consequently, implementations are encouraged to strip any trailing dots that might appear in the domain part of email addresses.

More generally, mail systems that are not responsible for final delivery of a message, but that intend to check the syntax of its email addresses, should be aware that there are many reasons that might cause a valid address to "look strange" or be rejected by tools that are inconsistent with these email standards.

In addition to the specific examples above, the most common cases include mechanisms for organizing messages on delivery systems and security issues (particularly efforts to identify messages other than those from the supposed sender). Especially when a relay system is involved, unless the mail system has special knowledge about the message and its originator, the best option is to treat the address as valid unless the address in question actually violates restrictions of the SMTP [I-D.ietf-emailcore-rfc5321bis] syntax. Section 6.4 of that document contains additional information that might be helpful.

Installations defining rules for assigning or allocating email addresses that expect the syntax of those addresses to be checked by tools with their own, more restrictive, rules should use care to consider both current and past versions of syntax specifications for those mechanisms in their decisions, weighing them against local

needs and other restrictions. Where those other rules allow syntax variations that the IETF specifications cited above do not, those variations should be avoided because they are unlikely to be accepted across the Internet email environment.

5. Use of Multipurpose Internet Mail Extensions (MIME)

Although the Multipurpose Internet Mail Extensions (MIME) [RFC2045] specification and its predecessors and updates have remained separate from the Internet Message Format (IMF) [I-D.ietf-emailcore-rfc5322bis] specification and its predecessors, MIME features such as non-textual message bodies, multi-part message bodies, and the use of character sets other than US-ASCII in message bodies have become nearly ubiquitous in contemporary email. As a result, IMF generators and parsers are expected to support MIME.

6. Confidentiality and Authentication with SMTP

SMTP is specified without embedded mechanisms for authentication or confidentiality; its traffic is therefore "in the clear". Years of operational experience have shown that such transmission exposes the message to easy compromise, including wiretapping and spoofing. To mitigate these risks, several protocols, mechanisms, and extensions have been developed that provide security services to email, most of which are outside the SMTP protocol itself. The most important of these include, but are not limited to:

* TLS [RFC8446], STARTTLS [RFC3207], MTA-STS [RFC8461], and DANE for SMTP [RFC7672] offer confidentiality services between SMTP Clients and the Servers to which they are transmitting messages.

* DKIM [RFC6376], DMARC [RFC7489], ARC [RFC8617], SPF [RFC7208], S/MIME [RFC8551], OpenPGP [RFC9580], and Header Protection for Cryptographically Protected E-mail [RFC9788], offer message level authentication services.

* SMTP Authentication [RFC4954] offers authentication services for an SMTP client connecting to an SMTP server.

* S/MIME [RFC8551] and OpenPGP [RFC9580] allow for message confidentiality outside of the operation of SMTP and were originally focused only on the message content. Newer specifications (see below) extend them to cover header confidentiality as well.

The following sections discuss these facilities and their most common uses.

6.1. Security at the Transport Layer

The Internet email environment has evolved over the years so that the SMTP protocol itself can be used in conjunction with Transport Layer Security (TLS) [RFC8446] protocol to provide both confidentiality and server authentication in the transmission of messages.

It is important that the reader understand what is meant by the terms "Authentication" and "Confidentiality" in this context, and for that we will borrow directly from the TLS specification [RFC8446] (although the pointers to other sections given are to this document).

* Authentication is the process of establishing the identity of one or more of the endpoints of a communication channel. TLS can be used without authentication (as described in Section 6.1.2), but even when it does use authentication, it typically only authenticates the server side of the communication channel (see Section 6.1.3).

* The term "confidentiality" describes a state where the data (i.e., the message) is transmitted in a way that it is only visible to the endpoints of a communication channel.

It is not uncommon for implementers to use the term "encryption" to mean "confidentiality", but this is not quite correct. Rather, encryption using TLS is the most common current method by which confidentiality is achieved with SMTP, but that does not mean that other methods might not be used or future ones developed.

6.1.1. The TLS Protocol

The TLS Protocol [RFC8446] provides confidentiality while the message is in transit from an SMTP client to the next SMTP server. Both client and server will have access to the plain text of the message and there is no guarantee that the message will be stored in an encrypted fashion at its destination. Furthermore, in situations where a message traverses multiple hops through multiple SMTP servers, each intermediate server will typically store the message in plain text and hence have access to that plain text of the message.

6.1.2. Opportunistic Confidentiality

The most common implementation of message confidentiality is known as "opportunistic TLS", which is frequently referred to as "opportunistic encryption". With this method, a receiving server announces in its greeting that it is capable of supporting TLS encryption through the presence of the "STARTTLS" keyword. The sending client then attempts to negotiate an encrypted connection,

and if successful, transmits the message in encrypted form; if negotiation fails, the client falls back to sending the message in clear text.

Opportunistic TLS is optional confidentiality due to provision for falling back to transmission in the clear if a secure connection cannot be established. Opportunistic TLS is often configured to provide confidentiality without authentication, where no effort is made to authenticate the receiving server [RFC3207], Section 4.1. Most modern implementations of SMTP support this method and so the vast majority of email traffic is encrypted during its time transiting from the client to the next server.

Note that opportunistic TLS via the STARTTLS [RFC3207] extension is vulnerable to man-in-the-middle attacks. Enforced confidentiality (Section 6.1.3) can be used to mitigate these attacks.

6.1.3. Enforced Confidentiality, with Receiving Server Authentication

Two protocols exist that move message confidentiality from opportunistic to enforced (with conditions as noted below) - MTA-STS [RFC8461] and DANE for SMTP [RFC7672]. While they differ in their implementation details, receiving servers relying on either protocol can state that they only accept mail if the transmission can be encrypted with TLS. Support for both protocols is increasing, but is not yet mandatory.

These two protocols differ from Opportunistic TLS in that they require receiving server authentication and there is no fallback to sending in the clear.

Note that the protocols mentioned in this section rely not only on the receiving server but also the sending client supporting the protocol intended to be used. If the sending client does not support the protocol requested by the receiving server, the sending client will use Opportunistic TLS or clear-text to transmit the message.

6.2. Message-Level Authentication

Protocols exist to allow for authentication of different identities associated with an email message:

* SPF [RFC7208] provides a method to ensure that the sending mail server is authorized to originate mail from the sender’s domain.

* DKIM [RFC6376] permits a person, role, or organization to claim some responsibility for an email message by associating a domain name [RFC1034] with the message, which they are authorized to use.

* DMARC [RFC7489] relies on SPF and DKIM to allow for validation of the domain in the visible From header.

* ARC [RFC8617] provides a method for each hop to record results of authentication checks performed at that hop.

* S/MIME [RFC8551] and OpenPGP [RFC9580], along with Header Protection for Cryptographically Protected E-mail [RFC9788], allow for email messages to be digitally signed, thereby providing a method to verify that an email message was actually sent by the entity claiming to be the sender.

All of these are outside the scope of this document, as they are outside the scope of SMTP. All of them are, to greater or lesser degrees, subject to risks of compromise on systems processing messages between transport links as discussed above.

6.3. SMTP Authentication

SMTP Authentication [RFC4954], which is often abbreviated as SMTP AUTH, is an extension to SMTP. While its name might suggest that it would be within scope for this section of the Applicability Statement, that is not the case.

SMTP AUTH defines a method for a client to identify itself to a Message Submission Agent (MSA) when presenting a message for transmission, usually using ports 465 or 587 rather than the traditional port 25. The most common implementation of SMTP AUTH is for a person to present a username and password to their mailbox provider’s outbound SMTP server when configuring their MUA for sending mail.

SMTP AUTH MAY be used to limit unauthorized use of VRFY and EXPN commands as described in Section 7.3 of [I-D.ietf-emailcore-rfc5321bis].

6.4. Message-Level Confidentiality

Protocols such as S/MIME [RFC8551] and OpenPGP [RFC9580] exist to allow for message confidentiality outside of the operation of SMTP. In other words, using these protocols results in encryption of the message body prior to its being submitted to the SMTP communications channel. Decryption of the message is then the responsibility of the message recipient. There are numerous implementations of S/MIME and OpenPGP, too many to list here. As both operate fully independent of SMTP, a more detailed discussion is out of scope for this document.

Header Protection for Cryptographically Protected E-mail [RFC9788] extends S/MIME such that some message headers can be encrypted.

6.5. Confidentiality Requirements

The vast majority of email sent on the Internet at present does not use message-level confidentiality. It has been recognized that Internet traffic is exposed to both active attacks and passive monitoring (see BCP61 [RFC3365] and BCP200 [RFC1984]), and therefore that message transmission over SMTP is subject to both. To mitigate these risks, opportunistic confidentiality is now widely implemented and used in Internet email, and some deployment and use of enforced confidentiality is also now seen. Therefore, confidentiality (for example, the STARTTLS extension) MUST be implemented by SMTP servers in order to at least provide over-the-wire confidentiality during an individual SMTP exchange. That said, there are many legacy implementations of SMTP that are still in widespread use in both private and Internet-connected networks and receiving server implementations will often be expected to be capable of receiving such messages. Therefore, SMTP servers MUST be configurable to allow for receiving messages without confidentiality between servers in order to maximize interoperation.

7. Acknowledgments

The Emailcore group arose out of discussions on the ietf-smtp group over changes and additions that should be made to the core email protocols. It was agreed upon that it was time to create a working group that would fix many potential errors and opportunities for misunderstandings within the RFCs.

Special thanks to the following for providing significant portions of text for this document: Dave Crocker, Todd Herr, Tero Kivinen, Barry Leiba, John Levine, Alexey Melnikov, Pete Resnick, and E. Sam.

8. IANA Considerations

This memo includes no requests to or actions for IANA. The IANA registries associated with the protocol specifications they reference are specified in their respective documents.

9. Security Considerations

Security and privacy considerations are discussed throughout this document as they pertain to the referenced specifications. Special note should be taken of the interaction between confidentiality and authentication mechanisms that are applicable to Internet links and therefore potentially sensitive to the multi-hop design of SMTP. Unless the relevant messages and mechanisms are protected from tampering or content exposure on systems that are the endpoints of those links, the security of the mechanisms depends on trust in those intermediate endpoints.

10. References

10.1. Normative References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <https://www.rfc-editor.org/info/rfc2026>.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/info/rfc2045>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2. Informative References

[I-D.ietf-emailcore-rfc5321bis] Klensin, J. C., "Simple Mail Transfer Protocol", Work in Progress, Internet-Draft, draft-ietf-emailcore-rfc5321bis-44, 31 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-emailcore-rfc5321bis-44>.

[I-D.ietf-emailcore-rfc5322bis] Resnick, P., "Internet Message Format", Work in Progress, Internet-Draft, draft-ietf-emailcore-rfc5322bis-12, 13 June 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-emailcore-rfc5322bis-12>.

[IDNA2008] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://www.rfc-editor.org/info/rfc5890>.

Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <https://www.rfc-editor.org/info/rfc5891>.

Faltstrom, P., Ed., "The Unicode Code Points and Internationalized Domain Names for Applications (IDNA)", RFC 5892, DOI 10.17487/RFC5892, August 2010, <https://www.rfc-editor.org/info/rfc5892>.

Alvestrand, H., Ed. and C. Karp, "Right-to-Left Scripts for Internationalized Domain Names for Applications (IDNA)", RFC 5893, DOI 10.17487/RFC5893, August 2010, <https://www.rfc-editor.org/info/rfc5893>.

Klensin, J., "Internationalized Domain Names for Applications (IDNA): Background, Explanation, and Rationale", RFC 5894, DOI 10.17487/RFC5894, August 2010, <https://www.rfc-editor.org/info/rfc5894>.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC1984] IAB and IESG, "IAB and IESG Statement on Cryptographic Technology and the Internet", BCP 200, RFC 1984, DOI 10.17487/RFC1984, August 1996, <https://www.rfc-editor.org/info/rfc1984>.

[RFC2034] Freed, N., "SMTP Service Extension for Returning Enhanced Error Codes", RFC 2034, DOI 10.17487/RFC2034, October 1996, <https://www.rfc-editor.org/info/rfc2034>.

[RFC2920] Freed, N., "SMTP Service Extension for Command Pipelining", STD 60, RFC 2920, DOI 10.17487/RFC2920, September 2000, <https://www.rfc-editor.org/info/rfc2920>.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, DOI 10.17487/RFC3207, February 2002, <https://www.rfc-editor.org/info/rfc3207>.

[RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", BCP 61, RFC 3365, DOI 10.17487/RFC3365, August 2002, <https://www.rfc-editor.org/info/rfc3365>.

[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/info/rfc3461>.

[RFC3463] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 3463, DOI 10.17487/RFC3463, January 2003, <https://www.rfc-editor.org/info/rfc3463>.

[RFC3464] Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", RFC 3464, DOI 10.17487/RFC3464, January 2003, <https://www.rfc-editor.org/info/rfc3464>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC4954] Siemborski, R., Ed. and A. Melnikov, Ed., "SMTP Service Extension for Authentication", RFC 4954, DOI 10.17487/RFC4954, July 2007, <https://www.rfc-editor.org/info/rfc4954>.

[RFC5248] Hansen, T. and J. Klensin, "A Registry for SMTP Enhanced Mail System Status Codes", BCP 138, RFC 5248, DOI 10.17487/RFC5248, June 2008, <https://www.rfc-editor.org/info/rfc5248>.

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

[RFC6152] Klensin, J., Freed, N., Rose, M., and D. Crocker, Ed., "SMTP Service Extension for 8-bit MIME Transport", STD 71, RFC 6152, DOI 10.17487/RFC6152, March 2011, <https://www.rfc-editor.org/info/rfc6152>.

[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/info/rfc6376>.

[RFC6522] Kucherawy, M., Ed., "The Multipart/Report Media Type for the Reporting of Mail System Administrative Messages", STD 73, RFC 6522, DOI 10.17487/RFC6522, January 2012, <https://www.rfc-editor.org/info/rfc6522>.

[RFC6533] Hansen, T., Ed., Newman, C., and A. Melnikov, "Internationalized Delivery Status and Disposition Notifications", RFC 6533, DOI 10.17487/RFC6533, February 2012, <https://www.rfc-editor.org/info/rfc6533>.

[RFC7085] Levine, J. and P. Hoffman, "Top-Level Domains That Are Already Dotless", RFC 7085, DOI 10.17487/RFC7085, December 2013, <https://www.rfc-editor.org/info/rfc7085>.

[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/info/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/info/rfc7489>.

[RFC7672] Dukhovni, V. and W. Hardaker, "SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)", RFC 7672, DOI 10.17487/RFC7672, October 2015, <https://www.rfc-editor.org/info/rfc7672>.

[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/info/rfc8446>.

[RFC8461] Margolis, D., Risher, M., Ramakrishnan, B., Brotman, A., and J. Jones, "SMTP MTA Strict Transport Security (MTA-STS)", RFC 8461, DOI 10.17487/RFC8461, September 2018, <https://www.rfc-editor.org/info/rfc8461>.

[RFC8551] Schaad, J., Ramsdell, B., and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC 8551, DOI 10.17487/RFC8551, April 2019, <https://www.rfc-editor.org/info/rfc8551>.

[RFC8617] Andersen, K., Long, B., Ed., Blank, S., Ed., and M. Kucherawy, Ed., "The Authenticated Received Chain (ARC) Protocol", RFC 8617, DOI 10.17487/RFC8617, July 2019, <https://www.rfc-editor.org/info/rfc8617>.

[RFC9580] Wouters, P., Ed., Huigens, D., Winter, J., and Y. Niibe, "OpenPGP", RFC 9580, DOI 10.17487/RFC9580, July 2024, <https://www.rfc-editor.org/info/rfc9580>.

[RFC9788] Gillmor, D. K., Hoeneisen, B., and A. Melnikov, "Header Protection for Cryptographically Protected Email", RFC 9788, DOI 10.17487/RFC9788, August 2025, <https://www.rfc-editor.org/info/rfc9788>.

[SMTPUTF8] Klensin, J. and Y. Ko, "Overview and Framework for Internationalized Email", RFC 6530, DOI 10.17487/RFC6530, February 2012, <https://www.rfc-editor.org/info/rfc6530>.

Yao, J. and W. Mao, "SMTP Extension for Internationalized Email", RFC 6531, DOI 10.17487/RFC6531, February 2012, <https://www.rfc-editor.org/info/rfc6531>.

Yang, A., Steele, S., and N. Freed, "Internationalized Email Headers", RFC 6532, DOI 10.17487/RFC6532, February 2012, <https://www.rfc-editor.org/info/rfc6532>.

Appendix A. Change Log

RFC Editor: Please remove this appendix before publication.

A.1. Changes from draft-klensin-email-core-as-00 (2020-03-30) to draft-ietf-emailcore-as-00

* Change of filename, metadata, and date to reflect transition to WG document for new emailcore WG. No other substantive changes

A.2. Changes from draft-ietf-emailcore-as-00 (2020-10-06) to -01

* Added co-authors (list is in alphabetical order for the present).

* Updated references to 5321bis and 5322bis.

* Added note at top, "This version is provided as a document management convenience to update the author list and make an un-expired version available to the WG. There are no substantive changes from the prior version", which should be removed for version -02.

A.3. Changes from draft-ietf-emailcore-as-01 (2021-04-09) to -02

* Added new editors and also added some issues the emailcore group will be dealing with.

* Added reference to RFC 6648.

A.4. Changes from draft-ietf-emailcore-as-02 (2021-08-06) to -03

* Moved discussion of address-literals (issue #1) and domain names in EHLO (issue #19) under SMTP Provisions section

* Moved discussion of empty quoted-strings under Message Format Provisions section

* Added text on use of addresses in TLDs (issue #50)

* Marked all authors as editors.

* Miscellaneous editorial changes.

A.5. Changes from draft-ietf-emailcore-as-03 (2022-01-31) to -04

* Added requirements for SMTP extensions (issue #40).

A.6. Changes from draft-ietf-emailcore-as-04 (2022-05-21) to -05

* Added text addressing use ofx enhanced status codes.

* Added text addressing confidentiality and authentication (issue #54).

A.7. Changes from draft-ietf-emailcore-as-05 (2022-10-24) to -06

* Converted source to xml2rfc v3.

* Replaced placeholder Introduction with new text.

* Updated keywords boilerplate.

* Added text on interoperability of email addresses in general and use in HTML forms (issue #51).

* Added text stating that implementations are expected to support MIME (issue #65).

* Added placeholders for issues #38 and #55.

* Add list of contributors in Acknowledgments.

* Added minimal Security Considerations section.

A.8. Changes from draft-ietf-emailcore-as-06 (2022-11-07) to -07

* Added text addressing use of FOR clause in Received header fields (issue #55).

* Miscellaneous editorial changes.

A.9. Changes from draft-ietf-emailcore-as-07 (2023-03-13) to -08

* Added text addressing use of Received header fields by MUAs (issue #85).

* Added advice against use of Percent-Encoding non-ASCII characters in email addresses (issue #78).

* Miscellaneous editorial changes.

A.10. Changes from draft-ietf-emailcore-as-08 (2023-12-18) to -09

* Acknowledge the existence of port 465 for submission (issue #80).

* Remove "Use of Time Zones in Date and Received Header Fields" placeholder (issue #66).

* Miscellaneous editorial changes.

A.11. Changes from draft-ietf-emailcore-as-09 (2024-07-02) to -10

* Added Open Issues Section

* Removed placeholder for issue #38 - Clarify 78 octet limit versus 998 line length limit (https://github.com/ietf-wg-emailcore/emailcore/issues/38)

* Applied "final" proposed text for issue #78 - Advice against using URL %-encoding on non-ASCII email addresses (https://github.com/ietf-wg-emailcore/emailcore/issues/78)

* Applied proposed text for issue #84 - Handling of Trace Header Fields by MUAs (https://github.com/ietf-wg-emailcore/emailcore/issues/84)

A.12. Changes from draft-ietf-emailcore-as-10 (2024-07-03) to -11

* Added Open Issue #94 - Use of Quoted Strings (https://github.com/ietf-wg-emailcore/emailcore/issues/94)

A.13. Changes from draft-ietf-emailcore-as-11 (2024-10-21) to -12

* Applied new proposed text to Section 3.1

* Applied new proposed text for issue #40 - Recommended SMTP Extensions (https://github.com/ietf-wg-emailcore/emailcore/issues/40)

* Applied new proposed text for issue #78 - Advice against using URL %-encoding on non-ASCII email addresses (https://github.com/ietf-wg-emailcore/emailcore/issues/78)

* Applied new proposed text for issue #84 - Handling of Trace Header Fields by MUAs (https://github.com/ietf-wg-emailcore/emailcore/issues/84)

* Applied new proposed text for issue #85 - What mail agents should do/not do with Received header fields (https://github.com/ietf-wg-emailcore/emailcore/issues/85)

A.14. Changes from draft-ietf-emailcore-as-12 (2024-11-09) to -13

* Fixed discussion of Punycode (domain-part -> local-part) in Section 4.2

* Removed Keywords from discussion in Section 3.1

* Added example of empty display-name in Section 3.1

A.15. Changes from draft-ietf-emailcore-as-13 (2025-01-30) to -14

* Added STARTTLS to the MUST implement list in Section 2.4

* Added Alexey Melnikov’s proposed text for issue #93 - "VRFY, EXPN, and Security" should point to SMTP AUTH RFC (https://github.com/ietf-wg-emailcore/emailcore/issues/94)

* Applied (with some editorial changes), Tero Kivinen’s proposed text to Section 6.

A.16. Changes from draft-ietf-emailcore-as-14 (2025-02-27) to -15

* Miscellaneous editorial changes

A.17. Changes from draft-ietf-emailcore-as-15 (2025-03-18) to -16

* Changed "FOR clause MUST NOT be generated if the message copy is associated with multiple recipients from multiple SMTP RCPT commands" to "SHOULD NOT".

* Reintroduced examples of non-interoperable local-parts containing empty quoted strings (issue #93 (https://github.com/ietf-wg-emailcore/emailcore/issues/94)).

* Added short descriptions of SPF and DKIM, and added S/MIME, OpenPGP, and Header Protection for Cryptographically Protected E-mail as methods of Message-Level Authentication (issues #110 (https://github.com/ietf-wg-emailcore/emailcore/issues/94), #132 (https://github.com/ietf-wg-emailcore/emailcore/issues/94), #133 (https://github.com/ietf-wg-emailcore/emailcore/issues/94)).

A.18. Changes from draft-ietf-emailcore-as-16 to -17

* Changed all instances of "optional confidentiality" to "opportunistic confidentiality" and all instances of "required confidentiality" to "enforced confidentiality". (issue #113 (https://github.com/ietf-wg-emailcore/emailcore/issues/113))

* Added Section "6.7 Confidentiality Requirements" (issue #113 (https://github.com/ietf-wg-emailcore/emailcore/issues/113))

* Updated DKIM description to use a slight modification to the first sentence of RFC 6376 Introduction (issue #138 (https://github.com/ietf-wg-emailcore/emailcore/issues/138)).

A.19. Changes from draft-ietf-emailcore-as-17 to -18

* Added text clarifying that hop-by-hop confidentiality does not guarantee end-to-end confidentiality.

A.20. Changes from draft-ietf-emailcore-as-18 to -19

* Added text stating that STARTTLS is vulnerable to man-in-middle-attacks (issue #134 (https://github.com/ietf-wg-emailcore/emailcore/issues/134))

* Rewrote opening paragraph of Opportunistic Confidentiality based on Rob Sayre’s suggestions (issue #135 (https://github.com/ietf-wg-emailcore/emailcore/issues/135))

* Rewrote text discussing use of email addresses in HTML forms and provided a more restricted Mailbox ABNF (issue #137 (https://github.com/ietf-wg-emailcore/emailcore/issues/137))

A.21. Changes from draft-ietf-emailcore-as-19 to -20

* Updated stats regarding MX records on top-level domains.

* Tweaked hop-by-hop confidentiality text again (Resnick).

* Made clear that TLS authentication is optional (Resnick/Sayre).

* Removed hop-by-hop paragraph in Opportunistic Confidentiality as its now discussed in TLS section (Sayre).

* Removed hop-by-hop paragraph in Enforced Confidentiality as its now discussed in TLS section (Sayre).

* Added reference to LAMPS documents in Message-Level Confidentiality (Sayre).

* Miscellaneous editorial changes.

A.22. Changes from draft-ietf-emailcore-as-20 to -21

* Restructured Section 4.3 and eliminated the dependency of the discussion on deviations from the core email specs on, e.g., various versons of HTML.
  Added new Section 4.4, and eliminated references that are now unnecessary.

* Minor editorial corrections.

A.23. Changes from draft-ietf-emailcore-as-21 to -22

* Rewrote Section 4.3 to further reflect the "there are problems out there" approach, further reducing the dependencies associated with HTML. Re-integrated the Section 4.4 material that was separated in -21.

* Rewrote and reorganized Section 6, grouping TLS-related material into another layer of subsections (Section 6.1) and applying a set of changes agreed by the WG.

* Numerous, but individually minor, editorial adjustments and corrections.

A.24. Changes from draft-ietf-emailcore-as-22 to -23

* Corrected an error in which IDNA2008 documents were cited rather than SMTPUTF8 ones and tuned text slightly.

* Tuned discussions of S/MIME, PGP, and RFC 9788 slightly, including new text in Section 6.4

* Corrected an error in the description of Opportunistic TLS.

Authors' Addresses

John C Klensin (editor)
1770 Massachusetts Ave, Ste 322
Cambridge, MA 02140
United States of America
Phone: +1 617 245 1457
Email: john-ietf@jck.com

Kenneth Murchison (editor)
Fastmail US LLC
1429 Walnut Street - Suite 1201
Philadelphia, PA 19102
United States of America
Email: murch@fastmailteam.com