Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 30 November 2026

A. Melnikov
Isode Ltd

29 May 2026

SMTP REMEMBERME extension for quick reauthentication token generation
draft-melnikov-smtp-rememberme-00

Abstract

This document specifies an SMTP extension for generating quick reauthentication tokens that allow clients to re-login without user interaction, once authentication using a strong SASL mechanism is completed.

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 30 November 2026.

Copyright Notice

Table of Contents

1. Introduction

This document specifies an SMTP [RFC5321] (update to rfc5321bis, once published) extension which is a protocol specific extension to Simple Authentication and Security Layer (SASL) [RFC4422] framework for generation of proof-of-posession reauthentication tokens. Such tokens can be used for subsequent 1 roundtrip reauthentication using SASL mechanisms such as REMEMBERME and HT2-*.

The typical sequence of events is going to be like this:

1. Client establishes SMTP connection protected by TLS on Connection 1.

2. On Connection 1 the client authenticates using a strong SASL mechanism, which might be CPU intensive, and most likely requires user interaction, e.g., SCRAM with 2FA extension, PASSKEY, OAUTH with 2FA.

3. On Connection 1 the client requests reauthentication token using REMEMBERME command.

4. <Connection gets interrupted or closed due to inactivity>

5. Client establishes another SMTP connection protected by TLS on Connection N. The client then uses a previous issues quick reauthentication token with one of 1 round trip SASL mechanisms such as REMEMBERME and HT2-*. The same token is reusable on other SMTP connections until it is replaced or revoked.

SMTP servers advertise support for this extension by returning one or more <token-type> in the EHLO REMEMBERME response.

2. 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.

3. REMEMBERME command

The REMEMBERME command is used to request a reauthentication token that is suitable for 1 round trip SASL authentication mechanisms. The REMEMBERME command takes 1 parameter which is token type name. See Section 5 for the list of registered tokens types.

This command is only allowed after a successfully completed AUTH command [RFC4954].

Upon receipt of REMEMBERME command the SMTP server checks that the specified token type is recognized and supported. If it is, it generates a new token of the requested type and returns it in the 235 response, that might also contain the 2.7.X enhanced status code.

```
  S: 220-smtp.example.com ESMTP Server
  C: EHLO client.example.com
  S: 250-smtp.example.com Hello client.example.com
  S: 250-AUTH GSSAPI PASSKEY SCRAM-SHA-256
  S: 250-ENHANCEDSTATUSCODES
  S: 250 STARTTLS
  C: STARTTLS
  S: 220 Ready to start TLS
    ... TLS negotiation proceeds, further commands
        protected by TLS layer ...
  C: EHLO client.example.com
  S: 250-smtp.example.com Hello client.example.com
  S: 250-AUTH GSSAPI PASSKEY SCRAM-SHA-256 PLAIN
  S: 250 REMEMBERME JWT RANDOM
  C: AUTH SCRAM-SHA-256 ...
   <SASL exchange>
  S: 235 2.7.0 Authentication successful
     ... later in the same session ...
  C: REMEMBERME JWT
  S: 235 2.7.X <base64-encoded token>
```

Note that in the above example list of capabilities returned in EHLO response changes after STARTTLS. Also note that the order of AUTH and REMEMBERME lines in EHLO response can be arbitrary.

4. Formal Syntax

```
rememberme-cmd = "REMEMBERME" SP token-type

token-type     = atom
                     ;; SHOULD be registered with IANA

rememberme-rsp = "235" [SP 2.7.X] SP base64-token
                     ;; Successful response to REMEMBERME command
                     ;; contains a base64-encoded token.
                     ;; An optional enhanced status code might preceed the token.

base64-token        = base64
```

5. IANA Considerations

TBD. Register the SMTP capabilities and create a separate registry of token types? The separate registry will be shared with the IMAP REMEMBERME document.

Also request assignment of 2.7.X from https://www.iana.org/assignments/smtp-enhanced-status-codes/smtp-enhanced-status-codes.xhtml

6. Security Considerations

TBD.

7. Normative References

[ABNF] Crocker, D., Ed. and P. Overell, Ed., "Augmented BNF for Syntax Specifications: ABNF", RFC 5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[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>.

[RFC4422] Melnikov, A., Ed. and K. Zeilenga, Ed., "Simple Authentication and Security Layer (SASL)", RFC 4422, DOI 10.17487/RFC4422, June 2006, <https://www.rfc-editor.org/info/rfc4422>.

[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>.

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

[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>.

Author’s Address

Alexey Melnikov
Isode Ltd
14 Castle Mews
Hampton
TW12 2NP
United Kingdom
Email: alexey.melnikov@isode.com