Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 18 August 2025

A. Melnikov
Isode Ltd

14 February 2025

IMAP REMEMBERME extension for quick reauthentication token generation
draft-melnikov-imap-rememberme-00

Abstract

This document specifies an IMAP 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 18 August 2025.

Copyright Notice

Table of Contents

1. Introduction 2
2. Conventions Used in This Document 3
3. REMEMBERME command 3
4. Formal Syntax 3
5. IANA Considerations 4
6. Security Considerations 4
7. Normative References 4
Author's Address 5

1. Introduction

This document specifies an IMAP [RFC9051] 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 HT-*.

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

1. Client establishes IMAP 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.

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 IMAP 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 HT-*. The same token is reusable on other IMAP connections until it is replaced or revoked.

IMAP servers advertise support for this extension by returning one or more TOKEN=<token-type> capabilities in the CAPABILITY 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

Arguments: Token type

Responses: REQUIRED TOKEN response code

Result: OK - new token successfully issued

NO - authentication mechanism too week, unrecognized token type

BAD - command unknown or arguments invalid,

invalid state

This command is only allowed in authenticated state.

Upon receipt of REMEMBERME command the IMAP 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 TOKEN response code in the tagged OK response.

```
  S: * OK ACME IMAP Server v1.23 is ready
  C: 22 CAPABILITY
  S: * CAPABILITY IMAP4rev1 IMAP4rev2 STARTTLS AUTH=PASSKEY AUTH=REMEMBERME AUTH=SCRAM-SH
A-256 TOKEN=JWT TOKEN=RANDOM
  S: 22 CAPABILITY completed
  C: 23 STARTTLS
  S: 23 OK Completed
  C: 24 AUTHENTICATE ...
   <SASL exchange>
  S: 24 OK Completed
  C: 25 REMEMBERME JWT
  S: 26 OK [TOKEN <base64-encoded token>] Completed
```

4. Formal Syntax

```
   capability     =/ "TOKEN=" token-type
                       ;; <capability> from [RFC3501]

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

   resp-text-code      =/ "TOKEN" SP base64-token

   base64-token        = base64
```

5. IANA Considerations

TBD. Regeister the IMAP capabilities and create a separate registry of token types.

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>.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <https://www.rfc-editor.org/info/rfc3501>.

[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>.

[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>.

[RFC9051] Melnikov, A., Ed. and B. Leiba, Ed., "Internet Message Access Protocol (IMAP) - Version 4rev2", RFC 9051, DOI 10.17487/RFC9051, August 2021, <https://www.rfc-editor.org/info/rfc9051>.

Author’s Address

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