Stream: Internet Engineering Task Force (IETF)
RFC: 9734
Category: Standards Track
Published: February 2025
ISSN: 2070-1721
Author: R. Mahy
Rohan Mahy Consulting Services

RFC 9734
X.509 Certificate Extended Key Usage (EKU) for Instant Messaging URIs

Abstract

RFC 5280 specifies several extended key purpose identifiers (KeyPurposeIds) for X.509 certificates. This document defines an Instant Messaging (IM) identity KeyPurposeId for inclusion in the Extended Key Usage (EKU) extension of X.509 v3 public key certificates

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9734.

Copyright Notice

Table of Contents

1. Introduction

Instant Messaging (IM) systems using the Messaging Layer Security (MLS) [RFC9420] protocol can incorporate per-client identity certificate credentials. A subjectAltName in these certificates can be an IM URI [RFC3860] or Extensible Messaging and Presence Protocol (XMPP) URI [RFC6121], for example.

Organizations may be unwilling to issue certificates for an IM client using a general KeyPurposeId, such as `id-kp-serverAuth` or `id-kp-clientAuth`, because of the risk that such certificates could be abused in a cross-protocol attack.

An explanation of MLS credentials as they apply to IM is described in [E2E-IDENTITY]. These credentials are expected to be heavily used in the More Instant Messaging Interoperability (MIMI) Working Group.

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. The IM URI EKU

This specification defines the KeyPurposeId `id-kp-imUri`, which may be included in certificates used to prove the identity of an IM client. This EKU extension **MAY**, at the option of the certificate issuer, be either critical or non-critical.

```
id-kp  OBJECT IDENTIFIER  ::= {
  iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) kp(3) }

id-kp-imUri OBJECT IDENTIFIER ::= { id-kp 40 }
```

4. Security Considerations

The security considerations of [RFC5280] are applicable to this document. The `id-kp-imUri` extended key purpose does not introduce new security risks but instead reduces existing security risks by providing means to identify if the certificate is generated to sign IM identity credentials. Issuers **SHOULD NOT** set the `id-kp-imUri` extended key purpose and an `id-kp-clientAuth` or `id-kp-serverAuth` extended key purpose: that would defeat the improved specificity offered by having an `id-kp-imUri` extended key purpose.

5. IANA Considerations

IANA has registered the following OID in the "SMI Security for PKIX Extended Key Purpose" registry (1.3.6.1.5.5.7.3). This OID is defined in Section 3.

Decimal	Description	References
40	id-kp-imUri	RFC 9734

Table 1

IANA has also registered the following ASN.1 [ITU.X690.2021] module OID in the "SMI Security for PKIX Module Identifier" registry (1.3.6.1.5.5.7.0). This OID is defined in Appendix A.

Decimal	Description	References
113	id-mod-im-eku	RFC 9734

Table 2

6. References

6.1. Normative References

[ITU.X680.2021] ITU-T, "Information Technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1:2021, February 2021, <https://www.itu.int/rec/T-REC-X.680>.

[ITU.X690.2021] ITU-T, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, ISO/IEC 8825-1-2021, February 2021, <https://www.itu.int/rec/T-REC-X.690>.

[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>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[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>.

6.2. Informative References

[E2E-IDENTITY] Barnes, R. and R. Mahy, "Identity for E2E-Secure Communications", Work in Progress, Internet-Draft, draft-barnes-mimi-identity-arch-01, 23 October 2023, <https://datatracker.ietf.org/doc/html/draft-barnes-mimi-identity-arch-01>.

[RFC3860] Peterson, J., "Common Profile for Instant Messaging (CPIM)", RFC 3860, DOI 10.17487/RFC3860, August 2004, <https://www.rfc-editor.org/info/rfc3860>.

[RFC6121] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence", RFC 6121, DOI 10.17487/RFC6121, March 2011, <https://www.rfc-editor.org/info/rfc6121>.

[RFC9420] Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", RFC 9420, DOI 10.17487/RFC9420, July 2023, <https://www.rfc-editor.org/info/rfc9420>.

Appendix A. ASN.1 Module

The following module adheres to ASN.1 specifications [ITU.X680.2021] and [ITU.X690.2021].

```
<CODE BEGINS>

IM-EKU
  { iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-im-eku (113) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- OID Arc

id-kp OBJECT IDENTIFIER ::=
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) kp(3) }

-- Extended Key Usage Values

id-kp-imUri OBJECT IDENTIFIER ::= { id-kp 40 }

END


<CODE ENDS>
```

Acknowledgments

Thanks to Sean Turner and Russ Housley for reviews, suggestions, corrections, and encouragement.

Author's Address

Rohan Mahy
Rohan Mahy Consulting Services
Email: rohan.ietf@gmail.com