

Workgroup: LAMPS
Internet-Draft:
draft-ietf-lamps-8410-ku-clarifications-01
Updates: [8410](#) (if approved)
Published: 1 April 2022
Intended Status: Standards Track
Expires: 3 October 2022
Authors: S. Turner S. Josefsson D. McCarney
 sn3rd SJD AB Square Inc.
 T. Ito
 SECOM CO., LTD.

Clarifications for Ed25519, Ed448, X25519, and X448 Algorithm Identifiers

Abstract

This document updates RFC 8410 to clarify existing and specify missing semantics for key usage bits when used in certificates that support the Ed25519, Ed448, X25519, and X448 Elliptic Curve Cryptography algorithms.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-ietf-lamps-8410-ku-clarifications/>.

Source for this draft and an issue tracker can be found at <https://github.com/lamps-wg/8410-ku-clarifications>.

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 3 October 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

- [1. Introduction](#)
- [2. Terminology](#)
- [3. New Section 5 for RFC 8410](#)
- [4. Security Considerations](#)
- [5. IANA Considerations](#)
- [6. References](#)
 - [6.1. Normative References](#)
 - [6.2. Informative References](#)
- [Acknowledgments](#)
- [Authors' Addresses](#)

1. Introduction

[[RFC8410](#)] specifies the syntax and semantics for the Subject Public Key Information field in certificates that support Ed25519, Ed448, X25519, and X448 Elliptic Curve Cryptography (ECC) algorithms. As part of these semantics, it defines what combinations are permissible for the values of the key usage extension [[RFC5280](#)]. [[RFC8410](#)] did not define what values are not permissible nor did it refer to keyEncipherment or dataEncipherment. [[ERRATA](#)] has also been submitted to clarify that keyCertSign is always set in certification authority certificates. To address these changes, this document replaces Section 5 of [[RFC8410](#)] with [Section 3](#).

2. Terminology

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. New Section 5 for RFC 8410

The intended application for the key is indicated in the keyUsage certificate extension.

If the keyUsage extension is present in a certificate that indicates id-X25519 or id-X448 in SubjectPublicKeyInfo, then the following **MUST** be present:

keyAgreement;

one of the following **MAY** also be present:

encipherOnly; or
decipherOnly;

and the following **MUST NOT** be present:

digitalSignature;
nonRepudiation;
keyEncipherment;
dataEncipherment;
keyCertSign; and
cRLSign.

If the keyUsage extension is present in an end-entity or CRL issuer certificate that indicates id-Ed25519 or id-Ed448 in SubjectPublicKeyInfo, then the keyUsage extension **MUST** contain at least one of the following:

nonRepudiation;
digitalSignature; and
cRLSign;

and the following **MUST NOT** be present:

keyEncipherment;
dataEncipherment;
keyAgreement;
keyCertSign;
encipherOnly; and
decipherOnly.

If the keyUsage extension is present in a certification authority certificate that indicates id-Ed25519 or id-Ed448 in SubjectPublicKeyInfo, then the keyUsage extension **MUST** contain:

keyCertSign

and zero or more of the following:

nonRepudiation;
digitalSignature; and
cRLSign;

and the following **MUST NOT** be present:

keyEncipherment;
dataEncipherment;
keyAgreement;
encipherOnly; and
decipherOnly.

4. Security Considerations

This document introduces no new security considerations beyond those found in [RFC8410].

5. IANA Considerations

This document has no IANA actions.

6. References

6.1. Normative References

- [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/rfc/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/rfc/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/rfc/rfc8174>>.
- [RFC8410] Josefsson, S. and J. Schaad, "Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure", RFC 8410, DOI 10.17487/RFC8410, August 2018, <<https://www.rfc-editor.org/rfc/rfc8410>>.

6.2. Informative References

- [ERRATA] Liao, L., "Errata 5696", 17 April 2019, <<https://www.rfc-editor.org/errata/eid5696>>.

Acknowledgments

We would like to thank Russ Housley, Mike Jenkins, and Corey Bonnell for the comments.

Authors' Addresses

Sean Turner
sn3rd

Email: sean@sn3rd.com

Simon Josefsson
SJD AB

Email: simon@josefsson.org

Daniel McCarney
Square Inc.

Email: daniel@binaryparadox.net

Tadahiko Ito
SECOM CO., LTD.

Email: tadahiko.ito.public@gmail.com