Stream:	Internet Engineering Task Force (IETF)
RFC:	9295
Updates:	8410
Category:	Standards Track
Published:	September 2022
ISSN:	2070-1721

Authors:	S. Turner	S. Josefsson	D. McCarney	T. Ito
	sn3rd	*SJD AB*	*Square Inc.*	*SECOM CO., LTD.*

RFC 9295
Clarifications for Ed25519, Ed448, X25519, and X448 Algorithm Identifiers

Abstract

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

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/rfc9295.

Copyright Notice

Table of Contents

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 keyUsage extension [RFC5280]. [RFC8410] did not define what values are not permissible, nor did it refer to keyEncipherment or dataEncipherment. [Err5696] 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
decipherOnly
```

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

```
digitalSignature
nonRepudiation
keyEncipherment
dataEncipherment
keyCertSign
cRLSign
```

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

```
nonRepudiation
digitalSignature
cRLSign
```

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

```
keyEncipherment
dataEncipherment
keyAgreement
keyCertSign
encipherOnly
decipherOnly
```

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

```
cRLSign
```

and zero or more of the following:

```
nonRepudiation
digitalSignature
```

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

```
keyEncipherment
dataEncipherment
keyAgreement
encipherOnly
decipherOnly
```

and if the CRL issuer is also a certification authority, then the keyUsage extension **MUST** also contain:

```
keyCertSign
```

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
cRLSign
```

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

```
keyEncipherment
dataEncipherment
keyAgreement
encipherOnly
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/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>.

[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/info/rfc8410>.

6.2. Informative References

[Err5696] RFC Errata, Erratum ID 5696, RFC 8410, <https://www.rfc-editor.org/errata/eid5696>.

Acknowledgments

We would like to thank Russ Housley, Mike Jenkins, and Corey Bonnell for their 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