

Internet Engineering Task Force (IETF)
Request for Comments: 8813
Updates: 5480
Category: Standards Track
ISSN: 2070-1721

T. Ito
SECOM CO., LTD.
S. Turner
sn3rd
August 2020

Clarifications for Elliptic Curve Cryptography Subject Public Key Information

Abstract

This document updates RFC 5480 to specify semantics for the `keyEncipherment` and `dataEncipherment` key usage bits when used in certificates that support Elliptic Curve Cryptography.

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/rfc8813>.

Copyright Notice

Copyright (c) 2020 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction
 2. Terminology
 3. Updates to Section 3
 4. Security Considerations
 5. IANA Considerations
 6. Normative References
- Authors' Addresses

1. Introduction

[RFC5480] specifies the syntax and semantics for the Subject Public Key Information field in certificates that support Elliptic Curve Cryptography. As part of these semantics, it defines what combinations are permissible for the values of the key usage extension [RFC5280]. [RFC5480] specifies 7 of the 9 values; it makes

no mention of the keyEncipherment and dataEncipherment key usage bits. This document corrects this omission by updating Section 3 of [RFC5480] to make it clear that neither keyEncipherment nor the dataEncipherment key usage bits are set for key agreement algorithms defined therein. The additions are to be made to the end of Section 3 of [RFC5480].

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. Updates to Section 3

If the keyUsage extension is present in a certificate that indicates id-ecPublicKey in SubjectPublicKeyInfo, then the following values MUST NOT be present:

keyEncipherment; and
dataEncipherment.

If the keyUsage extension is present in a certificate that indicates id-ecDH or id-ecMQV in SubjectPublicKeyInfo, then the following values also MUST NOT be present:

keyEncipherment; and
dataEncipherment.

4. Security Considerations

This document introduces no new security considerations beyond those found in [RFC5480].

5. IANA Considerations

This document has no IANA actions.

6. 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>>.
- [RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", RFC 5480, DOI 10.17487/RFC5480, March 2009, <<https://www.rfc-editor.org/info/rfc5480>>.
- [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>>.

Authors' Addresses

Tadahiko Ito
SECOM CO., LTD.

Email: tadahiko.ito.public@gmail.com

Sean Turner
sn3rd

Email: sean@sn3rd.com