Internet Engineering Task Force (IETF)
Request for Comments: 6161
Updates: 6033
Category: Standards Track
ISSN: 2070-1721

S. Turner
IECA

April 2011

Elliptic Curve Algorithms for Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type

Abstract

This document describes the conventions for using several Elliptic Curve cryptographic algorithms with the Cryptographic Message Syntax (CMS) encrypted key package content type. Specifically, it includes conventions necessary to implement Elliptic Curve Diffie-Hellman (ECDH) with EnvelopedData and Elliptic Curve Digital Signature Algorithm (ECDSA) with SignedData. This document extends RFC 6033.

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 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6161.

1. Introduction

This document describes the conventions for using Elliptic Curve cryptographic algorithms with the Cryptographic Message Syntax (CMS) encrypted key package content type [RFC6032]. Specifically, it includes conventions necessary to implement the following CMS content types: EnvelopedData [RFC5652] and SignedData [RFC5652]. This document amends [RFC6033]. Familiarity with [RFC6033] and [RFC5753] is assumed.

This document does not define any new algorithms; instead, it refers to previously defined algorithms.

1.1 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 [RFC2119].

2. EnvelopedData

When key agreement is used, standard (as opposed to cofactor) ECDH [RFC6090][RFC5753] MAY be supported.

3. SignedData

If an implementation encapsulates EncryptedKeyPackage with SignedData [RFC5652], then it MAY support the signature scheme ECDSA [RFC6090][RFC5753].

4. Public Key Sizes

The easiest way to implement SignedData and EnvelopedData is with public key certificates [RFC5280][RFC5480]. If an implementation supports ECDSA or ECDH, then it MUST support keys on the P-256 curve.

5. Security Considerations

The security considerations from [RFC5280], [RFC5480], [RFC5652], [RFC5753], [RFC6033], and [RFC6090] apply.

6. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[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, May 2008.

[RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", RFC 5480, March 2009.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, September 2009.

[RFC5753] Turner, S. and D. Brown, "Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)", RFC 5753, January 2010.

[RFC6032] Turner, S. and R. Housley, "Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type", RFC 6032, December 2010.

[RFC6033] Turner, S., "Algorithms for Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type", RFC 6033, December 2010.

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC 6090, February 2011.

Author's Address

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

EMail: turners@ieca.com