Internet Engineering Task Force (IETF)
Request for Comments: 6162
Updates: 5959
Category: Standards Track
ISSN: 2070-1721

S. Turner
IECA

April 2011

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

## Abstract

This document describes conventions for using Elliptic Curve cryptographic algorithms with SignedData and EnvelopedData to protect the AsymmetricKeyPackage 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 5959.

## 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/rfc6162.

## 1. Introduction

[RFC5959] describes conventions necessary to protect the AsymmetricKeyPackage content type [RFC5958] with Cryptographic Message Syntax (CMS) protecting the following content types: SignedData [RFC5652], EnvelopedData [RFC5652], EncryptedData [RFC5652], AuthenticatedData [RFC5652], and AuthEnvelopedData [RFC5083]. This document amends [RFC5959] by extending the algorithms used with SignedData and EnvelopedData to include Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH), respectively. Familiarity with [RFC5959] 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. AsymmetricKeyPackage

As noted in Asymmetric Key Packages [RFC5958], CMS can be used to protect the AsymmetricKeyPackage. The following provides guidance for SignedData [RFC5652] and EnvelopedData [RFC5652] when used with Elliptic Curve algorithms.

### 2.1. SignedData

If an implementation supports SignedData, then it MAY support ECDSA [RFC6090][RFC5753].

### 2.2. EnvelopedData

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

## 3. 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.

## 4. Security Considerations

The security considerations from [RFC5280], [RFC5480], [RFC5652], [RFC5753], [RFC5959], and [RFC6090] apply.

## 5. References

### 5.1. 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.

[RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, August 2010.

[RFC5959] Turner, S., "Algorithms for Asymmetric Key Package Content Type", RFC 5959, August 2010.

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

### 5.2. Informative Reference

[RFC5083] Housley, R., "Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type", RFC 5083, November 2007.

## Author's Address

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

EMail: turners@ieca.com