

Network Working Group
Internet-Draft
Updates: [5959](#) (once approved)
Intended status: Standards Track
Expires: August 10, 2011

S. Turner
IECA
February 11, 2011

Elliptic Curve Algorithms for Cryptographic Message Syntax (CMS)
Asymmetric Key Package Content Type
draft-turner-akf-algs-update-03.txt

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 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 <http://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 August 10, 2011.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft EC Algorithms for CMS Asymmetric Key Packages 2011-02-11

This document is subject to [BCP 78](http://trustee.ietf.org/license-info) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://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.

[1.](#) Introduction

[RFC5959] describes conventions necessary to protect the AsymmetricKeyPackage content type [RFC5958] with Cryptographic Message Syntax (CMS) protecting 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 co-factor) ECDH [[RFC6090](#)] [RFC5753] MAY be supported.

Turner

Expires 2011-08-10

[Page 2]

Internet-Draft EC Algorithms for CMS Asymmetric Key Packages 2011-02-11

[3.](#) Public Key Sizes

The easiest way to implement the 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.](#) IANA Considerations

None. Please remove this section prior to publication as an RFC.

[6.](#) Normative References

[6.1.](#) 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)", [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] Turners, S., "Asymmetric Key Packages", [RFC 5958](#), August 2010.

[RFC5959] Turners, S., "Asymmetric Key Packages", [RFC 5959](#), August 2010.

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

Turner

Expires 2011-08-10

[Page 3]

Internet-DraftEC Algorithms for CMS Asymmetric Key Packages 2011-02-11

[6.2.](#) Informative References

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

Authors' Addresses

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

EMail: turners@ieca.com

Turner

Expires 2011-08-10

[Page 4]