Internet-Draft
Intended status: Standards Track
Expires: 20 October 2016

R. Housley
Vigil Security

18 April 2016

Use of EdDSA Signatures in the Cryptographic Message Syntax (CMS)

<draft-housley-cms-eddsa-signatures-00.txt>

Abstract

This document describes the conventions for using Edwards-curve Digital Signature Algorithm (EdDSA) in the Cryptographic Message Syntax (CMS). The conventions for Ed25519, Ed25519ph, Ed448, and Ed448ph are described.

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 20 October 2016.

Copyright Notice

Copyright (c) 2016 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 (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

This document specifies the conventions for using the Edwards-curve Digital Signature Algorithm (EdDSA) [EDDSA] with the Cryptographic Message Syntax [CMS] signed-data content type. The conventions for two recommended elliptic curves are specified, Ed25519 and Ed448. For each curve, two modes are defined, the PureEdDSA mode without pre-hashing (Ed25519 and Ed448), and the HashEdDSA mode with pre-hashing (Ed25519ph and Ed448ph).

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [STDWORDS].

1.2. ASN.1

CMS values are generated using ASN.1 [X680], which uses the Basic Encoding Rules (BER) and the Distinguished Encoding Rules (DER) [X690].

2. EdDSA Signature Algorithm

The Edwards-curve Digital Signature Algorithm (EdDSA) {EDDSA] is a variant of Schnorr's signature system with (possibly twisted) Edwards curves. Ed25519 is intended to operate at around the 128-bit security level, and Ed448 at around the 224-bit security level.

A message digest is computed over the data to be signed using EdDSA, and then a private key operation is performed to generate the signature value. As described in Section 3.3 of [EDDSA], the signature value is the opaque value ENC(R) || ENC(S). As described in Section 5.3 of [CMS], the signature value is ASN.1 encoded as an OCTET STRING and included in the signature field of SignerInfo.

2.1. Certificate Identifiers

The EdDSA signature algorithm is defined in [EDDSA], and the conventions for encoding the public key are defined in [PKIXEDDSA].

The id-EdDSAPublicKey OID is used for identifying EdDSA public keys:

```
id-EdDSAPublicKey OBJECT IDENTIFIER ::= { 1 3 101 100 }
```

When the id-EdDSAPublicKey onject identifier is used, the AlgorithmIdentifier parameters field MUST contain EdDSAParameters to specify a particular set of EdDSA parameters:

```
EdDSAParameters ::= ENUMERATED {
  ed25519   (1),    -- PureEdDSA
  ed25519ph (2),    -- HashEdDSA
  ed448     (3),    -- PureEdDSA
  ed448ph   (4) }   -- HashEdDSA
```

2.2. Signature Identifiers

The algorithm identifier for EdDSA signatures is:

```
id-EdDSASignature OBJECT IDENTIFIER ::= { 1 3 101 101 }
```

When the id-EdDSASignature object identifier is used for a signature, the AlgorithmIdentifier parameters field MUST be absent.

3. Signed-data Conventions

digestAlgorithms SHOULD contain the one-way hash function used to compute the message digest on the eContent value.

The same one-way hash function SHOULD be used for computing the message digest on both the eContent and the signedAttributes value if signedAttributes are present.

signatureAlgorithm MUST contain id-EdDSASignature. The algorithm parameters field MUST be absent.

signature contains the single value resulting from the EdDSA signing operation.

4. Security Considerations

Implementations must protect the EdDSA private key. Compromise of the EdDSA private key may result in the ability to forge signatures.

The generation of EdDSA private key relies on random numbers. The use of inadequate pseudo-random number generators (PRNGs) to generate these values can result in little or no security. An attacker may find it much easier to reproduce the PRNG environment that produced the keys, searching the resulting small set of possibilities, rather than brute force searching the whole key space. The generation of quality random numbers is difficult. RFC 4086 [RANDOM] offers important guidance in this area.

Using the same private key for different algorithms has the potential of allowing an attacker to get extra information about the key. It is strongly suggested that the same key not be used with more than one EdDSA set of parameters.

When computing signatures, the same hash function should be used for all operations. This reduces the number of failure points in the signature process.

5. Normative References

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

[EDDSA] Josefsson, S. and I. Liusvaara, "Edwards-curve Digital Signature Algorithm (EdDSA)", draft-irtf-cfrg-eddsa-00, (work in progress), October 2015.

[PKIXEDDSA] Josefsson, S., "Using Curve25519 and Curve448 in PKIX", draft-ietf-curdle-pkix-eddsa-00, (work in progress), October 2015.

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

[X680] ITU-T, "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, 2002.

[X690] ITU-T, "Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, 2002.

6. Informative References

[RANDOM] Eastlake, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", RFC 4086, June 2005.

Author Address

Russ Housley
918 Spring Knoll Drive
Herndon, VA 20170
USA
housley@vigilsec.com