

IPSecME Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: October 7, 2017

Y. Nir  
Check Point  
April 5, 2017

Using Edwards-curve Digital Signature Algorithm (EdDSA) in the Internet  
Key Exchange (IKEv2)  
[draft-ietf-ipsecme-eddsa-02](#)

Abstract

This document describes the use of the Edwards-curve digital signature algorithm in the IKEv2 protocol.

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 October 7, 2017.

Copyright Notice

Copyright (c) 2017 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.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	Conventions Used in This Document . . . . .	<a href="#">3</a>
<a href="#">2.</a>	The "Identity" Hash Identifier . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Security Considerations . . . . .	<a href="#">3</a>
<a href="#">4.</a>	IANA Considerations . . . . .	<a href="#">3</a>
<a href="#">5.</a>	Normative References . . . . .	<a href="#">3</a>
<a href="#">Appendix A.</a>	ASN.1 Objects . . . . .	<a href="#">5</a>
<a href="#">A.1.</a>	ASN.1 Object for Ed25519 . . . . .	<a href="#">5</a>
<a href="#">A.2.</a>	ASN.1 Object for Ed448 . . . . .	<a href="#">5</a>
	Author's Address . . . . .	<a href="#">5</a>

## [1.](#) Introduction

The Internet Key Exchange protocol [[RFC7296](#)] can use arbitrary signature algorithms as described in [[RFC7427](#)]. The latter RFC defines the SIGNATURE\_HASH\_ALGORITHMS notification where each side of the IKE negotiation lists its supported hash algorithms. This assumes that all signature schemes involve a hashing phase followed by a signature phase. This made sense because most signature algorithms either cannot sign messages bigger than their key or truncate messages bigger than their key.

EdDSA ([[RFC8032](#)]) defines signature methods that do not require pre-hashing of the message. Unlike other methods, these accept arbitrary-sized messages, so no pre-hashing is required. These methods are called Ed25519 and Ed448, which respectively use the Edwards 25519 and the Edwards 448 ("Goldilocks") curves. Although that document also defines pre-hashed versions of these algorithm, those versions are not recommended for protocols where the entire to-be-signed message is available at once. See [section 8.5](#) or [RFC 8032](#) for that recommendation.

EdDSA defines the binary format of the signatures that should be used in the "Signature Value" field of the Authentication Data Format in [section 3](#). The CURDLE PKIX document ([[I.D-curdle-pkix](#)]) defines the object identifiers (OIDs) for these signature methods. For convenience, these OIDs are repeated in [Appendix A](#).

In order to signal within IKE that no hashing needs to be done, we define a new value has in the SIGNATURE\_HASH\_ALGORITHMS notification, one that indicates that no hashing is performed.



### **1.1. Conventions Used in This Document**

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 [[RFC2119](#)].

## **2. The "Identity" Hash Identifier**

This document defines a new value called "Identity" (value is 5) in the hash algorithm registry for use in the SIGNATURE\_HASH\_ALGORITHMS notification. Inserting this new value into the notification indicates that the receiver supports at least one signature algorithm that accepts arbitrary-sized messages such as Ed25519 and Ed448.

Ed25519 and Ed448 are only defined with the Identity hash, and MUST NOT be sent to a receiver that has not indicated support for the "Identity" hash.

The pre-hashed versions of Ed25519 and Ed448 (Ed25519ph and Ed448ph respectively) SHOULD NOT be used in IKE.

## **3. Security Considerations**

The new "Identity" value is needed only for signature algorithms that accept an arbitrary-sized input. It MUST NOT be used if none of the supported algorithms has this property. On the other hand there is no good reason to pre-hash the inputs where the signature algorithm either does not require it or performs a hash internally. For this reason implementations SHOULD have the "Identity" value in the SIGNATURE\_HASH\_ALGORITHMS notification when they support EdDSA. Implementations SHOULD NOT have other hash algorithms in the notification if all signature algorithms have this property.

## **4. IANA Considerations**

IANA has assigned the value 5 for the algorithm with the name "Identity" in the "IKEv2 Hash Algorithms" registry with this draft as reference.

Upon publication of this document IANA is requested to update the entry with this document as reference.

## **5. 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, <<http://www.rfc-editor.org/info/rfc2119>>.



- [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, [RFC 7296](https://www.rfc-editor.org/info/rfc7296), DOI 10.17487/RFC7296, October 2014, <<http://www.rfc-editor.org/info/rfc7296>>.
- [RFC7427] Kivinen, T. and J. Snyder, "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)", [RFC 7427](https://www.rfc-editor.org/info/rfc7427), DOI 10.17487/RFC7427, January 2015, <<http://www.rfc-editor.org/info/rfc7427>>.
- [RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", [RFC 8032](https://www.rfc-editor.org/info/rfc8032), DOI 10.17487/RFC8032, January 2017, <<http://www.rfc-editor.org/info/rfc8032>>.
- [I.D-curdle-pkix]  
Josefsson, S. and J. Schaad, "Algorithm Identifiers for Ed25519, Ed25519ph, Ed448, Ed448ph, X25519 and X448 for use in the Internet X.509 Public Key Infrastructure", November 2016, <<https://tools.ietf.org/html/draft-ietf-curdle-pkix-03>>.



## [Appendix A](#). ASN.1 Objects

The normative reference for the ASN.1 objects for Ed25519 and Ed448 is in [[I.D-curdle-pkix](#)]. They are repeated below for convenience.

### [A.1](#). ASN.1 Object for Ed25519

id-Ed25519 OBJECT IDENTIFIER ::= { 1.3.101.112 }

Parameters are absent. Length is 7 bytes.

Binary encoding: 3005 0603 2B65 70

### [A.2](#). ASN.1 Object for Ed448

id-Ed448 OBJECT IDENTIFIER ::= { 1.3.101.113 }

Parameters are absent. Length is 7 bytes.

Binary encoding: 3005 0603 2B65 71

#### Author's Address

Yoav Nir  
Check Point Software Technologies Ltd.  
5 Hasolelim st.  
Tel Aviv 6789735  
Israel

EMail: [ynir.ietf@gmail.com](mailto:ynir.ietf@gmail.com)



