Using Edwards-curve Digital Signature Algorithm (EdDSA) in the Internet Key Exchange (IKEv2)
draft-nir-ipsecme-eddsa-01

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 December 13, 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.
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 ([I.D-eddsa]) 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.

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 "EdDSA, Ed25519, Ed448, Curve25519 and Curve448 for X.509" 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 TBA by 
IANA) 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 is requested to assign a new value from the "IKEv2 Hash 
Algorithms" registry with name "Identity" and 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, 


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-Curve25519 OBJECT IDENTIFIER ::= { 1.3.101.110 }

Parameters are absent.
Binary encoding: TBA

A.2. ASN.1 Object for Ed448

id-Curve448 OBJECT IDENTIFIER ::= { 1.3.101.111 }

Parameters are absent.
Binary encoding: TBA

Author’s Address

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

EMail: ynir.ietf@gmail.com