Workgroup: IPSECME
Internet-Draft:
draft-moskowitz-ipsecme-ipseckey-eddsa-03
Published: 7 November 2022
Intended Status: Standards Track
Expires: 11 May 2023
Authors: R. Moskowitz   T. Kivinen   M. Richardson
         HTT Consulting   Sandelman

EdDSA value for IPSECKEY

Abstract

This document assigns a value for EdDSA Public Keys to the IPSECKEY IANA registry.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction
2. IPSECKEY support for EdDSA
3. IANA Considerations
   3.1. IANA IPSECKEY Registry Update
4. Security Considerations
5. References
   5.1. Normative References
   5.2. Informative References
Appendix A. IPSECKEY EdDSA example
Acknowledgments
Authors' Addresses

1. Introduction

IPSECKEY [RFC4025) is a resource record (RR) for the Domain Name System (DNS) that is used to store public keys for use in IP security (IPsec) systems. The IPSECKEY RR relies on the IPSECKEY Algorithm Type Field registry [IANA-IPSECKEY] to enumerate the permissible formats for the public keys.

This documents adds support for Edwards-Curve Digital Security Algorithm (EdDSA) public keys in the format defined in [RFC8080] to the IPSECKEY RR.

2. IPSECKEY support for EdDSA

Use of an EdDSA public key encoded in the format specified in [RFC8080] in an IPSECKEY RR is indicated as follows:

Value	Description
TBD1 (suggested value 4)	An EdDSA Public Key is present, in the format defined in [RFC8080]

3. IANA Considerations

3.1. IANA IPSECKEY Registry Update

This document requests IANA to update the "Description" field in existing entries of the "Algorithm Type Field" subregistry of the "IPSECKEY Resource Record Parameters" [IANA-IPSECKEY] to explicitly state that is for "Public" keys:

Value	Description	Format description	Reference
0	No key is present		[RFC4025]
1	A DSA Public Key	[RFC2536], Sec. 2	[RFC4025]
2	A RSA Public Key	[RFC3110], Sec. 2	[RFC4025]
3	An ECDSA Public Key	[RFC6605], Sec. 4	[RFC4025]

Further, this document requests IANA to make the following addition to the "IPSECKEY Resource Record Parameters" [IANA-IPSECKEY] registry:

IPSECKEY:

This document defines the new IPSECKEY value TBD1 (suggested: 4) (Section 2) in the "Algorithm Type Field" subregistry of the "IPSECKEY Resource Record Parameters" registry.

Value	Description	Format description	Reference
TBD1	An EdDSA Public Key	[RFC8080], Sec. 3	[ThisRFC]

4. Security Considerations

No new issues than [RFC4025] describes.

5. References

5.1. Normative References

[IANA-IPSECKEY] IANA, "IPSECKEY Resource Record Parameters", <https://www.iana.org/assignments/ipseckey-rr-parameters/ipseckey-rr-parameters.xhtml>.

[RFC8080] Sury, O. and R. Edmonds, "Edwards-Curve Digital Security Algorithm (EdDSA) for DNSSEC", RFC 8080, DOI 10.17487/RFC8080, February 2017, <https://www.rfc-editor.org/info/rfc8080>.

5.2. Informative References

[RFC4025] Richardson, M., "A Method for Storing IPsec Keying Material in DNS", RFC 4025, DOI 10.17487/RFC4025, March 2005, <https://www.rfc-editor.org/info/rfc4025>.

Appendix A. IPSECKEY EdDSA example

The following is an example of an IPSECKEY RR with an EdDSA public key base64 encode with no gateway:

```
foo.example.com IN IPSECKEY
(10 0 4 . 3WTXgUvpn1RlCXnm80gGY2LZ/ErUUEZtZ33IDi8yfhM= )
```

The associated EdDSA private key (in hex):

```
c7be71a45cbf87785f639dc4fd1c82637c21b5e02488939976ece32b9268d0b7
```

Acknowledgments

Thanks to Security Area director, Paul Wouters, for initial review. And Security Area director, Roman Danyliw, for final reviews and draft shepherding.

Authors' Addresses

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
United States of America

Email: rgm@labs.htt-consult.com

Tero Kivinen

Email: kivinen@iki.fi

Michael C. Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca
URI: http://www.sandelman.ca/