Workgroup: IPSECME
Internet-Draft:
draft-moskowitz-ipsecme-ipseckey-eddsa-01
Published: 5 August 2022
Intended Status: Standards Track
Expires: 6 February 2023
Authors: R. Moskowitz T. Kivinen
HTT Consulting

EdDSA value for IPSECKEY

Abstract

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

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 https://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 6 February 2023.

Copyright Notice

Table of Contents

1. Introduction

The IPSECKEY IANA Registry specifically enumerates the various Algorithm Types used. This document adds support for the EdDSA algorithm's Public Keys in IPSECKEY.

The IPSECKEY RR [RFC4025] defines the 'Algorithm Type' for specifying the PK Algorithm. Herein we are adding the EdDSA algorithm.

2. Terms and Definitions

2.1. Requirements 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. IPSECKEY support for EdDSA

The new EdDSA value uses [RFC8080] for the IPSECKEY encoding:

Value	Description
TBD2 (suggested value 4)	An EdDSA Public key is present, in the format defined in [RFC8080]

4. IANA Considerations

4.1. IANA IPSECKEY Registry Update

This document requests IANA to make the following change to the "IPSECKEY Resource Record Parameters" [IANA-IPSECKEY] registry:

IPSECKEY:
This document defines the new IPSECKEY value TBD2 (suggested: 4) (Section 3) in the "Algorithm Type Field" subregistry of the "IPSECKEY Resource Record Parameters" registry.

Value	Description	Reference
TBD2 (suggested value 4)	An EdDSA Public key is present, in the format defined in [RFC8080]	[This]

5. Security Considerations

TBD

6. References

6.1. 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, <https://www.rfc-editor.org/info/rfc2119>.

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

6.2. Informative 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>.

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
(a 0 4 3WTXgUvpn1RlCXnm80gGY2LZ/ErUUEZtZ33IDi8yfhM= )
```

The associated EdDSA private key (in hex):

```
c7be71a45cbf87785f639dc4fd1c82637c21b5e02488939976ece32b9268d0b7
```

Acknowledgments

Thanks to Security Area director, Paul Wouters, for initial review.

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