Internet Engineering Task Force (IETF)
Request for Comments: 9373
Category: Standards Track
ISSN: 2070-1721

R. Moskowitz
HTT Consulting
T. Kivinen
M. Richardson
Sandelman

March 2023

EdDSA Value for IPSECKEY

Abstract

This document assigns a value for Edwards-Curve Digital Signature Algorithm (EdDSA) Public Keys to the "IPSECKEY Resource Record Parameters" registry.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9373.

Table of Contents

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 document 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

When using the EdDSA public key in the IPSECKEY RR, the value 4 is used as an algorithm and the public key is formatted as specified in "Edwards-Curve Digital Security Algorithm (EdDSA) for DNSSEC" (Section 3 of [RFC8080]).

Value	Description	Format Description	Reference
4	An EdDSA Public Key	[RFC8080], Section 3	This RFC

Table 1

3. IANA Considerations

3.1. Update to the IANA IPSECKEY Registry

3.1.1. Reformat the Algorithm Type Field Registry

Per this document, IANA has added the "Format Description" field to the "Algorithm Type Field" registry of the "IPSECKEY Resource Record Parameters" [IANA-IPSECKEY]. In addition, IANA has updated the "Description" field in existing entries of that registry to explicitly state that they are for "Public" keys:

Value	Description	Format Description	Reference
0	No Public key is present		[RFC4025]
1	A DSA Public Key	[RFC2536], Section 2	[RFC4025]
2	An RSA Public Key	[RFC3110], Section 2	[RFC4025]

3	An ECDSA Public Key	[RFC6605], Section 4	[RFC8005]

Table 2

IANA added a reference to this document to the "Algorithm Type Field" registry.

3.1.2. Add to the Algorithm Type Field Registry

Further, IANA has made the following addition to the "Algorithm Type Field" registry within the "IPSECKEY Resource Record Parameters" [IANA-IPSECKEY]:

Value	Description	Format Description	Reference
4	An EdDSA Public Key	[RFC8080], Section 3	This RFC

Table 3

4. Security Considerations

The security considerations discussed in [RFC4025] apply. This document does not introduce any new security considerations.

5. References

5.1. Normative References

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

[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

[RFC2536] Eastlake 3rd, D., "DSA KEYs and SIGs in the Domain Name System (DNS)", RFC 2536, DOI 10.17487/RFC2536, March 1999, <https://www.rfc-editor.org/info/rfc2536>.

[RFC3110] Eastlake 3rd, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, DOI 10.17487/RFC3110, May 2001, <https://www.rfc-editor.org/info/rfc3110>.

[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>.

[RFC6605] Hoffman, P. and W.C.A. Wijngaards, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC", RFC 6605, DOI 10.17487/RFC6605, April 2012, <https://www.rfc-editor.org/info/rfc6605>.

[RFC8005] Laganier, J., "Host Identity Protocol (HIP) Domain Name System (DNS) Extension", RFC 8005, DOI 10.17487/RFC8005, October 2016, <https://www.rfc-editor.org/info/rfc8005>.

Appendix A. IPSECKEY EdDSA Example

The following is an example of an IPSECKEY RR with no gateway, and an EdDSA public key. It uses the IPSECKEY presentation format which is base64.

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

The associated EdDSA private key (in hex) is as follows:

```
c7be71a45cbf87785f639dc4fd1c82637c21b5e02488939976ece32b9268d0b7
```

Acknowledgments

Thanks to the Security Area Director, Paul Wouters, for his initial review. Also, thanks to Security Area Director, Roman Danyliw, for his final reviews and document 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: https://www.sandelman.ca/