RFC 9373
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.

Copyright Notice
Copyright (c) 2023 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 (https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.
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]).
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:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Format Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Public key is present</td>
<td></td>
<td>[RFC4025]</td>
</tr>
<tr>
<td>1</td>
<td>A DSA Public Key</td>
<td>[RFC2536], Section 2</td>
<td>[RFC4025]</td>
</tr>
<tr>
<td>2</td>
<td>An RSA Public Key</td>
<td>[RFC3110], Section 2</td>
<td>[RFC4025]</td>
</tr>
<tr>
<td>3</td>
<td>An ECDSA Public Key</td>
<td>[RFC6605], Section 4</td>
<td>[RFC8005]</td>
</tr>
</tbody>
</table>

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]:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Format Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>An EdDSA Public Key</td>
<td>[RFC8080], Section 3</td>
<td>This RFC</td>
</tr>
</tbody>
</table>

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


5.2. Informative References


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. 3WTXgUvpn1R1CXnm80gGY2LZ/ErUEZtZ33IDi8yfhM=)
```

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