INTERNET-DRAFT
Intended Status: Informational
Expires: March 4, 2015

S. Moonesamy

August 31, 2014

Using ED25519 in SSHFP Resource Records
draft-moonesamy-sshfp-ed25519-02

Abstract

The Ed25519 signature algorithm has been implemented in OpenSSH. This document updates the IANA "SSHFP RR Types for public key algorithms" registry by adding an algorithm number for Ed25519.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

1. Introduction

The Ed25519 [Ed25519] signature algorithm, specifically Ed25519-SHA-512, has been implemented in OpenSSH. RFC 4255 [RFC4255] defines a DNS resource record, "SSHFP", which can be used to publish a fingerprint of the SSH server public key in the DNS. This document updates the IANA "SSHFP RR Types for public key algorithms" registry by adding an algorithm number for Ed25519 [Ed25519].

2. ED25519 Public Key with SHA-256 Fingerprint

The SSHFP Resource Record for the ED25519 public key with SHA-256 fingerprint [FIPS180-4] would, for example, be:

```
ssh.example.com IN SSHFP [TBD] 2 ( a87f1b687ac0e57d2a081a2f2826723
                                   34d90ed316d2b818ca9580ea384d924
                                   01 )
```

[RFC Editor Note: Please replace TBD with the value assigned by IANA.]

The following body of the public key file was used as input to generate the above fingerprint:

```
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIGPKSUTyz1HwHReFVvD5obVsALAgJRNarH4TRpNePnAS
```

The opaque octet string output produced is placed as-is in the RDATA fingerprint field.

3. Security Considerations

The overall security of using SSHFP for SSH host key verification is dependent on the security policies of the SSH host administrator and DNS zone administrator (in transferring the fingerprint), detailed

aspects of how verification is done in the SSH implementation, and in the client's diligence in accessing the DNS in a secure manner. Please refer to RFC 4255 [RFC4255] for a discussion of the security considerations.

4. IANA Considerations

IANA is requested to add the following entry to the "SSHFP RR Types for public key algorithms" registry:

Value	Description	Reference
[TBD]	ED25519	[RFCXXXX]

[RFC Editor Note: Please replace TBD with the value assigned by IANA and RFCXXXX to refer to this document.]

5. Acknowledgements

Some of the text in this document was written by Ondrej Sury. The author would like to thank Damien Miller, Yoav Nir, and Paul Wouters for their feedback. Rene Struik provided advice about the usage of Ed25519. Stephen Farrell, as Security Area Director, reviewed the code point request.

6. References

6.1. Normative References

[RFC4255] Schlyter, J. and W. Griffin, "Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints", RFC 4255, January 2006.

6.2. Informative References

[Ed25519] Bernstein, D. J., Lange T., Schwabe P., Yang B-Y., High-Speed High-Security Signatures, Journal of Cryptographic Engineering, Vol. 2, September 26, 2011

[FIPS180-4] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-4, March 2012, <http://csrc.nist.gov/publications/fips/fips180-4/fips180-4_final.pdf>.

Appendix A: Changes

[RFC Editor Note: Please remove this appendix]

A.1 Changes since version 00

- Text about usage policy removed from Section 2
- SHA-1 Fingerprint removed

A.2 Changes since version 01

- Appendix B lists the implementation status of the Ed25519

signature algorithm.

- Added an example in Section 2 of the public key file used to generate the fingerprint.

Appendix B: Implementation Status

[RFC Editor Note: Please remove this appendix]

This section records the status of known implementations of the signature algorithm referenced by this specification at the time of posting of this Internet-Draft.

The Ed25519 signature algorithm, specifically Ed25519-SHA-512, has been implemented in OpenSSH (http://www.openssh.org) and it is featured in production version (http://www.openssh.com/txt/release-6.5). The software is distributed under a BSD license.

The Ed25519 signature algorithm has also been implemented in Tera Term (http://sourceforge.jp/ticket/browse.php?group_id=1412&tid=33263). The software is distributed under a BSD license.

Authors' Addresses

S. Moonesamy
76, Ylang Ylang Avenue
Quatres Bornes
Mauritius

Email: sm+ietf@elandsys.com