Internet Engineering Task Force
Internet-Draft
Updates: 4250 (if approved)
Intended status: Standards Track
Expires: February 7, 2018

B. Harris

L. Velvindron
Hackers.mu
August 6, 2017

Ed25519 public key algorithm for the Secure Shell (SSH) protocol
draft-ietf-curdle-ssh-ed25519-01

Abstract

This document describes the use of the Ed25519 digital signature algorithm in the Secure Shell (SSH) protocol.

Status of This Memo

Copyright Notice

1. Introduction

Secure Shell (SSH) [RFC4251] is a secure remote-login protocol. It provides for an extensible variety of public key algorithms for identifying servers and users to one another. Ed25519 [RFC8032] is a digital signature system. OpenSSH 6.5 [OpenSSH-6.5] introduced support for using Ed25519 for server and user authentication. Compatible support for Ed25519 has since been added to other SSH implementations.

This document describes the method implemented by OpenSSH and others, and formalizes its use of the name "ssh-ed25519".

[TO BE REMOVED: Please send comments on this draft to curdle@ietf.org.]

2. Conventions Used in This Document

The descriptions of key and signature formats use the notation introduced in [RFC4251], Section 3 [RFC4251] and the string data type from [RFC4251], Section 5 [RFC4251].

3. Public Key Algorithm

This document describes a public key algorithm for use with SSH in accordance with [RFC4253], Section 6.6 [RFC4253]. The name of the algorithm is "ssh-ed25519". This algorithm only supports signing and not encryption.

4. Public Key Format

The "ssh-ed25519" key format has the following encoding:

```
string    "ssh-ed25519"
string    key
```

Here 'key' is the 32-octet public key described by [RFC8032], Section 5.1.5 [RFC8032].

5. Signature Algorithm

Signatures are generated according to the procedure in [RFC8032], Section 5.1.6 [RFC8032].

6. Signature Format

The "ssh-ed25519" key format has the following encoding:

```
string    "ssh-ed25519"
string    signature
```

Here 'signature' is the 64-octet signature produced in accordance with [RFC8032], Section 5.1.6 [RFC8032].

7. Verification Algorithm

Signatures are verified according to the procedure in [RFC8032], Section 5.1.7 [RFC8032].

8. SSHFP DNS resource records

The generation of SSHFP resource records for "ssh-ed25519" keys is described in [RFC7479].

9. IANA Considerations

This document augments the Public Key Algorithm Names in [RFC4250], Section 4.6.2 [RFC4250].

IANA is requested to add to the Public Key Algorithm Names registry [IANA-PKA] with the following entry:

Public Key Algorithm Name	Reference
ssh-ed25519	This Draft

[TO BE REMOVED: This registration should take place at the following location: <http://www.iana.org/assignments/ssh-parameters/ssh-parameters.xhtml#ssh-parameters-19>]

10. Security Considerations

The security considerations in [RFC4251], Section 9 [RFC4251] apply to all SSH implementations, including those using Ed25519.

The security considerations in [RFC8032], Section 8 [RFC8032] apply to all uses of Ed25519, including those in SSH.

11. Acknowledgements

The OpenSSH implementation of Ed25519 in SSH was written by Markus Friedl.

12. References

12.1. Normative References

[RFC4250] Lehtinen, S. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, DOI 10.17487/RFC4250, January 2006, <http://www.rfc-editor.org/info/rfc4250>.

[RFC4251] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture", RFC 4251, DOI 10.17487/RFC4251, January 2006, <http://www.rfc-editor.org/info/rfc4251>.

[RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, DOI 10.17487/RFC4253, January 2006, <http://www.rfc-editor.org/info/rfc4253>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <http://www.rfc-editor.org/info/rfc8032>.

12.2. Informative References

[IANA-PKA]
Internet Assigned Numbers Authority (IANA), "Secure Shell (SSH) Protocol Parameters: Public Key Algorithm Names", May 2017, <http://www.iana.org/assignments/ssh-parameters/ssh-parameters.xhtml#ssh-parameters-19>.

[OpenSSH-6.5]
Friedl, M., Provos, N., de Raadt, T., Steves, K., Miller, D., Tucker, D., Rice, T., and B. Lindstrom, "OpenSSH 6.5 release notes", January 2014, <http://www.openssh.com/txt/release-6.5>.

[RFC7479] Moonesamy, S., "Using Ed25519 in SSHFP Resource Records", RFC 7479, DOI 10.17487/RFC7479, March 2015, <http://www.rfc-editor.org/info/rfc7479>.

Authors' Addresses

Ben Harris
2A Eachard Road
CAMBRIDGE CB3 0HY
UNITED KINGDOM

Email: bjh21@bjh21.me.uk

Loganaden Velvindron
Hackers.mu
88, Avenue De Plevitz
Roches Brunes
Mauritius

Email: logan@hackers.mu