Internet Engineering Task Force (IETF)
Request for Comments: 8709
Updates: 4253
Category: Standards Track
ISSN: 2070-1721

B. Harris

L. Velvindron
cyberstorm.mu

February 2020

Ed25519 and Ed448 Public Key Algorithms for the Secure Shell (SSH) Protocol

Abstract

This document describes the use of the Ed25519 and Ed448 digital signature algorithms in the Secure Shell (SSH) protocol. Accordingly, this RFC updates RFC 4253.

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/rfc8709.

Table of Contents

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 and was then followed by other SSH implementations.

This document describes the method implemented by OpenSSH and others and formalizes the use of the name "ssh-ed25519". Additionally, this document describes the use of Ed448 and formalizes the use of the name "ssh-ed448".

2. Conventions Used in This Document

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

2.1. Requirements Language

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. Public Key Algorithm

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

Additionally, this document describes another public key algorithm. The name of the algorithm is "ssh-ed448". This algorithm only supports signing and not encryption.

Standard implementations of SSH SHOULD implement these signature algorithms.

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 in [RFC8032], Section 5.1.5.

The "ssh-ed448" key format has the following encoding:

```
string  "ssh-ed448"

string  key
```

Here, 'key' is the 57-octet public key described in [RFC8032], Section 5.2.5.

5. Signature Algorithm

Signatures are generated according to the procedure in Sections 5.1.6 and 5.2.6 of [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.

The "ssh-ed448" key format has the following encoding:

```
string  "ssh-ed448"

string  signature
```

Here, 'signature' is the 114-octet signature produced in accordance with [RFC8032], Section 5.2.6.

7. Verification Algorithm

Ed25519 signatures are verified according to the procedure in [RFC8032], Section 5.1.7.

Ed448 signatures are verified according to the procedure in [RFC8032], Section 5.2.7.

8. SSHFP DNS Resource Records

Usage and generation of the SSHFP DNS resource record is described in [RFC4255]. The generation of SSHFP resource records for "ssh-ed25519" keys is described in [RFC7479]. This section illustrates the generation of SSHFP resource records for "ssh-ed448" keys, and this document also specifies the corresponding Ed448 code point to "SSHFP RR Types for public key algorithms" in the "DNS SSHFP Resource Record Parameters" IANA registry [IANA-SSHFP].

The generation of SSHFP resource records for "ssh-ed448" keys is described as follows.

The encoding of Ed448 public keys is described in [ED448]. In brief, an Ed448 public key is a 57-octet value representing a 455-bit y-coordinate of an elliptic curve point, and a sign bit indicating the corresponding x-coordinate.

The SSHFP Resource Record for the Ed448 public key with SHA-256 fingerprint would, for example, be:

```
example.com. IN SSHFP 6 2 ( a87f1b687ac0e57d2a081a2f2826723
                            34d90ed316d2b818ca9580ea384d924
                            01 )
```

The '2' here indicates SHA-256 [RFC6594].

9. IANA Considerations

This document augments the Public Key Algorithm Names in [RFC4250], Section 4.11.3.

IANA has added the following entry to "Public Key Algorithm Names" in the "Secure Shell (SSH) Protocol Parameters" registry [IANA-SSH]:

Public Key Algorithm Name	Reference
ssh-ed25519	RFC 8709
ssh-ed448	RFC 8709

Table 1

IANA has added the following entry to "SSHFP RR Types for public key algorithms" in the "DNS SSHFP Resource Record Parameters" registry [IANA-SSHFP]:

Value	Description	Reference
6	Ed448	RFC 8709

Table 2

10. Security Considerations

The security considerations in [RFC4251], Section 9 apply to all SSH implementations, including those using Ed25519 and Ed448.

The security considerations in [RFC8032], Section 8 and [RFC7479], Section 3 apply to all uses of Ed25519 and Ed448, including those in SSH.

11. References

11.1. 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>.

[RFC4250] Lehtinen, S. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, DOI 10.17487/RFC4250, January 2006, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc4253>.

[RFC4255] Schlyter, J. and W. Griffin, "Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints", RFC 4255, DOI 10.17487/RFC4255, January 2006, <https://www.rfc-editor.org/info/rfc4255>.

[RFC6594] Sury, O., "Use of the SHA-256 Algorithm with RSA, Digital Signature Algorithm (DSA), and Elliptic Curve DSA (ECDSA) in SSHFP Resource Records", RFC 6594, DOI 10.17487/RFC6594, April 2012, <https://www.rfc-editor.org/info/rfc6594>.

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

[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>.

11.2. Informative References

[ED448] Hamburg, M., "Ed448-Goldilocks, a new elliptic curve", January 2015, <https://eprint.iacr.org/2015/625.pdf>.

[IANA-SSH] IANA, "Secure Shell (SSH) Protocol Parameters", <https://www.iana.org/assignments/ssh-parameters>.

[IANA-SSHFP] IANA, "DNS SSHFP Resource Record Parameters", <https://www.iana.org/assignments/dns-sshfp-rr-parameters>.

[OpenSSH-6.5]

Friedl, M., Provos, N., de Raadt, T., Steves, K., Miller, D., Tucker, D., McIntyre, J., 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, <https://www.rfc-editor.org/info/rfc7479>.

Acknowledgements

The OpenSSH implementation of Ed25519 in SSH was written by Markus Friedl. We are also grateful to Mark Baushke, Benjamin Kaduk, and Daniel Migault for their comments.

Authors' Addresses

Ben Harris
2A Eachard Road
Cambridge
CB3 0HY
United Kingdom

Email: bjh21@bjh21.me.uk

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

Email: logan@cyberstorm.mu