Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 8, 2015

B. Harris
June 6, 2015

Ed25519 public key algorithm for the Secure Shell (SSH) protocol draft-bjh21-ssh-ed25519-00

Abstract

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

Editorial Note

Comments on this draft are welcomed and should be sent to the author.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on December 8, 2015.

Copyright Notice

Copyright (c) 2015 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 (http://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 Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

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 [I-D.josefsson-eddsa-ed25519] is a digital signature system. OpenSSH 6.5 [OpenSSH-6.5] introduced support for using Ed25519 for server and user authentication. This document describes the method implemented by OpenSSH and formalizes its use of the name "ssh-ed25519".

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.

3. Public Key Algorithm

This document describes a public key algorithm for use with SSH in accordance with [RFC4253] section 6.6. 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 [I-D.josefsson-eddsa-ed25519] section 5.5.

5. Signature Algorithm

Signatures are generated according to the procedure in [I-D.josefsson-eddsa-ed25519] section 5.6.

6. Signature format

The corresponding signature format is:

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

Here 'signature' is the 64-octet signature produced in accordance with [I-D.josefsson-eddsa-ed25519], Section 5.6.

7. Verification Algorithm

Signatures are verified according to the procedure in [I-D.josefsson-eddsa-ed25519], Section 5.7.

8. SSHFP DNS resource records

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

9. IANA Considerations

IANA is requested to assign the Public Key Algorithm name "ssh-ed25519" in accordance with [RFC4250], Section 4.11.3:

Public Key Algorithm Name	Reference
ssh-ed25519	[RFCXXXX]

[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 section 9 of [RFC4251] apply to all SSH implementations, including those using Ed25519.

The security considerations in section 9 of [I-D.josefsson-eddsa-ed25519] 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, "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, January 2006.

[RFC4251] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

[RFC4253] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, January 2006.

[I-D.josefsson-eddsa-ed25519] Josefsson, S. and N. Moller, "EdDSA and Ed25519", draft-josefsson-eddsa-ed25519-03 (work in progress), May 2015.

12.2. Informative References

[RFC7479] Moonesamy, S., "Using Ed25519 in SSHFP Resource Records", RFC 7479, March 2015.

[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>.

Author's Address

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

Email: bjh21@bjh21.me.uk