Abstract

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

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 February 2, 2016.

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. 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".

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

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:

```plaintext
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:
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 4.6.2:

<table>
<thead>
<tr>
<th>Public Key Algorithm Name Reference</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh-ed25519</td>
<td>[RFCXXXX]</td>
</tr>
</tbody>
</table>

[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 apply to all SSH implementations, including those using Ed25519.

The security considerations in [I-D.josefsson-eddsa-ed25519], Section 9 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


12.2. Informative References


Author’s Address

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

Email: bjh21@bjh21.me.uk