

INTERNET-DRAFT  
[draft-ietf-secsh-fingerprint-00.txt](#)  
Expires in six months

Markus Friedl  
The OpenBSD Project  
March 2002

## SSH Fingerprint Format

### Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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/ietf/lid-abstracts.txt>

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

Distribution of this memo is unlimited.

### Abstract

This document formally documents the fingerprint format in use for verifying public keys from SSH clients and servers.

### Introduction

The security of the SSH protocols relies on the verification of public host keys. Since public keys tend to be very large, it is difficult for a human to verify an entire host key. Even with a PKI in place, it is useful to have a standard for exchanging short fingerprints of public keys.

This document formally describes the simple key fingerprint format.

---

INTERNET-DRAFT

July 2000

## Fingerprint Format

The fingerprint of a public key consists of the output of the MD5 message-digest algorithm [[RFC-1321](#)]. The input to the algorithm is the public key blob as described in [[SSH-TRANS](#)]. The output of the algorithm is presented to the user as a sequence of 16 octets printed as hexadecimal with lowercase letters and separated by colons.

For example: "c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87"

## References

[SSH-TRANS] Ylonen, T., et al: "SSH Transport Layer Protocol", Internet Draft, [draft-secsh-transport-14.txt](#)

[RFC-1321] R. Rivest: "The MD5 Message-Digest Algorithm", April 1992.

[RFC-2026] S. Bradner: "The Internet Standards Process -- Revision 3", October 1996.

## Author's Address:

Markus Friedl  
markus@openbsd.org  
Munich, Germany

Friedl

[Page 2]