Secure Shell Working Group
Internet-Draft
Expires: January 30, 2004

J. Galbraith
VanDyke Software
R. Thayer
The Tillerman Group
August 1, 2003

SSH Public Key File Format
draft-ietf-secsh-publickeyfile-04.txt

Status of this Memo

This Internet-Draft will expire on January 30, 2004.

Copyright Notice

Abstract

This document formally documents the existing public key file format in use for exchanging public keys between different SSH implementations.

Table of Contents

1. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [4].

2. Introduction

In order to use public key authentication, public keys must be exchanged between client and server. This document formally describes the existing public key file format, with few exceptions.

Where this document departs from current practice, it also suggests a mechanism for backwards compatibility.

3. Key File Format

SSH implementations must share public key files between the client and the server in order to interoperate.

A key file is a text file, containing a sequence of lines. Each line in the file MUST NOT be longer than 72 bytes.

3.1 Line termination Characters

In order to achieve the goal of being able to exchange public key files between servers, implementations are REQUIRED to read files using any of the common line termination sequence, <CR>, <LF> or <CR><LF>.

Implementations may generate files using which ever line termination convention is most convenient

3.2 Begin and end markers

The first line of a conforming key file MUST be a begin marker, which is the literal text:

---- BEGIN SSH2 PUBLIC KEY ----

The last line of a conforming key file MUST be a end marker, which is the literal text:

---- END SSH2 PUBLIC KEY ----

3.3 Key File Header

The key file header section consists of multiple RFC822 - style header fields. Each field is a line of the following format:

Header-tag ':' ' ' Header-value

The Header-tag MUST NOT be more than 64 bytes. The Header-value MUST NOT be more than 1024 bytes. Each line in the header MUST NOT be more than 72 bytes.

A line is continued if the last character in the line is a '\'. If the last character of a line is a '\', then the logical contents of the line is formed by removing the '\' and appending the contents of the next line.

The Header-tag MUST be US-ASCII. The Header-value MUST be encoded in UTF-8. [2]

A line that is not a continuation line that has no ':' in it is assumed to be the first line of the base 64 encoded body (Section 8)

Compliant implementations MUST ignore unrecognized header fields. Implementations SHOULD preserve unrecognized header fields when manipulating the key file.

Existing implementations may not correctly handle unrecognized fields. During a transition period, implementations SHOULD generate key file headers that contain only a Subject field followed by a Comment field.

3.3.1 Subject Header

This field currently is used to store the login-name that the key was generated under. For example:

Subject: user

3.3.2 Comment Header

Contain a user specified comment which will be displayed when using the key.

It is suggested that this field default to user@hostname for the user and machine used to generate the key. For example:

Comment: user@mycompany.com

Currently, common practice is to quote the Header-value of the Comment, and some existing implementations fail if these quotes are omitted.

Compliant implementations MUST function correctly if the quotes are omitted.

During an interim period implementations MAY include the quotes. If the first and last characters of the Header-value are matching quotes, implementations SHOULD remove them before using the value.

3.4 Public Key File Body

The body of a public key file consists of the public key blob as described in the SSH transport draft [1], section 4.6, "Public Key Algorithms", encoded in base 64 as specified in RFC-2045, section 6.8, "Base64 Content-Transfer-Encoding". [5]

As with all other lines, each line in the body MUST NOT be longer

than 72 characters.

3.5 Examples

The following are some example public key files that are compliant:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "1024-bit RSA, converted from OpenSSH by galb@test1"
AAAAB3NzaC1yc2EAAAABIwAAAIEA1on8gxCGJJWSRT4uOrR13mUaUk0hRf4RzxSZ1zRbYY
Fw8pfGesIFoEuVth4HKyF8k1y4mRUnYHP1XNMNMJl1JcEArC2asV8sHf6zSPVffozZ5TT4
SfsUu/iKy9lUcCfXzwre4WWZSXXcPff+EHtWshahu3WzBdnGxm5Xoi89zcE=
---- END SSH2 PUBLIC KEY ----


---- BEGIN SSH2 PUBLIC KEY ----
Comment: DSA Public Key for use with MyIsp
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbETW6
ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdHYI14
Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5cvwHWTZ
DPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGfJ0/RHd+N
jB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAAvioUPkmdMc
0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACBAN7CY+KKv1gH
pRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HSn24VYtYtsMu74q
XviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5sY29ouezv4Xz2PuM
ch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----


---- BEGIN SSH2 PUBLIC KEY ----
Subject: galb
Comment: 1024-bit rsa, created by galb@shimi Mon Jan 15 08:31:24 2001
AAAAB3NzaC1yc2EAAAABJQAAAIEAiPWx6WM4lhHNedGfBpPJNPpZ7yKu+dnn1SJejgt459
6k6YjzGGphH2TUxwKzxcKDKKezwkpfnxPkSMkuEspGRt/aZZ9wa++Oi7Qkr8prgHc4soW6
NUlfDzpvZK2H5E7eQaSeP3SAwGmQKUFHCddNaP0L+hM7zhFNzjFvpaMgJw0=
---- END SSH2 PUBLIC KEY ----
```

4. Security Considerations

The file format described by this document provides no mechanism to verify the integrity or otherwise detect tampering with the data stored in such files. Given the potential of an adversarial tampering with this data, system-specific measures (e.g. Access Control Lists, UNIX permissions, other Discretionary and/or Mandatory Access Controls) SHOULD be used to protect these files. Also, if the contents of these files are transferred it SHOULD be done over a trusted channel.

The header data allowed by this file format could contain an unlimited range of information. While in many environments the information conveyed by this header data may be considered innocuous public information, it may constitute a channel through which information about a user, a key or its use may be disclosed intentionally or otherwise (e.g "Comment: Mary E. Jones, 123 Main St, Home Phone:..."). The presence and use of this header data SHOULD be reviewed by sites that deploy this file format.

Normative References

[1] Rinne, T., Ylonen, T., Kivinen, T., Saarinen, M. and S. Lehtinen, "SSH Protocol Transport Protocol", September 2002.

[2] Yergeau, F., "UTF-8, a Transformation Format of Unicode and ISO 10646", October 1996.

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

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

[5] Freed and Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", November 1996.

Authors' Addresses

Joseph Galbraith
VanDyke Software
4848 Tramway Ridge Blvd
Suite 101
Albuquerque, NM 87111
US

Phone: +1 505 332 5700
EMail: galb-list@vandyke.com

Rodney Thayer
The Tillerman Group
370 Altair Way, PMB 321
Sunnyvale, CA 94086

Phone: +1 408 757 9693
EMail: rodney@tillerman.to

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.