Network Working Group
Internet-Draft
Expires: March 31, 2004

S. Lehtinen
SSH Communications Security Corp
D. Moffat, Ed.
Sun Microsystems
Oct 2003

SSH Protocol Assigned Numbers
draft-ietf-secsh-assignednumbers-05.txt

Abstract

This document defines the initial state of the IANA assigned numbers for the SSH protocol. It is intended only for initalization of the IANA databases referenced in those documents.

Table of Contents

1. Introduction

This document does not define any new protocols. It is intended only to create the initial state of the IANA databases for the SSH protocol. Except for one HISTORIC algorithm generally regarded as obsolete, this document does not define any new protocols or any number ranges not already defined in: [SSH-ARCH], [SSH-TRANS], [SSH-USERAUTH], [SSH-CONNECT]

2. Conventions Used in This Document

The keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", and "MAY" that appear in this document are to be interpreted as described in [RFC2119]

The used data types and terminology are specified in the architecture document [SSH-ARCH]

The architecture document also discusses the algorithm naming conventions that MUST be used with the SSH protocols.

3. IANA Considerations

3.1 Message Numbers

The Message Number is an 8-bit value, which describes the payload of a packet.

Protocol packets have message numbers in the range 1 to 255. These numbers have been allocated as follows in [SSH-ARCH]:

Transport layer protocol:

1 to 19	Transport layer generic (e.g. disconnect, ignore, debug, etc.)
20 to 29	Algorithm negotiation
30 to 49	Key exchange method specific (numbers can be reused for different authentication methods)

User authentication protocol:

50 to 59	User authentication generic
60 to 79	User authentication method specific (numbers can be reused for different authentication methods)

Connection protocol:

80 to 89	Connection protocol generic
90 to 127	Channel related messages

Reserved for client protocols:

128 to 191 Reserved

Local extensions:

192 to 255 Local extensions

Requests for assignments of new message numbers must be accompanied by an RFC which describes the new packet type. If the RFC is not on the standards-track (i.e. it is an informational or experimental RFC), it must be explicitly reviewed and approved by the IESG before the RFC is published and the message number is assigned.

Message ID	Value	Reference
SSH_MSG_DISCONNECT	1	[SSH-TRANS]
SSH_MSG_IGNORE	2	[SSH-TRANS]
SSH_MSG_UNIMPLEMENTED	3	[SSH-TRANS]
SSH_MSG_DEBUG	4	[SSH-TRANS]
SSH_MSG_SERVICE_REQUEST	5	[SSH-TRANS]
SSH_MSG_SERVICE_ACCEPT	6	[SSH-TRANS]
SSH_MSG_KEXINIT	20	[SSH-TRANS]
SSH_MSG_NEWKEYS	21	[SSH-TRANS]
SSH_MSG_KEXDH_INIT	30	[SSH-TRANS]
SSH_MSG_KEXDH_REPLY	31	[SSH-TRANS]
SSH_MSG_USERAUTH_REQUEST	50	[SSH-USERAUTH]
SSH_MSG_USERAUTH_FAILURE	51	[SSH-USERAUTH]
SSH_MSG_USERAUTH_SUCCESS	52	[SSH-USERAUTH]
SSH_MSG_USERAUTH_BANNER	53	[SSH-USERAUTH]
SSH_MSG_USERAUTH_PK_OK	60	[SSH-USERAUTH]
SSH_MSG_GLOBAL_REQUEST	80	[SSH-CONNECT]
SSH_MSG_REQUEST_SUCCESS	81	[SSH-CONNECT]
SSH_MSG_REQUEST_FAILURE	82	[SSH-CONNECT]
SSH_MSG_CHANNEL_OPEN	90	[SSH-CONNECT]
SSH_MSG_CHANNEL_OPEN_CONFIRMATION	91	[SSH-CONNECT]
SSH_MSG_CHANNEL_OPEN_FAILURE	92	[SSH-CONNECT]
SSH_MSG_CHANNEL_WINDOW_ADJUST	93	[SSH-CONNECT]
SSH_MSG_CHANNEL_DATA	94	[SSH-CONNECT]
SSH_MSG_CHANNEL_EXTENDED_DATA	95	[SSH-CONNECT]
SSH_MSG_CHANNEL_EOF	96	[SSH-CONNECT]
SSH_MSG_CHANNEL_CLOSE	97	[SSH-CONNECT]
SSH_MSG_CHANNEL_REQUEST	98	[SSH-CONNECT]
SSH_MSG_CHANNEL_SUCCESS	99	[SSH-CONNECT]
SSH_MSG_CHANNEL_FAILURE	100	[SSH-CONNECT]

3.1.1 Disconnect Codes

The Disconnect code is an 8-bit value, which describes the disconnect reason. Requests for assignments of new disconnect codes must be accompanied by an RFC which describes the new disconnect reason code.

Disconnect code	Value	Reference
SSH_DISCONNECT_HOST_NOT_ALLOWED_TO_CONNECT	1	[SSH-TRANS]
SSH_DISCONNECT_PROTOCOL_ERROR	2	[SSH-TRANS]
SSH_DISCONNECT_KEY_EXCHANGE_FAILED	3	[SSH-TRANS]
SSH_DISCONNECT_RESERVED	4	[SSH-TRANS]
SSH_DISCONNECT_MAC_ERROR	5	[SSH-TRANS]
SSH_DISCONNECT_COMPRESSION_ERROR	6	[SSH-TRANS]
SSH_DISCONNECT_SERVICE_NOT_AVAILABLE	7	[SSH-TRANS]
SSH_DISCONNECT_PROTOCOL_VERSION_NOT_SUPPORTED	8	[SSH-TRANS]
SSH_DISCONNECT_HOST_KEY_NOT_VERIFIABLE	9	[SSH-TRANS]
SSH_DISCONNECT_CONNECTION_LOST	10	[SSH-TRANS]
SSH_DISCONNECT_BY_APPLICATION	11	[SSH-TRANS]
SSH_DISCONNECT_TOO_MANY_CONNECTIONS	12	[SSH-TRANS]
SSH_DISCONNECT_AUTH_CANCELLED_BY_USER	13	[SSH-TRANS]
SSH_DISCONNECT_NO_MORE_AUTH_METHODS_AVAILABLE	14	[SSH-TRANS]
SSH_DISCONNECT_ILLEGAL_USER_NAME	15	[SSH-TRANS]

3.2 Service Names

The Service Name is used to describe a protocol layer. These names MUST be printable US-ASCII strings, and MUST NOT contain the characters at-sign ('@'), comma (','), or whitespace or control characters (ASCII codes 32 or less). Names are case-sensitive, and MUST NOT be longer than 64 characters.

Requests for assignments of new service names must be accompanied by an RFC which describes the interpretation for the service name. If the RFC is not on the standards-track (i.e. it is an informational or experimental RFC), it must be explicitly reviewed and approved by the IESG before the RFC is published and the service name is assigned.

Service name	Reference
ssh-userauth	[SSH-USERAUTH]
ssh-connection	[SSH-CONNECT]

3.2.1 Authentication Method Names

The Authentication Method Name is used to describe an authentication method for the "ssh-userauth" service [SSH-USERAUTH]. These names MUST be printable US-ASCII strings, and MUST NOT contain the characters at-sign ('@'), comma (','), or whitespace or control characters (ASCII codes 32 or less). Names are case-sensitive, and MUST NOT be longer than 64 characters.

Requests for assignments of new authentication method names must be accompanied by an RFC which describes the interpretation for the authentication method.

Method name	Reference
publickey	[SSH-USERAUTH, Section 4]
password	[SSH-USERAUTH, Section 5]
hostbased	[SSH-USERAUTH, Section 6]
none	[SSH-USERAUTH, Section 2.3]

3.2.2 Connection Protocol Assigned Names

The following request and type names MUST be printable US-ASCII strings, and MUST NOT contain the characters at-sign ('@'), comma (','), or whitespace or control characters (ASCII codes 32 or less). Names are case-sensitive, and MUST NOT be longer than 64 characters.

Requests for assignments of new assigned names must be accompanied by an RFC which describes the interpretation for the type or request.

3.2.2.1 Connection Protocol Channel Types

Channel type	Reference
session	[SSH-CONNECT, Section 4.1]
x11	[SSH-CONNECT, Section 4.3.2]
forwarded-tcpip	[SSH-CONNECT, Section 5.2]
direct-tcpip	[SSH-CONNECT, Section 5.2]

3.2.2.2 Connection Protocol Global Request Names

Request type	Reference
tcpip-forward	[SSH-CONNECT, Section 5.1]
cancel-tcpip-forward	[SSH-CONNECT, Section 5.1]

3.2.2.3 Connection Protocol Channel Request Names

Request type	Reference
pty-req	[SSH-CONNECT, Section 4.2]
x11-req	[SSH-CONNECT, Section 4.3.1]
env	[SSH-CONNECT, Section 4.4]
shell	[SSH-CONNECT, Section 4.5]
exec	[SSH-CONNECT, Section 4.5]
subsystem	[SSH-CONNECT, Section 4.5]
window-change	[SSH-CONNECT, Section 4.7]
xon-xoff	[SSH-CONNECT, Section 4.8]
signal	[SSH-CONNECT, Section 4.9]
exit-status	[SSH-CONNECT, Section 4.10]
exit-signal	[SSH-CONNECT, Section 4.10]

3.3 Key Exchange Method Names

The Key Exchange Method Name describes a key-exchange method for the protocol [SSH-TRANS]. The names MUST be printable US-ASCII strings, and MUST NOT contain the characters at-sign ('@'), comma (','), or whitespace or control characters (ASCII codes 32 or less). Names are case-sensitive, and MUST NOT be longer than 64 characters.

Requests for assignment of new key-exchange method names must be accompanied by a reference to a standards-track or Informational RFC which describes this method.

Method name	Reference
diffie-hellman-group1-sha1	[SSH-TRANS, Section 4.5]

3.4 Assigned Algorithm Names

The following identifiers (names) MUST be printable US-ASCII strings, and MUST NOT contain the characters at-sign ('@'), comma (','), or whitespace or control characters (ASCII codes 32 or less). Names are case-sensitive, and MUST NOT be longer than 64 characters.

Requests for assignment of new algorithm names must be accompanied by a reference to a standards-track or Informational RFC or a reference to published cryptographic literature which describes the algorithm.

3.4.1 Encryption Algorithm Names

Cipher name	Reference

3des-cbc	[SSH-TRANS, Section 4.3]
blowfish-cbc	[SSH-TRANS, Section 4.3]
twofish256-cbc	[SSH-TRANS, Section 4.3]
twofish-cbc	[SSH-TRANS, Section 4.3]
twofish192-cbc	[SSH-TRANS, Section 4.3]
twofish128-cbc	[SSH-TRANS, Section 4.3]
aes256-cbc	[SSH-TRANS, Section 4.3]
aes192-cbc	[SSH-TRANS, Section 4.3]
aes128-cbc	[SSH-TRANS, Section 4.3]
serpent256-cbc	[SSH-TRANS, Section 4.3]
serpent192-cbc	[SSH-TRANS, Section 4.3]
serpent128-cbc	[SSH-TRANS, Section 4.3]
arcfour	[SSH-TRANS, Section 4.3]
idea-cbc	[SSH-TRANS, Section 4.3]
cast128-cbc	[SSH-TRANS, Section 4.3]
none	[SSH-TRANS, Section 4.3]
des-cbc	[FIPS-46-3] HISTORIC; See page 4 of [FIPS 46-3]

3.4.2 MAC Algorithm Names

MAC name	Reference
hmac-sha1	[SSH-TRANS, Section 4.4]
hmac-sha1-96	[SSH-TRANS, Section 4.4]
hmac-md5	[SSH-TRANS, Section 4.4]
hmac-md5-96	[SSH-TRANS, Section 4.4]
none	[SSH-TRANS, Section 4.4]

3.4.3 Public Key Algorithm Names

Algorithm name	Reference
ssh-dss	[SSH-TRANS, Section 4.6]
ssh-rsa	[SSH-TRANS, Section 4.6]
x509v3-sign-rsa	[SSH-TRANS, Section 4.6]
x509v3-sign-dss	[SSH-TRANS, Section 4.6]
spki-sign-rsa	[SSH-TRANS, Section 4.6]
spki-sign-dss	[SSH-TRANS, Section 4.6]
pgp-sign-rsa	[SSH-TRANS, Section 4.6]
pgp-sign-dss	[SSH-TRANS, Section 4.6]

3.4.4 Compression Algorithm Names

Algorithm name	Reference
none	[SSH-TRANS, Section 4.2]
zlib	[SSH-TRANS, Section 4.2]

4. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF Secretariat.

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

Normative References

[SSH-ARCH]
Ylonen, T., "SSH Protocol Architecture", I-D draft-ietf-architecture-15.txt, Oct 2003.

[SSH-TRANS]
Ylonen, T., "SSH Transport Layer Protocol", I-D draft-ietf-transport-17.txt, Oct 2003.

[SSH-USERAUTH]
Ylonen, T., "SSH Authentication Protocol", I-D draft-ietf-userauth-18.txt, Oct 2003.

[SSH-CONNECT]
Ylonen, T., "SSH Connection Protocol", I-D draft-ietf-connect-18.txt, Oct 2003.

[SSH-NUMBERS]

Lehtinen, S. and D. Moffat, "SSH Protocol Assigned Numbers", I-D draft-ietf-secsh-assignednumbers-05.txt, Oct 2003.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Informative References

[FIPS-46-3]
U.S. Dept. of Commerce, "FIPS PUB 46-3, Data Encryption Standard (DES)", October 1999.

Authors' Addresses

Sami Lehtinen
SSH Communications Security Corp
Fredrikinkatu 42
HELSINKI FIN-00100
Finland

EMail: sjl@ssh.com

Darren J Moffat (editor)
Sun Microsystems
901 San Antonio Road
Palo Alto 94303
USA

EMail: Darren.Moffat@Sun.COM

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

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