Workgroup: Internet Engineering Task Force
Internet-Draft:
draft-yee-ssh-iana-requirements-01
Updates: 4250, 4716, 4819, 8308 (if approved)
Published: 8 September 2023
Intended Status: Standards Track
Expires: 11 March 2024
Authors: P. Yee
AKAYLA

Update to the IANA SSH Protocol Parameters Registry Requirements

Abstract

This specification updates the requirements for adding new entries to the IANA Secure Shell (SSH) Protocol Parameters registry. Currently, the requirement is generally for "IETF Review", as defined in RFC 8126, although a few portions of the registry require "Standards Action". This specification will change that former requirement to "Expert Review". This draft updates RFC 4250, RFC 4716, RFC 4819, RFC 8308.

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 https://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 11 March 2024.

Table of Contents

1. Introduction

The IANA Secure Shell (SSH) Protocol Parameters registry was populated by several RFCs including [RFC4250], [RFC4716], [RFC4819], and [RFC8308]. Outside of some narrow value ranges that require Standards Action in order to add new values or are marked for private use, all other portions of the registry require IETF Review [RFC8126]. This specification changes the requirement for sections currently requiring IETF Review to Expert Review. This change is made in line with similar changes undertaken for certain IPsec and TLS registries.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. SSH Protocol Parameters Affected

The following table lists the "Secure Shell (SSH) Protocol Parameters" registries whose registration policy is changed from IETF Review to Expert Review. Where this change applies to a specific range of values within the particular parameter, that range is given in the notes column.

Parameter Name	RFC	Notes
Authentication Method Names	[RFC4250]	

Parameter Name	RFC	Notes
Channel Connection Failure Reason Codes and Descriptions	[RFC4250]	0x00000001-0xFDFFFFFF (inclusive)
Compression Algorithm Names	[RFC4250]	
Connection Protocol Channel Request Names	[RFC4250]	
Connection Protocol Channel Types	[RFC4250]	
Connection Protocol Global Request Names	[RFC4250]	
Connection Protocol Subsystem Names	[RFC4250]	
Disconnection Messages Reason Codes and Descriptions	[RFC4250]	0x00000001-0xFDFFFFFF (inclusive)
Encryption Algorithm Names	[RFC4250]	
Extended Channel Data Transfer data_type_code and Data	[RFC4250]	0x00000001-0xFDFFFFFF (inclusive)
Extension Names	[RFC8308]	
Key Exchange Method Names	[RFC4250]	
MAC Algorithm Names	[RFC4250]	
Pseudo-Terminal Encoded Terminal Modes	[RFC4250]	
Public Key Algorithm Names	[RFC4250]	
Publickey Subsystem Attributes	[RFC4819]	
Publickey Subsystem Request Names	[RFC4819]	
Publickey Subsystem Response Names	[RFC4819]	
Service Names	[RFC4250]	
Signal Names	[RFC4250]	
SSH Public-Key File Header Tags	[RFC4716]	Excluding header-tags beginning with x-

Table 1: Secure Shell (SSH) Protocol Parameters Affected

The only IANA SSH protocol parameter registries not affected are "Message Numbers" and "Publickey Subsystem Status Codes", as these remain at standard track policy due to their limited resources as one-byte registry values.

3. Designated Expert Pool

Expert Review [RFC8126] registry requests are registered after a three-week review period on the <ssh-reg-review@ietf.org> mailing list, and on the advice of one or more designated experts. However, to allow for the allocation of values prior to publication, the

designated experts may approve registration once they are satisfied that such a specification will be published.

Registration requests sent to the mailing list for review SHOULD use an appropriate subject (e.g., "Request to register value in SSH protocol parameters <specific parameter> registry").

Within the review period, the designated experts will either approve or deny the registration request, communicating this decision to the review list and IANA. Denials MUST include an explanation and, if applicable, suggestions as to how to make the request successful. Registration requests that are undetermined for a period longer than 21 days can be brought to the IESG's attention (using the <iesg@ietf.org> mailing list) for resolution.

Criteria that SHOULD be applied by the designated experts includes determining whether the proposed registration duplicates existing functionality (which is not permitted), whether it is likely to be of general applicability or useful only for a single application, and whether the registration description is clear.

IANA MUST only accept registry updates from the designated experts and the IESG. It SHOULD direct all requests for registration from other than those sources to the review mailing list.

It is suggested that multiple designated experts be appointed who are able to represent the perspectives of different applications using this specification, in order to enable broadly informed review of registration decisions. In cases where a registration decision could be perceived as creating a conflict of interest for a particular Expert, that Expert SHOULD defer to the judgment of the other Experts.

4. Acknowledgements

The impetus for this specification was a February 2021 discussion on the CURDLE mailing list [CURDLE-MA].

5. IANA Considerations

This memo is entirely about updating the IANA SSH Protocol Parameters registry.

6. Security Considerations

This memo does not change the Security Considerations for any of the updated RFCs.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4250] Lehtinen, S. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, DOI 10.17487/RFC4250, January 2006, <https://www.rfc-editor.org/info/rfc4250>.

[RFC4819] Galbraith, J., Van Dyke, J., and J. Bright, "Secure Shell Public Key Subsystem", RFC 4819, DOI 10.17487/RFC4819, March 2007, <https://www.rfc-editor.org/info/rfc4819>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8308] Bider, D., "Extension Negotiation in the Secure Shell (SSH) Protocol", RFC 8308, DOI 10.17487/RFC8308, March 2018, <https://www.rfc-editor.org/info/rfc8308>.

7.2. Informative References

[CURDLE-MA] Turner, S., "Time to Review IANA SSH Registries Policies?", February 2021, <https://mailarchive.ietf.org/arch/msg/curdle/gdiOlZr9bnrZv8umVyguGG3woIM/>.

[RFC4716] Galbraith, J. and R. Thayer, "The Secure Shell (SSH) Public Key File Format", RFC 4716, DOI 10.17487/RFC4716, November 2006, <https://www.rfc-editor.org/info/rfc4716>.

Author's Address

Peter E. Yee
AKAYLA
Mountain View, Calif. 94043
United States of America

Email: peter@akayla.com