RFC 9519
Update to the IANA SSH Protocol Parameters Registry Requirements

Abstract
This specification updates the registration policies for adding new entries to registries within the IANA "Secure Shell (SSH) Protocol Parameters" group of registries. Previously, the registration policy was generally IETF Review, as defined in RFC 8126, although a few registries require Standards Action. This specification changes it from IETF Review to Expert Review. This document updates RFCs 4250, 4716, 4819, and 8308.

Status of This Memo
This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9519.

Copyright Notice
Copyright (c) 2024 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 (https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction 2
   1.1. Requirements Language 2
2. SSH Protocol Parameters Affected 3
3. Designated Expert Pool 4
4. IANA Considerations 5
5. Security Considerations 5
6. References 5
   6.1. Normative References 5
   6.2. Informative References 5
Acknowledgements 6
Author's Address 6

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 that are marked for Private Use, the registration policy for other portions of the registry was IETF Review [RFC8126]. This specification changes the policy from IETF Review to Expert Review. This change is 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 has changed from IETF Review to Expert Review. Where this change applied to a specific range of values within the particular parameter, that range is given in the notes column. Affected registries now list this document as a reference.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>RFC</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Channel Connection Failure Reason Codes and Descriptions</td>
<td>[RFC4250]</td>
<td>0x00000001-0xFDFFFFFF (inclusive)</td>
</tr>
<tr>
<td>Compression Algorithm Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Connection Protocol Channel Request Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Connection Protocol Channel Types</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Connection Protocol Global Request Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Connection Protocol Subsystem Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Disconnection Messages Reason Codes and Descriptions</td>
<td>[RFC4250]</td>
<td>0x00000001-0xFDFFFFFF (inclusive)</td>
</tr>
<tr>
<td>Encryption Algorithm Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Extended Channel Data Transfer data_type_code and Data</td>
<td>[RFC4250]</td>
<td>0x00000001-0xFDFFFFFF (inclusive)</td>
</tr>
<tr>
<td>Extension Names</td>
<td>[RFC8308]</td>
<td></td>
</tr>
<tr>
<td>Key Exchange Method Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>MAC Algorithm Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Pseudo-Terminal Encoded Terminal Modes</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Public Key Algorithm Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Publickey Subsystem Attributes</td>
<td>[RFC4819]</td>
<td></td>
</tr>
</tbody>
</table>
The only IANA SSH protocol parameter registries not affected are "Message Numbers" and "Publickey Subsystem Status Codes", as these remain Standards Action 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 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.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>RFC</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publickey Subsystem Request Names</td>
<td>[RFC4819]</td>
<td></td>
</tr>
<tr>
<td>Publickey Subsystem Response Names</td>
<td>[RFC4819]</td>
<td></td>
</tr>
<tr>
<td>Service Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Signal Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>SSH Public-Key File Header Tags</td>
<td>[RFC4716]</td>
<td>Excluding header-tags beginning with x-</td>
</tr>
</tbody>
</table>

*Table 1: Secure Shell (SSH) Protocol Parameters Affected*
4. IANA Considerations

This memo is entirely about updating the IANA “Secure Shell (SSH) Protocol Parameters” registry.

5. Security Considerations

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

6. References

6.1. Normative References


6.2. Informative References


Acknowledgements

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

Author's Address

Peter E. Yee
AKAYLA
Mountain View, CA 94043
United States of America
Email: peter@akayla.com