Internet Engineering Task Force (IETF) P. Yee
Request for Comments: 9519 AKAYLA
Updates: 4250, 4716, 4819, 8308 January 2024
Category: Standards Track
ISSN: 2070-1721

Update to the IANA SSH Protocol Parameters Registry Requirements

Обновление требований к реестру параметров протокола SSH

Аннотация

Эта спецификация обновляет правила регистрации для добавления новых записей в реестры группы IANA Secure Shell (SSH) Protocol Parameters. Ранее обычно применялась процедура IETF Review, определённая в RFC 8126, хотя для некоторых реестров требовалась процедура Standards Action. Эта спецификация заменяет IETF Review процедурой Expert Review. Документ обновляет RFC 4250, 4716, 4819, 8308.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке https://www.rfc-editor.org/info/rfc9519.

Оглавление

1. Введение

Реестр IANA Secure Shell (SSH) Protocol Parameters заполнялся несколькими RFC, включая [RFC4250], [RFC4716], [RFC4819], [RFC8308]. За исключением небольших подддиапазонов значений, требующих использовать процедуру Standards Action или помеченных для частного использования (Private Use), добавление значений происходило по процедуре IETF Review [RFC8126]. Эта спецификация заменяет правило IETF Review на Expert Review. Изменение соответствует похожим изменениям для некоторых реестров IPsec и TLS.

1.1. Уровни требований

Ключевые слова **должно** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

2. Затрагиваемые параметры протокола SSH

В таблице 1 приведены реестры Secure Shell (SSH) Protocol Parameters, для которых политика регистрации IETF Review заменена на Expert Review. Если изменения относятся к определённому диапазону, он указывается в колонке примечаний. Затронутые реестры ссылаются на данный документ.

[1] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

Таблица 1. Затронутые параметры протокола Secure Shell (SSH).

Имя параметра	*RFC*	*Примечания*
Authentication Method Names	[RFC4250]	
Channel Connection Failure Reason Codes and Descriptions	[RFC4250]	0x00000001-0xFDFFFFFF (включительно)
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 (включительно)
Encryption Algorithm Names	[RFC4250]	
Extended Channel Data Transfer data_type_code and Data	[RFC4250]	0x00000001-0xFDFFFFFF (включительно)
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]	За исключением тегов, начинающихся с x-

Не затронуты изменениями лишь реестры протокола IANA SSH Message Numbers и Publickey Subsystem Status Codes, поскольку для них сохраняется процедура Standards Action из-за ограниченности ресурсов однобайтовых значений.

3. Пул назначаемых экспертов

По процедуре Expert Review [RFC8126] запросы на регистрацию рассматриваются в течение трёх недель в почтовой конференции <ssh-reg-review@ietf.org>, по рекомендации одного или нескольких назначенных экспертов. Однако для выделения значений до публикации документа назначенные эксперты могут одобрять регистрацию, как только они будут уверены, что спецификация будет опубликована.

В запросах на регистрацию, направляемых в список рассылки для рецензирования, **следует** использовать подходящую тему (например, Request to register value in SSH protocol parameters <specific parameter> registry).

В течение периода рецензирования назначенные эксперты одобряют или отклоняют запрос на регистрацию, сообщая о своём решении в списке рассылки и направляя его в IANA. Отказ **должен** включать обоснование и, если это применимо, предложения в части требуемых для принятия изменений. Запросы на регистрацию, по которым не принято решения по истечении 21 дня, могут передаваться в IESG через почтовую конференцию <iesg@ietf.org> для разрешения вопроса.

Критерии, которые **следует** применять назначенным экспертам, включают определение дублирования предложенной регистрацией имеющейся функциональности (это недопустимо), применимости для общих целей или лишь одного приложения, а также ясность описания регистрации.

Агентство IANA **должно** принимать обновления реестрой только от назначенных экспертов и IESG, а запросы на регистрацию из других источников **следует** направлять в почтовую конференцию для рецензирования.

Предполагается назначение нескольких экспертов, способных представить точки зрения разных приложений, применяющих спецификацию, чтобы обеспечить широкую информированность при решении вопроса о регистрации. Если решение может казаться вызывающим конфликт интересов для конкретного эксперта, ему **следует** принять решение других экспертов.

4. Взаимодействие с IANA

Этот документ полностью посвящён обновлению реестра IANA Secure Shell (SSH) Protocol Parameters.

5. Вопросы безопасности

Этот документ не меняет содержимого разделов «Вопросы безопасности» в затронутых RFC.

6. Литература

6.1. Нормативные документы

[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>.

6.2. Дополнительная литература

[CURDLE-MA] Turner, S., "Subject: [Curdle] Time to Review IANA SSH Registries Policies?", message to the Curdle mailing list, 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>.

Благодарности

Толчком к созданию этого документа послужило обсуждение в феврале 2021 г. в почтовой конференции CURDLE [CURDLE-MA].

Адрес автора

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

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru