Groupe de travail Réseau
Request for Comments : 4250
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

S. Lehtinen, SSH Communications Security Corp
C. Lonvick, éd. Cisco Systems, Inc.

janvier 2006

Numéros alloués du protocole Secure Shell (SSH)

Statut de ce mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document définit les instructions à l'IANA et l'état initial des numéros alloués par l'IANA pour le protocole Secure Shell (SSH). Il est destiné seulement à l'initialisation des registres de l'IANA référencés dans l'ensemble des documents relatifs à SSH.

Table des matières

1. Introduction

Le présent document ne définit aucun nouveau protocole. Il est seulement destiné à créer l'état initial des bases de données de l'IANA pour le protocole SSH et il contient aussi des instructions pour les allocations futures. Sauf un algorithme historique généralement considéré comme obsolète, le présent document ne définit aucun nouveau protocole ou gamme de numéros qui ne soit déjà défini dans les [RFC4251], [RFC4252], [RFC4253], [RFC4254].

2. Contributeurs

Les contributeurs majeurs originaux de cet ensemble de documents ont été Tatu Ylonen, Tero Kivinen, Timo J. Rinne, Sami Lehtinen (tous de SSH Communications Security Corp) et Markku-Juhani O. Saarinen (Université de Jyvaskyla). Darren Moffat était l'éditeur original de cet ensemble de documents et y a aussi fait de très substantielles contributions.

De nombreuses personnes ont contribué au développement de ce document au fil des ans. Les personnes qui doivent en être remerciées incluent Mats Andersson, Ben Harris, Bill Sommerfeld, Brent McClure, Niels Moller, Damien Miller, Derek Fawcus, Frank Cusack, Heikki Nousiainen, Jakob Schlyter, Jeff Van Dyke, Jeffrey Altman, Jeffrey Hutzelman, Jon Bright, Joseph Galbraith, Ken Hornstein, Markus Friedl, Martin Forssen, Nicolas Williams, Niels Provos, Perry Metzger, Peter Gutmann, Simon Josefsson, Simon Tatham, Wei Dai, Denis Bider, der Mouse, et Tadayoshi Kohno. La présence de leur noms ici ne signifie pas qu'ils approuvent le présent document, mais qu'il y ont contribué.

3. Conventions utilisée dans ce document

3.1 Mots-clés de la RFC 2119

Tous les documents relatifs aux protocoles SSH devront utiliser les mots-clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" pour décrire les exigences. Ces mots-clés sont à interpréter comme décrit dans la [RFC2119].

3.2 Mots-clés de la RFC 2434

Les mots clés "UTILISATION PRIVÉE", "ALLOCATION HIÉRARCHIQUE", "PREMIER ARRIVÉ PREMIER SERVI", "REVUE D'EXPERT", "SPÉCIFICATION EXIGÉE", "APPROBATION DE L'IESG", "CONSENSUS DE L'IETF", et "ACTION DE NORMALISATION" qui apparaissent dans ce document lorsque ils sont utilisés pour décrire l'allocation d'espaces de noms sont à interpréter comme décrit dans la [RFC2434]. Ces désignations sont répétées ici pour éviter au lecteur de les chercher ailleurs.

UTILISATION PRIVÉE - seulement pour utilisation privée ou locale, avec le type et l'objet définis par le site local. Aucune tentative n'est faite pour empêcher plusieurs sites d'utiliser la même valeur de façons différentes (et incompatibles). Il n'est pas nécessaire que l'IANA revoit de telles allocations qui ne sont généralement d'aucune utilité pour l'interopérabilité.

ALLOCATION HIÉRARCHIQUE - des gestionnaires délégués peuvent allouer des valeurs pourvu qu'on leur ait donné le contrôle sur cette partie de l'espace de noms. L'IANA contrôle les niveaux supérieurs de l'espace de noms en accord avec une des autres politiques.

PREMIER ARRIVÉ, PREMIER SERVI - tout un chacun peut obtenir un numéro alloué, pour autant qu'il fournisse un point de contact et une brève description de l'utilisation de la valeur. Pour les numéros, la valeur exacte est généralement allouée par l'IANA ; avec les noms, des noms spécifiques sont généralement demandés.

REVUE D'EXPERT - l'approbation par un expert désigné est exigée.

SPÉCIFICATION EXIGÉE - les valeurs et leur signification doivent être documentées dans une RFC ou autre référence permanente et directement disponible, avec un détail suffisant pour que l'interopérabilité entre des mises en œuvre indépendantes soit possible.

APPROBATION DE L'IESG - les nouvelles allocations doivent être approuvées par l'IESG, mais il n'est pas exigé que la demande soit documentée dans une RFC (bien qu'il soit à la discrétion de l'IESG de demander des documents ou autres matériaux de support au cas par cas).

CONSENSUS DE L'IETF - les nouvelles valeurs sont allouées par le processus de consensus de l'IETF. Précisément, les nouvelles allocations sont faites via des RFC approuvées par l'IESG. Normalement, l'IESG va rechercher des informations sur les perspectives d'allocation auprès des personnes appropriées (par exemple, le groupe de travail pertinent si il en existe un).

ACTION DE NORMALISATION - les valeurs ne sont allouées que pour des RFC sur la voie de la normalisation approuvées par l'IESG.

3.3 Champs et valeurs du protocole

Les champs du protocole et les valeurs possibles pour les remplir sont définies dans cet ensemble de documents. Les champs de protocole seront définis dans les définitions de message. Par exemple, SSH_MSG_CHANNEL_DATA est défini comme suit :

octet SSH_MSG_CHANNEL_DATA
uint32 canal receveur
chaîne données

Tout au long de ces documents, quand on se réfère aux champs, ils apparaissent entre des guillemets simples. Quand on se réfère aux valeurs pour remplir ces champs, elle vont apparaître entre des guillemets doubles. En utilisant l'exemple ci-dessus, les valeurs possibles pour 'données' sont "foo" et "bar".

4. Considérations relatives à l'IANA

Ce document entier constitue les considérations relatives à l'IANA pour le protocole SSH, tel que défini dans les [RFC4251], [RFC4252], [RFC4253], [RFC4254]. Cette section contient les conventions utilisées pour la désignation des espaces de noms, l'état initial du registre, et les instructions pour les allocations futures.

4.1 Numéros de message

Le numéro de message est une valeur d'octet qui décrit la charge utile d'un paquet.

4.1.1 Conventions

Les paquets du protocole ont des numéros de message dans la gamme de 1 à 255. Ces numéros sont alloués comme suit :

Protocole de couche transport :
1 à 19 : couche de transport générique (par exemple, déconnecter, ignorer, déboguer, etc.)
20 à 29 : négociation d'algorithme
30 à 49 : spécificités de la méthode d'échange de clés (les numéros peuvent être réutilisés pour des méthodes authentification différentes)

Protocole d'authentification d'utilisateur
50 à 59 : authentification générique d'utilisateur
60 à 79 : spécificités de la méthode d'authentification d'utilisateur (les numéros peuvent être réutilisés pour des méthodes authentification différentes)

Protocole de connexion :
80 à 89 : protocole de connexion générique
90 à 127 : messages relatifs au canal

Réservé pour les protocoles de client : 128 à 191

Extensions locales : 192 à 255

4.1.2 Allocations initiales

Le tableau qui suit identifie les allocations initiales des valeurs d'identifiant de message.

Identifiant de message	Valeur	Référence
SSH_MSG_DISCONNECT	1	[RFC4253]
SSH_MSG_IGNORE	2	[RFC4253]
SSH_MSG_UNIMPLEMENTED	3	[RFC4253]
SSH_MSG_DEBUG	4	[RFC4253]
SSH_MSG_SERVICE_REQUEST	5	[RFC4253]
SSH_MSG_SERVICE_ACCEPT	6	[RFC4253]
SSH_MSG_KEXINIT	20	[RFC4253]
SSH_MSG_NEWKEYS	21	[RFC4253]

SSH_MSG_USERAUTH_REQUEST	50	[RFC4252]
SSH_MSG_USERAUTH_FAILURE	51	[RFC4252]
SSH_MSG_USERAUTH_SUCCESS	52	[RFC4252]
SSH_MSG_USERAUTH_BANNER	53	[RFC4252]
SSH_MSG_GLOBAL_REQUEST	80	[RFC4254]
SSH_MSG_REQUEST_SUCCESS	81	[RFC4254]
SSH_MSG_REQUEST_FAILURE	82	[RFC4254]
SSH_MSG_CHANNEL_OPEN	90	[RFC4254]
SSH_MSG_CHANNEL_OPEN_CONFIRMATION	91	[RFC4254]
SSH_MSG_CHANNEL_OPEN_FAILURE	92	[RFC4254]
SSH_MSG_CHANNEL_WINDOW_ADJUST	93	[RFC4254]
SSH_MSG_CHANNEL_DATA	94	[RFC4254]
SSH_MSG_CHANNEL_EXTENDED_DATA	95	[RFC4254]
SSH_MSG_CHANNEL_EOF	96	[RFC4254]
SSH_MSG_CHANNEL_CLOSE	97	[RFC4254]
SSH_MSG_CHANNEL_REQUEST	98	[RFC4254]
SSH_MSG_CHANNEL_SUCCESS	99	[RFC4254]
SSH_MSG_CHANNEL_FAILURE	100	[RFC4254]

4.1.3 Allocations futures

Les demandes d'allocation de nouveaux numéros de message dans la gamme de 1 à 29, de 50 à 59, et de 80 à 127 DOIVENT être faites par la méthode ACTION DE NORMALISATION, comme décrit dans la [RFC2434].

La signification des numéros de message dans la gamme de 30 à 49 est spécifique de la méthode d'échange de clés utilisée, et leur signification est spécifiée par la définition de cette méthode.

La signification des numéros de message dans la gamme de 60 à 79 est spécifique de la méthode d'authentification d'utilisateur utilisée, et elle sera spécifiée par la définition de cette méthode.

Les demandes d'allocation de nouveaux numéros de message dans la gamme de 128 à 191 DOIVENT être faites par la méthode de CONSENSUS DE L'IETF, comme décrit dans la [RFC2434].

L'IANA ne contrôle pas les numéros de message dans la gamme de 192 à 255. Cette gamme est laissé pour UTILISATION PRIVÉE.

4.2 Codes et descriptions de cause de message de déconnexion

Le champ 'code de cause' d'un message de déconnexion est une valeur de uint32 *(entier non signé de 32 bits)*. Le champ 'description' associé au message de déconnexion est lisible par l'homme et décrit la raison de la déconnexion.

4.2.1 Conventions

Les paquets de protocole qui contiennent le message SSH_MSG_DISCONNECT DOIVENT avoir des valeurs de 'code de cause' de message de déconnexion dans la gamme de 0x00000001 à 0xFFFFFFFF. Elles sont décrites dans la [RFC4253].

4.2.2 Allocations initiales

Le tableau qui suit identifie les allocations initiales des valeurs de 'description' et de 'code de cause' de SSH_MSG_DISCONNECT.

Nom symbolique	**Code de cause**
SSH_DISCONNECT_HOST_NOT_ALLOWED_TO_CONNECT	1
SSH_DISCONNECT_PROTOCOL_ERROR	2
SSH_DISCONNECT_KEY_EXCHANGE_FAILED	3
SSH_DISCONNECT_RESERVED	4
SSH_DISCONNECT_MAC_ERROR	5
SSH_DISCONNECT_COMPRESSION_ERROR	6
SSH_DISCONNECT_SERVICE_NOT_AVAILABLE	7
SSH_DISCONNECT_PROTOCOL_VERSION_NOT_SUPPORTED	8
SSH_DISCONNECT_HOST_KEY_NOT_VERIFIABLE	9

SSH_DISCONNECT_CONNECTION_LOST	10
SSH_DISCONNECT_BY_APPLICATION	11
SSH_DISCONNECT_TOO_MANY_CONNECTIONS	12
SSH_DISCONNECT_AUTH_CANCELLED_BY_USER	13
SSH_DISCONNECT_NO_MORE_AUTH_METHODS_AVAILABLE	14
SSH_DISCONNECT_ILLEGAL_USER_NAME	15

4.2.3 Allocations futures

Les valeurs de 'code de cause' de message de déconnexion DOIVENT être allouées en séquence. Les demandes d'allocations de nouvelles valeurs de 'code de cause' de message de déconnexion, et leur texte de 'description' de message de déconnexion associé, dans la gamme de 0x00000010 à 0xFDFFFFFF, DOIVENT être faites par la méthode du CONSENSUS DE L'IETF, comme décrit dans la [RFC2434]. L'IANA n'allouera pas de valeurs de 'code de cause' de message de déconnexion dans la gamme de 0xFE000000 à 0xFFFFFFFF. Les valeurs de 'code de cause' de message de déconnexion dans cette gamme sont laissées pour UTILISATION PRIVÉE, comme décrit dans la [RFC2434].

4.3 Codes et descriptions des causes de défaillance de connexion de canal

Le 'code de cause' d'échec de connexion de canal est une valeur de uint32. Le texte associé de 'description' d'échec de connexion de canal est un message lisible par l'homme qui décrit la raison de l'échec de connexion de canal. Il est décrit dans la [RFC4254].

4.3.1 Conventions

Les paquets de protocole qui contiennent le message SSH_MSG_CHANNEL_OPEN_FAILURE DOIVENT avoir des valeurs de 'code de cause' d'échec de connexion de canal dans la gamme de 0x00000001 à 0xFFFFFFFF.

4.3.2 Allocations initiales

Les allocations initiales pour les valeurs de 'code de cause' et de 'description' sont données dans le tableau ci-dessous. Noter que les valeurs pour le 'code de cause' sont données en format décimal pour la lisibilité, mais elles sont en fait des valeurs de uint32.

Nom symbolique	**code de cause**
SSH_OPEN_ADMINISTRATIVELY_PROHIBITED	1
SSH_OPEN_CONNECT_FAILED	2
SSH_OPEN_UNKNOWN_CHANNEL_TYPE	3
SSH_OPEN_RESOURCE_SHORTAGE	4

4.3.3 Allocations futures

Les valeurs de 'code de cause' d'échec de connexion de canal DOIVENT être allouées en séquence. Les demandes d'allocations de nouvelles valeurs de 'code de cause' d'échec de connexion de canal, et leur chaîne de description associée d'échec de connexion de canal, dans la gamme de 0x00000005 à 0xFDFFFFFF, DOIVENT être faites par la méthode de CONSENSUS DE L'IETF, comme décrit dans la [RFC2434]. L'IANA n'allouera pas de valeurs de 'code de cause' d'échec de connexion de canal dans la gamme de 0xFE000000 à 0xFFFFFFFF. Ces valeurs sont laissées pour UTILISATION PRIVÉE, comme décrit dans la [RFC2434].

4.3.4 Notes sur la gamme UTILISATION PRIVÉE

Bien qu'il soit entendu que l'IANA n’aura aucun contrôle sur la gamme de 0xFE000000 à 0xFFFFFFFF, cette gamme sera partagée en deux parties et administrée par les conventions suivantes.

- La gamme de 0xFE000000 à 0xFEFFFFFF est à utiliser en conjonction avec des canaux alloués en local. Par exemple, si un canal est proposé avec un 'type de canal' de "exemple_session@exemple.com" mais échoue, le serveur va alors répondre avec un 'code de cause' alloué par l'IANA (comme indiqué ci-dessus et dans la gamme de 0x00000001 à 0xFDFFFFFF) ou avec une valeur allouée en local dans la gamme de 0xFE000000 à 0xFEFFFFFF. Naturellement, si le serveur ne comprend pas le 'type de canal' proposé, même si il est un 'type de canal' défini en local, alors le 'code de cause' DOIT être 0x00000003, comme décrit ci-dessus. Si le serveur comprend bien le 'type de canal', mais si le canal échoue encore à s'ouvrir, le serveur DEVRAIT alors répondre avec une valeur de 'code de cause' allouée en local

cohérente avec le 'type de canal' local proposé. On suppose qu'en pratique on essayera d'abord d'utiliser les valeurs de 'code de cause' allouées par l'IANA, et qu'ensuite on documentera les valeurs de 'code de cause' allouées en local.

o Il n'y a pas de restrictions ni suggestions pour la gamme commençant par 0xFF. Aucune interopérabilité n'est attendue pour ce qui sera utilisé dans cette gamme. Elle est essentiellement pour l'expérimentation.

4.4 Transfert de données de canal étendu "data_type_code" et "data"

Le 'code de type de données' de transfert de données de canal étendu est une valeur de uint32. Les 'données' associées de transfert de données de canal étendu sont un message lisible par l'homme qui décrit le type de données dont le transfert est permis dans le canal.

4.4.1 Conventions

Les paquets de protocole qui contiennent le message SSH_MSG_CHANNEL_EXTENDED_DATA DOIVENT avoir des valeurs de 'code de type de données' de transfert de données de canal étendu dans la gamme de 0x00000001 à 0xFFFFFFFF. Elles sont décrites dans la [RFC4254].

4.4.2 Allocations initiales

Les allocations initiales pour les valeurs de 'code de type de données' et les valeurs de 'données' sont données dans le tableau ci-dessous. Noter que la valeur pour le 'code de type de données' est donnée en format décimal pour la lisibilité, mais que les valeurs réelles sont en uint32.

Nom symbolique	code de type de données
SSH_EXTENDED_DATA_STDERR	1

4.4.3 Allocations futures

Les valeurs de 'code de type de données' de transfert de données de canal étendu DOIVENT être allouées à la suite. Les demandes d'allocation de nouvelles valeurs de 'code de type de données' de transfert de données de canal étendu, et les chaînes associées de 'données' de transfert de données de canal étendu dans la gamme de 0x00000002 à 0xFDFFFFFF, DOIVENT être faites par la méthode du CONSENSUS DE L'IETF, comme décrit dans la [RFC2434]. L'IANA n'allouera pas de valeurs de 'code de type de données' de transfert de données de canal étendu dans la gamme de 0xFE000000 à 0xFFFFFFFF. Ces valeurs sont laissées pour UTILISATION PRIVÉE, comme décrit dans la [RFC2434].

4.5 Modes de terminal codé de pseudo terminal

Les messages SSH_MSG_CHANNEL_REQUEST avec une chaîne "pty-req" *(demande de pseudo terminal)* DOIVENT contenir des 'modes de terminal codés'. La valeur de 'modes de terminal codés' est un flux d'octets de paires opcode-argument.

4.5.1 Conventions

Les paquets de protocole qui contiennent le message SSH_MSG_CHANNEL_REQUEST avec une chaîne "pty-req" DOIVENT contenir une valeur de 'modes de terminal codés'. Les valeurs de opcode consistent en un seul octet et sont dans la gamme de 1 à 255. Les opcodes 1 à 159 ont un argument uint32. Les opcodes 160 à 255 ne sont pas encore définis.

4.5.2 Allocations initiales

Le tableau qui suit identifie les allocations initiales des valeurs de opcode qui sont utilisées dans la valeur de 'modes de terminal codés'.

Opcode	Mnémonique	Description
0	TTY_OP_END	Indique la fin des options.
1	VINTR	Caractère d'interruption ; 255 si aucun. De même pour les autres caractères. Tous ces caractères ne sont pas supportés sur tous les systèmes.
2	VQUIT	Caractère quitte (envoie le signal SIGQUIT sur les systèmes POSIX).

3	VERASE	Écrase le caractère à gauche du curseur.
4	VKILL	Écrase la ligne d'entrée en cours.
5	VEOF	Caractère fin de fichier (envoie EOF à partir du terminal).
6	VEOL	Caractère fin de ligne en plus de retour chariot et/ou saut à la ligne.
7	VEOL2	Caractère fin de ligne supplémentaire.
8	VSTART	Continue la pause de résultat (normalement contrôle-Q).
9	VSTOP	Pause du résultat (normalement contrôle-S).
10	VSUSP	Suspend le programme en cours.
11	VDSUSP	Autre caractère de suspension.
12	VREPRINT	Ré imprime la ligne d'entrée en cours.
13	VWERASE	Écrase un mot à gauche du curseur.
14	VLNEXT	Entre le prochain caractère tapé littéralement, même si c'est un caractère spécial
15	VFLUSH	Caractère pour purger le résultat.
16	VSWTCH	Passe à une couche de coquille différente.
17	VSTATUS	Imprime la ligne d'état de système (charge, commande, pid, etc).
18	VDISCARD	Bascule la purge d'un résultat terminal.
30	IGNPAR	Fanion ignorer la parité. Le paramètre DEVRAIT être 0 si ce fanion est FAUX, et 1 si il est VRAI.
31	PARMRK	Erreurs de parité et de tramage de marque.
32	INPCK	Permet la vérification d'erreurs de parité.
33	ISTRIP	Supprime le huitième bit des caractères.
34	INLCR	Transpose NL en CR sur l'entrée.
35	IGNCR	Ignorer le CR en entrée.
36	ICRNL	Transpose CR en NL sur l'entrée.
37	IUCLC	Transpose les caractères majuscules en minuscules.
38	IXON	Active le contrôle de flux en sortie.
39	IXANY	Tout caractère va recommencer après l'arrêt.
40	IXOFF	Active le contrôle de flux en entrée.
41	IMAXBEL	Sonnerie quand la file d'attente d'entrée est pleine.
50	ISIG	Active les signaux INTR, QUIT, [D]SUSP.
51	ICANON	Canonise les lignes d'entrée.
52	XCASE	Permet l'entrée et la sortie de caractères majuscules en faisant précéder leur équivalent minuscule de "\".
53	ECHO	Active l'écho.
54	ECHOE	Visualisation des caractères écrasés.
55	ECHOK	Le caractère Kill élimine la ligne en cours.
56	ECHONL	Écho de NL même si ECHO est désactivé.
57	NOFLSH	Ne pas purger après l'interruption.
58	TOSTOP	Arrêt des tâches d'arrière plan provenant de la sortie.
59	IEXTEN	Active les extensions.
60	ECHOCTL	Faire écho des caractères de contrôle avec ^(Char).
61	ECHOKE	Écrasement visuel pour suppression de ligne.
62	PENDIN	Refrappe de l'entrée en cours.

70	OPOST	Permet le traitement de la sortie.
71	OLCUC	Convertit les minuscules en majuscules.
72	ONLCR	Transpose NL en CR-NL.
73	OCRNL	Traduit le retour chariot en nouvelle ligne (en sortie).
74	ONOCR	Traduit la nouvelle ligne en retour chariot-nouvelle ligne (en sortie).
75	ONLRET	Nouvelle ligne effectue un retour chariot (en sortie).
90	CS7	Mode 7 bits.
91	CS8	Mode 8 bits.
92	PARENB	Parité activée.
93	PARODD	Parité impaire, autrement, paire.
128	TTY_OP_ISPEED	Spécifie le taux d'entrée en bauds en bits par seconde.
129	TTY_OP_OSPEED	Spécifie le taux de sortie en bauds en bits par seconde.

4.5.3 Allocations futures

Les demandes d'allocations de nouveaux opcodes et de leurs arguments associés DOIVENT être faites par la méthode du CONSENSUS DE L'IETF, comme décrit dans la [RFC2434].

4.6 Noms

Dans les paragraphes qui suivent, les valeurs pour les espaces de noms sont textuelles. Les conventions et instructions à l'IANA pour les allocations futures sont données dans ce paragraphe. Les allocations initiales sont données dans leurs paragraphes respectifs.

4.6.1 Conventions pour les noms

Tous les noms enregistrés par l'IANA dans les paragraphes qui suivent DOIVENT être des chaînes US-ASCII imprimables, et NE DOIVENT PAS contenir les caractères arobase ("@"), virgule (","), espace, les caractères de contrôle (codes ASCII 32 ou moins) ou le code ASCII 127 (DEL). Les noms sont sensibles à la casse, et NE DOIVENT PAS faire plus de 64 caractères.

On fait ici une mention des noms extensibles en local. L'IANA n'enregistre pas, et ne contrôle pas, les noms qui portent en eux le caractère arobase (@).

Les noms qui comportent le signe arobase auront le format de "nom@nomdedomaine" (sans les guillemets) où la partie précédant l'arobase est le nom. Le format de la partie qui précède l'arobase n'est pas spécifié ; cependant, ces noms DOIVENT être des chaînes US-ASCII imprimables, et NE DOIVENT PAS contenir le caractère virgule (","), espace, des caractères de contrôles (codes ASCII 32 ou moins), ou le code ASCII 127 (DEL). Ils ne DOIVENT comporter qu'un seul caractère arobase. La partie qui suit l'arobase DOIT être un nom de domaine Internet valide, pleinement qualifié [RFC1034] contrôlé par la personne ou organisation qui définit le nom. Les noms sont sensibles à la casse et NE DOIVENT PAS faire plus de 64 caractères. Il appartient à chaque domaine de déterminer comment il gère son espace de noms local. On a noté que ces noms ressemblent aux adresses de messagerie électronique du STD 11 [RFC0822]. C'est une pure coïncidence et ils n'ont rien à voir avec le STD 11 [RFC0822]. Un exemple de nom défini en local est "ourcipher-cbc@example.com" (sans les guillemets).

4.6.2. Allocations futures des noms

Les demandes d'allocations de nouveaux noms DOIVENT être faites selon la méthode de CONSENSUS DE L'IETF, comme décrit dans la [RFC2434].

4.7 Noms de service

Le 'nom de service' est utilisé pour décrire une couche de protocole. Le tableau qui suit fait la liste des allocations initiales des valeurs de 'nom de service'.

Nom de service	Référence
ssh-userauth	[RFC4252]
ssh-connection	[RFC4254]

4.8 Nom de méthode d'authentification

Le nom de méthode d'authentification est utilisé pour décrire une méthode d'authentification pour le service "ssh-userauth" [RFC4252]. Le tableau qui suit identifie les allocations initiales des noms de méthode d'authentification.

Nom de méthode	Référence
publickey	[RFC4252], Section 7]
password	[RFC4252], Section 8]
hostbased	[RFC4252], Section 9]
none	[RFC4252], paragraphe 5.2]

4.9 Noms alloués de protocole de connexion

Le tableau qui suit fait la liste des allocations initiales des noms de type et de demande du protocole de connexion.

4.9.1 Types de canaux de protocole de connexion

Le tableau qui suit fait la liste des allocations initiales de types de protocole de connexion.

Type de canal	Référence
session	[RFC4254], paragraphe 6.1]
x11	[RFC4254], paragraphe 6.3.2]
forwarded-tcpip	[RFC4254], paragraphe 7.2]
direct-tcpip	[RFC4254], paragraphe 7.2]

4.9.2 Noms de demande globale de protocole de connexion

Le tableau qui suit fait la liste des allocations initiales des noms de demande globale de protocole de connexion.

Type de demande	Référence
tcpip-forward	[RFC4254], paragraphe 7.1]
cancel-tcpip-forward	[RFC4254], paragraphe 7.1]

4.9.3 Noms de demande de canal de protocole de connexion

Le tableau qui suit fait la liste des allocations initiales des noms de demande de canal de protocole de connexion.

Type de demande	Référence
pty-req	[RFC4254], paragraphe 6.2]
x11-req	[RFC4254], paragraphe 6.3.1]
env	[RFC4254], paragraphe 6.4]
shell	[RFC4254], paragraphe 6.5]
exec	[RFC4254], paragraphe 6.5]
subsystem	[RFC4254], paragraphe 6.5]
window-change	[RFC4254], paragraphe 6.7]
xon-xoff	[RFC4254], paragraphe 6.8]
signal	[RFC4254], paragraphe 6.9]
exit-status	[RFC4254], paragraphe 6.10]
exit-signal	[RFC4254], paragraphe 6.10]

4.9.4 Allocations initiales de noms de signaux

Le tableau qui suit fait la liste des allocations initiales de noms de signal.

Signal	Référence
ABRT	RFC4254]

ALRM	[RFC4254]
FPE	[RFC4254]
HUP	[RFC4254]
ILL	[RFC4254]
INT	[RFC4254]
KILL	[RFC4254]
PIPE	[RFC4254]
QUIT	[RFC4254]
SEGV	[RFC4254]
TERM	[RFC4254]
USR1	[RFC4254]
USR2	[RFC4254]

4.9.5 Noms de sous système de protocole de connexion

Il n'y a pas d'allocations initiales des noms de sous-système de protocole de connexion.

4.10 Noms de méthode d'échange de clé

Le nom "diffie-hellman-group1-sha1" est utilisé pour une méthode d'échange de clés qui utilise un groupe Oakley, comme défini dans la [RFC2409]. SSH tient son propre espace d'identifiants de groupe, qui est logiquement distinct de Oakley [RFC2412] et de IKE ; cependant, pour un groupe supplémentaire, le groupe de travail a adopté le numéro alloué par la [RFC3526], utilisant "diffie-hellman-group14-sha1" pour le nom du second groupe défini. Les mises en œuvre devraient traiter ces noms comme des identifiants opaques et ne devraient pas supposer de relation entre les groupes utilisés par SSH et les groupes définis pour IKE.

Le tableau qui suit identifie les allocations initiales des méthodes d'échange de clés.

Nom de méthode	**Référence**
diffie-hellman-group1-sha1	[RFC4253], paragraphe 8.1]
diffie-hellman-group14-sha1	[RFC4253], paragraphe 8.2]

4.11 Noms d'algorithme alloués

4.11.1 Noms d'algorithme de chiffrement

Le tableau qui suit identifie les allocations initiales des noms d'algorithme de chiffrement.

Nom d'algorithme de chiffrement	**Référence**
3des-cbc	[RFC4253], paragraphe 6.3
blowfish-cbc	[RFC4253], paragraphe 6.3
twofish256-cbc	[RFC4253], paragraphe 6.3
twofish-cbc	[RFC4253], paragraphe 6.3
twofish192-cbc	[RFC4253], paragraphe 6.3
twofish128-cbc	[RFC4253], paragraphe 6.3
aes256-cbc	[RFC4253], paragraphe 6.3
aes192-cbc	[RFC4253], paragraphe 6.3
aes128-cbc	[RFC4253], paragraphe 6.3
serpent256-cbc	[RFC4253], paragraphe 6.3
serpent192-cbc	[RFC4253], paragraphe 6.3
serpent128-cbc	[RFC4253], paragraphe 6.3
arcfour	[RFC4253], paragraphe 6.3
idea-cbc	[RFC4253], paragraphe 6.3
cast128-cbc	[RFC4253], paragraphe 6.3
none	[RFC4253], paragraphe 6.3
des-cbc	[FIPS-46-3] HISTORIQUE; voir la page 4 de [FIPS-46-3]

4.11.2 Noms d'algorithme de MAC

Le tableau qui suit identifie les allocations initiales des noms d'algorithme de MAC.

Nom d'algorithme de MAC	Référence
hmac-sha1	[RFC4253], paragraphe 6.4
hmac-sha1-96	[RFC4253], paragraphe 6.4
hmac-md5	[RFC4253], paragraphe 6.4
hmac-md5-96	[RFC4253], paragraphe 6.4
none	[RFC4253], paragraphe 6.4

4.11.3 Noms d'algorithme de clé publique

Le tableau qui suit identifie les allocations initiales des noms d'algorithme de clé publique.

Nom d'algorithme de clé publique	Référence
ssh-dss	[RFC4253], paragraphe 6.6]
ssh-rsa	[RFC4253], paragraphe 6.6]
pgp-sign-rsa	[RFC4253], paragraphe 6.6]
pgp-sign-dss	[RFC4253], paragraphe 6.6]

4.11.4 Noms d'algorithme de compression

Le tableau qui suit identifie les allocations initiales des noms d'algorithme de compression.

Nom d'algorithme de compression	Référence
none	[RFC4253], paragraphe 6.2]
zlib	[RFC4253], paragraphe 6.2]

5. Considérations sur la sécurité

Ce protocole fournit un canal chiffré sûr sur un réseau non sûr.

Les considérations de sécurité complètes pour ce protocole figurent dans la [RFC4251].

6. Références

6.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC3526] T. Kivinen et M. Kojo, "Groupes supplémentaires d'exponentiation modulaire (MODP) Diffie-Hellman pour l'échange de clés Internet (IKE)", mai 2003.

[RFC4251] T. Ylonen et C. Lonvick, "Architecture du protocole Secure Shell (SSH)", janvier 2006. *(P.S. ; MàJ par* RFC8308)

[RFC4252] T. Ylonen et C. Lonvick, éd., "Protocole d'authentification Secure Shell (SSH)", janvier 2006. *(P.S .; MàJ par* RFC8308, 8332)

[RFC4253] C. Lonvick, "Protocole de couche Transport Secure Shell (SSH)", janvier 2006. *(P.S., MàJ par* RFC6668, 8268, 8308, 8332, 8709)

[RFC4254] T. Ylonen et C. Lonvick, éd., "Protocole de connexion Secure Shell (SSH)", janvier 2006. *(P.S. ; MàJ par* RFC8308)

6.2 Références pour information

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, voir RFC*5322)

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482, 8767)

[RFC2412] H. Orman, "Protocole OAKLEY de détermination de clés", novembre 1998. *(Information)*

[FIPS-46-3] US National Institute of Standards and Technology, "Data Encryption Standard (DES)", Federal Information Processing Standards Publication 46-3, octobre 1999.

Adresse des auteurs

Sami Lehtinen
SSH Communications Security Corp
Valimotie 17
00380 Helsinki
Finland
mél : sjl@ssh.com

Chris Lonvick (editor)
Cisco Systems, Inc.
12515 Research Blvd.
Austin 78759
USA
mél : clonvick@cisco.com

Notice de marque commerciale
"ssh" est une marque commerciale déposée aux États-Unis et/ou dans d'autres pays.

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.