Groupe de travail Réseau
Request for Comments : 3779
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

C. Lynn, BBN Technologies
S. Kent, BBN Technologies
K. Seo, BBN Technologies
juin 2004

Extensions X.509 pour adresses IP et identifiants d'AS

Résumé
Le présent document définit deux extensions de certificat X.509 v3. La première lie une liste de blocs d'adresse IP, ou préfixes, au sujet d'un certificat. La seconde lie une liste d'identifiants de systèmes autonomes au sujet d'un certificat. Ces extensions peuvent être utilisées pour porter l'autorisation du sujet d'utiliser les adresses IP et les identifiants de système autonome contenus dans les extensions.

Table des matières

1. Introduction

Le présent document définit deux extensions de certificat X.509 v3 qui autorisent le transfert du droit d'utilisation pour un ensemble d'adresses IP et d'identifiants de systèmes autonomes de l'IANA par les registres régionaux de l'Internet (RIR, *regional Internet registry*) aux fournisseurs d'accès Internet (FAI) et organisations d'utilisateurs. La première lie une liste de blocs d'adresses IP, souvent représentés comme des préfixes d'adresse IP, au sujet (détenteur de clé privée) d'un certificat. La seconde lie une liste d'identifiants de systèmes autonomes (AS, *Autonomous System*) au sujet (détenteur de clé privée) d'un certificat. Le producteur du certificat est une entité (par exemple, l'IANA, un registre Internet régional, ou un FAI) qui a l'autorité de transférer la garde ("allouer") de l'ensemble de blocs d'adresses IP et d'identifiants d'AS au sujet du certificat. Ces certificats fournissent un moyen adaptable pour vérifier le droit d'utilisation d'un ensemble de préfixes d'adresses IP et d'identifiants d'AS. Ils peuvent être utilisés par les protocoles d'acheminement, comme BGP sécurisé [S-BGP], pour vérifier la légitimité et la correction des informations d'acheminement, ou par les registres d'acheminement Internet pour vérifier les

données qu'ils reçoivent.

Les Sections 2 et 3 spécifient plusieurs règles sur le codage des extensions définies dans cette spécification qui DOIVENT être suivies. Ces règles de codage servent les objets suivants. D'abord, elles résultent en un codage unique des valeurs d'extension ; deux instances d'une extension peuvent être comparées pour égalité octet par octet. Ensuite, elles réalisent la taille minimale de codage des informations. Enfin, elles permettent aux consommateurs d'assertions d'utiliser des algorithmes à un seul passage quand ils effectuent la validation du chemin de certification ; en particulier, les consommateurs d'assertions n'ont pas besoin de trier les informations, ou de mettre en œuvre du code supplémentaire dans les algorithmes de vérification de sous ensembles pour traiter les cas de frontières multiples (gammes adjacentes, se chevauchant, ou s'incluant).

1.1 Terminologie

Le lecteur est supposé familier des termes et concepts décrits dans "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet" [RFC3280], "Protocole Internet" [RFC0791], "Architecture d'adressage du protocole Internet version 6 (IPv6)" [RFC3513], "Lignes directrices pour l'allocation des adresses IP par les registraires Internet" [RFC2050], et les documents en rapport de politique de gestion d'adresse des registraires Internet régionaux. Certains des termes pertinents sont :

allouer : transfert de la garde d'une ressource à une organisation intermédiaire (voir la [RFC2050]).

affecter : transfert de la garde d'une ressource à une organisation finale (voir la [RFC2050]).

système autonome (AS, *Autonomous System*) : ensemble de routeurs sous une seule administration technique avec une politique uniforme, utilisant un ou plusieurs protocoles de passerelle intérieure et métriques pour déterminer comment acheminer les paquets au sein du système autonome, et utilisant un protocole de passerelle extérieure pour déterminer comment acheminer les paquets aux autres systèmes autonomes.

numéro de système autonome : numéro de 32 bits qui identifie un système autonome.

déléguer : transfert de la garde (c'est-à-dire, du droit d'utilisation) d'un bloc d'adresses IP ou d'identifiants d'AS par la production d'un certificat à une entité.

octet initial : premier octet de la valeur d'une CHAINE BINAIRE codée en DER [X.690].

adresse IPv4 : identifiant de 32 bits écrit comme quatre chiffres décimaux, chacun dans la gamme de 0 à 255, séparés par un ".". 10.5.0.5 est un exemple d'adresse IPv4.

adresse IPv6 :- identifiant de 128 bits écrit comme huit quantités hexadécimales, chacune dans la gamme de 0 à ffff, séparées par un ":". 2001:0:200:3:0:0:0:1 est un exemple d'adresse IPv6. Une chaîne de champs :0: peut être remplacée par "::", donc 2001:0:200:3::1 représente la même adresse que l'exemple immédiatement précédant. (Voir la [RFC3513]).

préfixe : chaîne binaire qui consiste en un certain nombre de bits initiaux d'une adresse, écrits comme une adresse, suivis par un "/", et le nombre de bits initiaux. 10.5.0.0/16 et 2001:0:200:3:0:0:0:0/64 (ou 2001:0:200:3::/64) sont des exemples de préfixes. Un préfixe est souvent abrégé en omettant les champs de moindre poids de zéros, mais il devrait y avoir assez de champs pour contenir le nombre indiqué de bits initiaux. 10.5/16 et 2001:0:200:3/64 sont des exemples de préfixes abrégés.

registre Internet régional (RIR) : tout organisme reconnu par l'IANA comme autorité régionale de gestion des adresses IP et identifiants d'AS. Au moment de la rédaction, cela inclut AfriNIC, APNIC, ARIN, LACNIC, et RIPE NCC.

droit d'utilisation : pour un préfixe d'adresse IP, être autorisé à spécifier l'AS qui peut générer des annonces du préfixe à travers l'Internet. Pour un identifiant de système autonome, être autorisé à opérer sur un ou des réseaux qui s'identifient aux autres opérateurs de réseau en utilisant cet identifiant de système autonome.

octets suivants : du second au dernier octet dans la valeur d'une CHAINE BINAIRE codée en DER [X.690].

ancre de confiance : certificat qui est de confiance lorsque on effectue la validation du chemin de certification (voir la [RFC3280]).

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Extension de délégation d'adresse IP

Cette extension porte l'allocation des adresses IP à une entité en liant ces adresses à une clé publique qui appartient à l'entité.

2.1 Contexte

L'espace d'adresses IP est actuellement géré par une hiérarchie dont la racine est l'IANA, mais qui est gérée par les RIR. L'IANA alloue l'espace d'adresses IP aux RIR, qui à leur tour allouent l'espace d'adresses IP aux fournisseurs d'accès Internet (FAI) qui peuvent allouer l'espace d'adresses IP à des fournisseurs en aval, à des clients, etc. Les RIR peuvent aussi affecter un espace d'adresses IP aux organisations qui sont des entités terminales, c'est-à-dire, des organisations qui ne vont pas réallouer de parties de leur espace à d'autres organisations. (Voir la [RFC2050] et les documents relatifs à la politique des RIR pour les directives sur le processus d'allocation et d'affectation).

L'extension de délégation d'adresse IP est destinée à permettre la vérification de la délégation appropriée des blocs d'adresses IP, c'est-à-dire, de l'autorisation d'une entité d'utiliser ou sous allouer l'espace d'adresses IP. En conséquence, il y a du sens à tirer parti du caractère autorisatoire inhérent au cadre administratif existant pour allouer l'espace d'adresses IP. Comme décrit à la Section 1, cela va se faire en produisant des certificats qui portent l'extension décrite dans cette section. Un exemple d'utilisation des informations de cette extension est une entité qui l'utilise pour vérifier l'autorisation d'une organisation pour générer un BGP UPDATE annonçant un chemin pour un bloc particulier d'adresses IP ; voir, par exemple, la [RFC1771], ou [S-BGP].

2.1.1 Codage d'une adresse ou d'un préfixe IP

Il y a deux familles d'adresses IP : IPv4 et IPv6.

Une adresse IPv4 est une quantité de 32 bits qui est écrite avec quatre nombres décimaux, chacun dans la gamme de 0 à 255, séparés par un point ("."). 10.5.0.5 est un exemple d'adresse IPv4.

Une adresse IPv6 est une quantité de 128 bits qui est écrite comme huit nombres hexadécimaux, chacun dans la gamme de 0 à ffff, séparés par deux points (":") ; 2001:0:200:3:0:0:0:1 est un exemple d'adresse IPv6. Les adresses IPv6 ont fréquemment des champs adjacents dont la valeur est 0. Un tel groupe de champs de 0 peut être abrégé par deux caractères deux points ("::"). L'exemple précédent peut donc être représenté par 2001:0:200:3::1.

Un préfixe d'adresse est un ensemble de 2^k adresses continues dont les bits de poids fort sont identiques. Par exemple, l'ensemble des 512 adresses IPv4 de 10.5.0.0 à 10.5.1.255 ont toutes les mêmes 23 bits de poids fort. L'ensemble d'adresses est écrit en ajoutant une barre oblique ("/") et le nombre de bits constants à la plus basse adresse de l'ensemble. Le préfixe pour l'exemple est 10.5.0.0/23, et contient 2^(32-23) = 2^9 adresses. L'ensemble d'adresses IPv6 2001:0:200:0:0:0:0:0 à 2001:0:3ff:ffff:ffff:ffff:ffff:ffff (2^89 adresses) est représenté par 2001:0:200:0:0:0:0:0/39 ou de façon équivalente par 2001:0:200::/39. Un préfixe peut être abrégé en omettant les champs de moindre poids de zéros, mais il devrait y avoir assez de champs pour contenir le nombre indiqué de bits constants. La forme abrégée de l'exemple de préfixe IPv4 est 10.5.0/23, et celle de l'exemple de préfixe IPv6 est 2001:0:200/39.

Une adresse ou préfixe IP est codé dans l'extension de délégation d'adresse IP comme une CHAINE BINAIRE ASN.1 codée en DER contenant les bits de poids fort constants. On rappelle [X.690] que le codage en DER d'une CHAINE BINAIRE consiste en le type CHAINE BINAIRE (0x03) suivi par le (codage du) nombre d'octets de la valeur, suivi par la valeur. La valeur consiste en un "octet initial" qui spécifie le nombre de bits non utilisés dans le dernier octet de valeur, suivi par les "octets suivants" qui contiennent les octets de la chaîne binaire. (Pour les adresses IP, le codage de la longueur va être juste la longueur.)

Dans le cas d'une seule adresse, tous les bits sont constants, de sorte que la chaîne binaire pour une adresse IPv4 contient 32 bits. Les octets suivants dans le codage DER de l'adresse 10.5.0.4 sont 0x0a 0x05 0x00 0x04. Comme tous les bits dans le dernier octet sont utilisés, l'octet initial est 0x00. Les octets dans la CHAINE BINAIRE codée en DER sont donc :

```
Type   Longueur    Bits inutilisés...
0x03     0x05       0x00  0x0a 0x05 0x00 0x04
```

De même, le codage DER du préfixe 10.5.0/23 est :

```
Type   Longueur    Bits inutilisés...
0x03     0x04       0x01  0x0a 0x05 0x00
```

Dans ce cas, les trois octets suivants contiennent 24 bits, mais le préfixe n'en utilise que 23, de sorte qu'il y a un bit inutilisé dans le dernier octet, et donc l'octet initial est 1 (le DER exige que tous les bits inutilisés DOIVENT être mis à zéro).

Le codage DER de l'adresse IPv6 2001:0:200:3:0:0:0:1 est :

```
Type   Longueur    Bits inutilisés...
0x03     0x11       0x00  0x20 0x01 0x00 0x00 0x02 0x00 0x00 0x03 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x01
```

et le codage DER du préfixe 2001:0:200/39, qui a un bit inutilisé dans le dernier octet, est :

```
Type   Longueur    Bits inutilisés...
0x03     0x06       0x01  0x20 0x01 0x00 0x00 0x02
```

2.1.2 Codage d'une gamme d'adresses IP

Bien que toute gamme contiguë d'adresses IP puisse être représentée par un ensemble de préfixes contigus, une représentation plus concise est réalisée en codant la gamme comme une SEQUENCE contenant la plus petite adresse et la plus grande adresse, où chaque adresse est codée comme une CHAINE BINAIRE. Dans la SEQUENCE, la chaîne binaire qui représente la plus petite adresse dans la gamme est formée en retirant tous les bits à zéro de moindre poids de l'adresse, et la chaîne binaire représentant la plus forte adresse de la gamme est formée en retirant tous les bits à un de moindre poids. Le codage DER de CHAINE BINAIRE exige que tous les bits inutilisés dans le dernier octet soient réglés à zéro. Noter qu'un préfixe peut toujours être exprimé comme une gamme, mais une gamme ne peut pas toujours être exprimée par un préfixe.

La gamme des adresses représentée par le préfixe 10.5.0/23 est de 10.5.0.0 à 10.5.1.255. La plus faible adresse se termine sur seize bits de zéro qui sont retirés. Le codage DER de la chaîne de seize bits résultante est :

```
Type   Longueur    Bits inutilisés...
0x03     0x03       0x00  0x0a 0x05
```

La plus forte adresse se termine sur neuf bits de uns qui sont supprimés. Le codage DER de la chaîne résultante de vingt trois bits est :

```
Type   Longueur    Bits inutilisés...
0x03     0x04       0x01  0x0a 0x05 0x00
```

Le préfixe 2001:0:200/39 peut être codé comme une gamme où le codage DER de la plus petite adresse (2001:0:200::) est :

```
Type   Longueur    Bits inutilisés...
0x03     0x06       0x01  0x20 0x01 0x00 0x00 0x02
```

et la plus grande adresse (2001:0:3ff:ffff:ffff:ffff:ffff:ffff) qui, après suppression des quatre-vingt dix bits de moindre poids de uns laisse une chaîne binaire de trente huit bits, est codée :

```
Type   Longueur    Bits inutilisés...
0x03     0x06       0x02  0x20 0x01 0x00 0x00 0x00
```

Le cas particulier de tous les blocs d'adresses IP, c'est-à-dire, un préfixe de tous les bits à zéro -- "0/0", DOIT être codé en DER par un octet de longueur de un, un octet initial de zéro, et pas d'octet suivant :

```
Type   Longueur    Bits inutilisés...
0x03     0x01       0x00
```

Noter que pour les adresses IP le nombre de bits zéro en queue est significatif. Par exemple, le codage DER de 10.64/12 :

```
Type   Longueur    Bits inutilisés...
0x03     0x03        0x04  0x0a 0x40
```

est différent du codage DER de 10.64.0/20 :

```
Type   Longueur    Bits inutilisés...
0x03     0x04        0x04  0x0a 0x40 0x00
```

2.2 Spécification

2.2.1 OID

L'OID pour cette extension est id-pe-ipAddrBlocks.

IDENTIFIANT D'OBJET id-pe-ipAddrBlocks ::= { id-pe 7 }

où la [RFC3280] définit :

IDENTIFIANT D'OBJET id-pkix ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

IDENTIFIANT D'OBJET id-pe ::= { id-pkix 1 }

2.2.2 Criticité

Cette extension DEVRAIT être CRITIQUE. L'usage prévu de cette extension est de connoter un droit d'utilisation pour le ou les blocs d'adresses IP identifiés dans l'extension. Une autorité de certification (CA) marque l'extension comme CRITIQUE pour porter la notion qu'un consommateur d'assertions DOIT comprendre la sémantique de l'extension pour faire usage du certificat selon l'objet qui lui a été assigné. Les applications nouvellement créées qui utilisent des certificats contenant cette extension sont supposés reconnaître l'extension.

2.2.3 Syntaxe

```
IDENTIFIANT D'OBJET id-pe-ipAddrBlocks  ::= { id-pe 7 }

IPAddrBlocks   ::= SEQUENCE DE IPAddressFamily

IPAddressFamily    ::= SEQUENCE {                    -- AFI & SAFI facultatif --
    addressFamily        CHAINE BINAIRE (TAILLE (2..3)),
    ipAddressChoice      IPAddressChoice }

IPAddressChoice    ::= CHOIX {
    inherit                NUL,                      -- hérité du producteur --
    addressesOrRanges    SEQUENCE DE IPAddressOrRange }

IPAddressOrRange   ::= CHOIX {
    addressPrefix       IPAddress,
    addressRange        IPAddressRange }

IPAddressRange   ::= SEQUENCE {
    min               IPAddress,
    max               IPAddress }

IPAddress   ::=  CHAINE BINAIRE
```

2.2.3.1 Type IPAddrBlocks

Le type IPAddrBlocks est une SEQUENCE de types IPAddressFamily.

2.2.3.2 Type IPAddressFamily

Le type IPAddressFamily est une SEQUENCE contenant un élément addressFamily et un élément ipAddressChoice.

2.2.3.3 Élément addressFamily

L'élément addressFamily est une CHAINE BINAIRE contenant un identifiant de famille d'adresse (AFI, *Address Family Identifier*) de deux octets, dans l'ordre des octets du réseau, facultativement suivi par un identifiant de famille d'adresse suivante (SAFI, *Subsequent Address Family Identifier*) d'un octet. Les AFI et les SAFI sont spécifiés dans [IANA-AFI] et [IANA-SAFI], respectivement.

Si aucune autorisation n'est accordée pour un AFI particulier et un SAFI facultatif, alors il NE DOIT PAS y avoir de membre IPAddressFamily pour cet AFI/SAFI dans la SEQUENCE IPAddrBlocks.

Il DOIT y avoir seulement une SEQUENCE IPAddressFamily par combinaison unique de AFI et SAFI. Chaque SEQUENCE DOIT être ordonnée par valeur croissante de addressFamily (en traitant les octets comme des quantités non signées). Une addressFamily sans SAFI DOIT précéder une qui en contient un. Quand des adresses IPv4 et IPv6 sont spécifiées, les adresses IPv4 DOIVENT précéder les adresses IPv6 (car l'AFI IPv4 de 0001 est moins que l'AFI IPv6 de 0002).

2.2.3.4 Élément ipAddressChoice et type IPAddressChoice

L'élément ipAddressChoice est du type IPAddressChoice. Le type IPAddressChoice est un CHOIX d'élément inherit ou addressesOrRanges.

2.2.3.5 Élément inherit

Si le CHOIX IPAddressChoice contient l'élément inherit, alors l'ensemble d'adresses IP autorisé pour l'AFI spécifié et le SAFI facultatif est pris dans le certificat du producteur, ou dans le certificat de producteur du producteur, de façon récurrente, jusqu'à ce que un certificat contenant un IPAddressChoice contenant un élément addressesOrRanges soit localisé.

2.2.3.6 Élément addressesOrRanges

L'élément addressesOrRanges est une SEQUENCE DE types IPAddressOrRange. Les éléments addressPrefix et addressRange DOIVENT être triés en utilisant la représentation binaire de :

<plus petite adresse IP dans la gamme> | <longueur de préfixe>

où "|" représente l'enchaînement. Noter que les octets dans cette représentation (a.b.c.d | longueur pour IPv4 ou s:t:u:v:w:x:y:z | longueur pour IPv6) ne sont pas les octets qui sont dans la valeur de CHAINE BINAIRE codée en DER. Par exemple, soient deux addressPrefix :

Adresse IP	longueur		Codage DER
	Type	Long	Bits inutilisés...
10.32.0.0	12	03	03 04 0a 20
10.64.0.0	16	03	03 00 0a 40

le préfixe 10.32.0.0/12 DOIT venir avant le préfixe 10.64.0.0/16 car 32 est moins que 64 ; tandis que si on devait trier par la CHAINE BINAIRE DER, l'ordre serait inversé car l'octet de bits inutilisés serait trié dans l'ordre opposé. Toute paire de choix IPAddressOrRange dans une extension NE DOIT PAS se chevaucher avec une autre. Tout préfixe ou gamme d'adresses contiguës DOIT être combinée en une seule gamme ou, chaque fois que possible, un seul préfixe.

2.2.3.7 Type IPAddressOrRange

Le type IPAddressOrRange est un CHOIX d'élément addressPrefix (un préfixe ou adresse IP) ou addressRange (une gamme d'adresses IP).

La présente spécification exige que toute gamme d'adresses qui peut être codée comme un préfixe DOIT être codée en

utilisant un élément IPAddress (une CHAINE BINAIRE) et que toute gamme qui ne peut pas être codée comme un préfixe DOIT être codée en utilisant une IPAddressRange (une SEQUENCE contenant deux CHAINE BINAIRE). Le pseudo code suivant illustre comment choisir le codage d'une certaine gamme d'adresses.

SOIT N = le nombre de bits de poids fort correspondants dans les plus faibles et plus fortes adresses de la gamme
SI tous les bits restants dans la plus faible adresse sont des bits à zéro
ET tous les bits restants dans la plus forte adresse sont des bits à un
ALORS la gamme DOIT être codée comme IPAddress de N-bits
AUTREMENT, la gamme DOIT être codée comme IPAddressRange

2.2.3.8 Élément addressPrefix et type IPAddress

L'élément addressPrefix est un type IPAddress. Le type IPAddress définit une gamme d'adresses IP dans laquelle les N bits de poids fort (les plus à gauche) de l'adresse restent constants, tandis que les bits restants (32 - N bits pour IPv4, ou 128 - N bits pour IPv6) peuvent être zéro ou un. Par exemple, le préfixe IPv4 10.64/12 correspond aux adresses 10.64.0.0 à 10.79.255.255, tandis que 10.64/11 correspond à 10.64.0.0 à 10.95.255.255. Le préfixe IPv6 2001:0:2/48 représente les adresses 2001:0:2:: à 2001:0:2:ffff:ffff:ffff:ffff:ffff.

Un préfixe d'adresse IP est codé comme une CHAINE BINAIRE. Le codage DER d'une CHAINE BINAIRE utilise l'octet initial de la chaîne pour spécifier combien des bits de moindre poids du dernier octet suivant sont inutilisés. Le codage DER spécifie que ces bits inutilisés DOIVENT être réglés à zéro.

Exemple :
128.0.0.0 = 1000 0000.0000 0000.0000 0000.0000 0000
à 143.255 255 255 = 1000 1111.1111 1111.1111 1111.1111 1111
chaîne binaire à coder = 1000
Type Long Bits inutilisés...
Codage = 0x03 0x02 0x04 0x80

2.2.3.9 Élément addressRange et type IPAddressRange

L'élément addressRange est du type IPAddressRange. Le type IPAddressRange consiste en une SEQUENCE contenant une adresse IP minimum (élément min) et une adresse IP maximum (élément max). Chaque adresse IP est codée comme CHAINE BINAIRE. L'interprétation sémantique de l'adresse minimum dans une IPAddressRange est que tous les bits non spécifiés (pour la longueur complète de l'adresse IP) sont des bits zéro. L'interprétation sémantique de l'adresse maximum est que tous les bits non spécifiés sont des bits de un. La CHAINE BINAIRE pour l'adresse minimum résulte de la suppression de tous les bits zéro de moindre poids de l'adresse minimum. La CHAINE BINAIRE pour l'adresse maximum résulte de la suppression de tous les bits un de moindre poids de l'adresse maximum.

Exemple :
129.64.0.0 = 1000 0001.0100 0000.0000 0000.0000 0000
à 143.255.255.255 = 1000 1111.1111 1111.1111 1111.1111 1111
chaîne binaire minimum = 1000 0001.01
chaîne binaire maximum = 1000
Codage = SEQUENCE {
Type Long Bits inutilisés...
min 0x03 0x03 0x06 0x81 0x40
max 0x03 0x02 0x04 0x80
}

2.3 Validation de chemin de certification d'extension de délégation d'adresse IP

La validation du chemin de certification d'un certificat contenant l'extension de délégation d'adresse IP exige un traitement supplémentaire. Lorsque chaque certificat dans un chemin est validé, les adresses IP dans l'extension de délégation d'adresse IP du certificat DOIVENT être remplacées par les adresses IP dans l'extension de délégation d'adresse IP du certificat du producteur. La validation DOIT échouer quand ce n'est pas le cas. Un certificat qui est une ancre de confiance pour la validation du chemin de certification des certificats qui contiennent l'extension de délégation d'adresse IP, ainsi que tous les certificats le long du chemin, DOIVENT chacun contenir l'extension de délégation d'adresse IP. L'ensemble initial des gammes d'adresses permises est tiré du certificat d'ancre de confiance.

3. Extension de délégation d'identifiant de système autonome

Cette extension porte l'allocation des identifiants de système autonome (AS) à une entité en liant ces identifiants d'AS à une clé publique qui appartient à l'entité.

3.1 Contexte

La délégation d'identifiant d'AS est actuellement gérée par une hiérarchie dont la racine nominale est l'IANA, mais qui est gérée par les RIR. L'IANA alloue les identifiants d'AS aux RIR, qui à leur tour allouent les identifiants d'AS aux organisations qui sont des entités d'extrémité, c'est-à-dire, qui ne vont ré-allouer aucun de leurs identifiants d'AS à d'autres organisations. L'extension de délégation d'identifiant d'AS est destinée à permettre la vérification de la délégation appropriée d'identifiants d'AS, c'est-à-dire, de l'autorisation d'une entité d'utiliser ces identifiants d'AS. En conséquence, il y a du sens à tirer parti du caractère autorisatoire inhérent au cadre administratif existant pour la gestion des identifiants d'AS. Comme décrit à la Section 1, ceci va être réalisé en produisant des certificats qui portent l'extension décrite dans cette section. Un exemple d'utilisation des informations de cette extension est une entité qui l'utilise pour vérifier l'autorisation d'une organisation de gérer l'AS identifié par un identifiant d'AS dans l'extension. L'utilisation de cette extension pour représenter l'allocation des identifiants d'AS n'est pas destinée à altérer les procédures de gestion des identifiants d'AS, ou le moment où un AS devrait être utilisé, voir la [RFC1930].

3.2 Spécification

3.2.1 OID

L'OID pour cette extension est id-pe-autonomousSysIds.

IDENTIFIANT D'OBJET id-pe-autonomousSysIds ::= { id-pe 8 }

où la [RFC3280] définit :

IDENTIFIANT D'OBJET id-pkix ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5)
pkix(7) }

IDENTIFIANT D'OBJET id-pe ::= { id-pkix 1 }

3.2.2 Criticité

Cette extension DEVRAIT être CRITIQUE. L'utilisation prévue de cette extension est de connoter un droit d'utilisation pour les identifiants d'AS dans l'extension. Une CA marque l'extension comme CRITIQUE pour porter la notion qu'un consommateur d'assertions doit comprendre la sémantique de l'extension pour utiliser le certificat pour l'objet pour lequel il a été produit. Les applications nouvellement créées qui utilisent des certificats contenant cette extension sont supposés reconnaître l'extension.

3.2.3 Syntaxe

IDENTIFIANT D'OBJET id-pe-autonomousSysIds ::= { id-pe 8 }

```
ASIdentifiers  ::= SEQUENCE {
     asnum         [0] EXPLICIT ASIdentifierChoice FACULTATIF,
     rdi           [1] EXPLICIT ASIdentifierChoice FACULTATIF}

ASIdentifierChoice  ::= CHOIX {
    inherit              NULL,                          -- hérité du producteur --
    asIdsOrRanges     SEQUENCE DE ASIdOrRange }

ASIdOrRange     ::= CHOIX {
     id             ASId,
     range           ASRange }

ASRange          ::= SEQUENCE {
```

```
    min             ASId,
    max             ASId }

ASId    ::= ENTIER
```

3.2.3.1 Type ASIdentifiers

Le type ASIdentifiers est une SEQUENCE contenant une ou plusieurs formes d'identifiant de système autonome – numéros d'AS (dans l'élément asnum) ou identifiants de domaine d'acheminement (dans l'élément rdi). Quand le type ASIdentifiers contient plusieurs formes d'identifiant, l'entrée asnum DOIT précéder l'entrée rdi. Les numéros d'AS sont utilisés par BGP, et les identifiants de domaine d'acheminement sont spécifiés dans IDRP [RFC1142].

3.2.3.2 Éléments asnum, rdi, et type ASIdentifierChoice

Les éléments asnum et rdi sont tous deux de type ASIdentifierChoice. Le type ASIdentifierChoice est un CHOIX entre l'élément inherit et l'élément asIdsOrRanges.

3.2.3.3 Élément inherit

Si le choix ASIdentifierChoice contient l'élément inherit, alors l'ensemble d'identifiants d'AS autorisés est tiré du certificat du producteur ou du certificat de producteur du producteur, de façon récurrente, jusqu'à ce qu'un certificat contenant un ASIdentifierChoice contenant un élément asIdsOrRanges soit localisé. Si aucune autorisation n'est accordée pour une forme particulière d'identifiant d'AS, alors il NE DOIT PAS y avoir de membre asnum/rdi correspondant dans la séquence ASIdentifiers.

3.2.3.4 Élément asIdsOrRanges

L'élément asIdsOrRanges est une SEQUENCE de types ASIdOrRange. Aucune paire d'éléments dans la SEQUENCE asIdsOrRanges NE DOIT se chevaucher. Toute série contiguë d'identifiants d'AS DOIT être combinée en une seule gamme chaque fois que possible. Les identifiants d'AS dans l'élément asIdsOrRanges DOIVENT être triés par valeur numérique croissante.

3.2.3.5 Type ASIdOrRange

Le type ASIdOrRange est un CHOIX entre un seul entier (ASId) ou une seule séquence (ASRange).

3.2.3.6 Élément id

L'élément id a le type ASId.

3.2.3.7 Élément range

L'élément range a le type ASRange.

3.2.3.8 Type ASRange

Le type ASRange est une SEQUENCE consistant en un élément minimum et un élément maximum, et est utilisé pour spécifier une gamme de valeurs d'identifiant d'AS.

3.2.3.9 Éléments min et max

Les éléments min et max ont le type ASId. L'élément min est utilisé pour spécifier la valeur de l'identifiant d'AS minimum dans la gamme, et l'élément max spécifie la valeur de l'identifiant d'AS maximum dans la gamme.

3.2.3.10 Type ASId

Le type ASId est un ENTIER.

3.3 Validation de chemin de certification d'extension de délégation d'identifiant de système autonome

La validation de chemin de certification d'un certificat contenant l'extension de délégation d'identifiant de système autonome requiert un traitement supplémentaire. Lorsque chaque certificat dans un chemin est validé, les identifiants d'AS dans l'extension de délégation d'identifiant de système autonome de ce certificat DOIVENT être remplacés par les identifiants d'AS de l'extension de délégation d'identifiant de système autonome du certificat du producteur. La validation DOIT échouer quand ce n'est pas le cas. Un certificat qui est une ancre de confiance pour la validation de chemin de certification des certificats contenant l'extension de délégation d'identifiant de système autonome, ainsi que tous les certificats le long du chemin, DOIVENT chacun contenir l'extension de délégation d'identifiant de système autonome. L'ensemble initial des identifiants d'AS permis est tiré du certificat d'ancre de confiance.

4. Considérations sur la sécurité

La présente spécification décrit deux extensions à X.509. Comme les certificats X.509 sont signés numériquement, aucun service supplémentaire de protection de l'intégrité n'est nécessaire. Les certificats qui ont ces extensions n'ont pas besoin de rester secrets, et un accès sans restriction et anonyme à ces certificats n'a pas d'implications pour la sécurité.

Cependant, des facteurs de sécurité en dehors du domaine d'application de la présente spécification vont affecter l'assurance fournie aux utilisateurs de certificats. Cette section souligne les questions critiques qui devraient être considérées par les mises en œuvre, les administrateurs, et les utilisateurs.

Ces extensions représentent des informations d'autorisation, c'est-à-dire, un droit d'utilisation des adresses IP ou identifiants d'AS. Elles ont été développées pour prendre en charge une version sécurisée de BGP [S-BGP], mais peuvent être employées dans d'autres contextes. Dans le contexte de BGP sécurisé, les certificats qui contiennent ces extensions fonctionnent comme des capacités : le certificat affirme que le détenteur de la clé privée (le sujet) est autorisé à utiliser les adresses IP ou identifiants d'AS représentés dans la ou les extensions. Par suite de ce modèle de capacité, le champ Sujet est largement non pertinent pour les questions de sécurité, contrairement aux conventions PKI courantes.

5. Remerciements

Les auteurs tiennent à remercier de leurs contributions à la présente spécification Charles Gardiner, Russ Housley, James Manger, et Jim Schaad.

Appendice A -- Module ASN.1

Cet appendice normatif décrit selon la syntaxe ASN.1 les extensions d'adresse IP et d'identifiant d'AS utilisées par les composants PKI conformes.

```
IPAddrAndASCertExtn { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) mod(0) id-
                      mod-ip-addr-et-as-ident(30) }
ÉTIQUETTES EXPLICITES DE DEFINITIONS ::=
DEBUT
-- Copyright (C) The Internet Society (2004). Cette version de ce module ASN.1 fait partie de la RFC 3779 ; voir les notices
légales complètes dans la RFC elle-même.  --

-- EXPORTE TOUT --

IMPORTE

-- OID et arcs spécifiques de PKIX --
id-pe FROM PKIX1Explicit88 { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-
                             mod(0) id-pkix1-explicit(18) };

-- OID d'extension de délégation d'adresse IP --

IDENTIFIANT D'OBJET id-pe-ipAddrBlocks ::= { id-pe 7 }
```

```
-- Syntaxe d'extension de délégation d'adresse IP --

IPAddrBlocks  ::= SEQUENCE DE IPAddressFamily

IPAddressFamily     ::= SEQUENCE {                    -- AFI & SAFI facultatif --
     addressFamily         CHAINE D'OCTETS (TAILLE (2..3)),
     ipAddressChoice      IPAddressChoice }

IPAddressChoice     ::= CHOIX {
     inherit                   NUL,                          -- hérité du producteur --
     addressesOrRanges    SEQUENCE DE IPAddressOrRange }

IPAddressOrRange    ::= CHOIX {
     addressPrefix        IPAddress,
     addressRange         IPAddressRange }

IPAddressRange      ::= SEQUENCE {
     min                IPAddress,
     max                IPAddress }

IPAddress ::= CHAINE BINAIRE

-- OID d'extension de délégation d'identifiant de système autonome --

IDENTIFIANT D'OBJET id-pe-autonomousSysIds ::= { id-pe 8 }

-- Syntaxe d'extension de délégation d'identifiant de système autonome --

ASIdentifiers   ::= SEQUENCE {
      asnum          [0] ASIdentifierChoice FACULTATIF,
      rdi            [1] ASIdentifierChoice FACULTATIF }

ASIdentifierChoice  ::= CHOIX {
     inherit               NUL,                          -- hérité du producteur --
     asIdsOrRanges      SEQUENCE DE ASIdOrRange }

ASIdOrRange     ::= CHOIX {
      id                ASId,
      range             ASRange }

ASRange     ::= SEQUENCE {
      min               ASId,
      max               ASId }

ASId  ::= ENTIER

FIN
```

Appendice B -- Exemples d'extensions de délégation d'adresse IP

Une extension critique de certificat X.509 v3 qui spécifie :
des préfixes d'adresse d'envoi individuel IPv4
1) 10.0.32/20 c'est-à-dire, de 10.0.32.0 à 10.0.47.255
2) 10.0.64/24 c'est-à-dire, de 10.0.64.0 à 10.0.64.255
3) 10.1/16 c'est-à-dire, de 10.1.0.0 à 10.1.255.255
4) 10.2.48/20 c'est-à-dire, de 10.2.48.0 à 10.2.63.255
5) 10.2.64/24 c'est-à-dire, de 10.2.64.0 à 10.2.64.255
6) 10.3/16 c'est-à-dire, de 10.3.0.0 à 10.3.255.255, et

7) hérite de toutes les adresses IPv6 du certificat du producteur serait (en hexadécimal) :

```
30 46                Extension {
  06 08 2b06010505070107    extnID       1.3.6.1.5.5.7.1.7
  01 01 ff             critical
  04 37                extnValue {
    30 35               IPAddrBlocks {
      30 2b              IPAddressFamily {
        04 03 0001  01        addressFamily: IPv4 Unicast
                           IPAddressChoice
        30 24                 addressesOrRanges {
                           IPAddressOrRange
          03 04 04 0a0020          addressPrefix 10.0.32/20
                           IPAddressOrRange
          03 04 00 0a0040          addressPrefix 10.0.64/24
                           IPAddressOrRange
          03 03 00 0a01            addressPrefix    10.1/16
                           IPAddressOrRange
          30 0c                 addressRange {
            03 04 04 0a0230         min       10.2.48.0
            03 04 00 0a0240         max       10.2.64.255
                            } -- addressRange
                           IPAddressOrRange
          03 03 00 0a03            addressPrefix    10.3/16
                        } -- addressesOrRanges
                      } -- IPAddressFamily
      30 06            IPAddressFamily {
        04 02 0002           addressFamily: IPv6
                         IPAddressChoice
        05 00                hérite du producteur
                      } -- IPAddressFamily
                    } -- IPAddrBlocks
                  } -- extnValue
                } -- Extension
```

Cet exemple illustre comment sont triés les préfixes et les gammes.

+ Le préfixe 1 DOIT précéder le préfixe 2, même si le nombre de bits inutilisés (4) dans le préfixe 1 est supérieur au nombre de bits inutilisés (0) dans le préfixe 2.

+ Le préfixe 2 DOIT précéder le préfixe 3 même si le nombre d'octets (4) dans le codage de CHAINE BINAIRE du préfixe 2 est supérieur au nombre d'octets (3) dans le codage de CHAINE BINAIRE du préfixe 3.

+ Les préfixes 4 et 5 sont adjacents (représentant la gamme d'adresses de 10.2.48.0 à 10.2.64.255) et donc DOIVENT être combinés en une gamme (car la gamme ne peut pas être codée par un seul préfixe).

+ Noter que les six bits à zéro en queue dans l'élément max de la gamme sont significatifs pour l'interprétation de la signification de la valeur (car tous les bits inutilisés sont interprétés comme étant des 1, pas des 0). Les quatre bits à zéro en queue dans l'élément ne sont pas significatifs et DOIVENT être retirés (donc les (4) bits inutilisés dans le codage de l'élément min). (Le codage en DER exige que tous les bits inutilisés dans le dernier octet suivant DOIVENT être réglés à zéro.)

+ La gamme formée par les préfixes 4 et 5 DOIT précéder le préfixe 6 même si l'étiquette SEQUENCE pour une gamme (30) est supérieure à l'étiquette pour la CHAINE BINAIRE (03) utilisée pour coder le préfixe 6.

+ Les informations IPv4 DOIVENT précéder les informations IPv6 car l'identifiant de famille d'adresse pour IPv4 (0001) est moins que l'identifiant pour IPv6 (0002).

Une extension qui spécifie le préfixe IPv6 2001:0:2/48 et les préfixes IPv4 10/8 et 172.16/12, et qui hérite de toutes les adresses de diffusion groupée IPv4 du certificat du producteur serait (en hexadécimal) :

```
30 3d                Extension {
  06 08 2b06010505070107   extnID      1.3.6.1.5.5.7.1.7
  01 01 ff             critical
  04 2e                extnValue {
    30 2c              IPAddrBlocks {
      30 10            IPAddressFamily {
        04 03 0001 01        addressFamily: IPv4 Unicast
                       IPAddressChoice
        30 09              addressesOrRanges {
                         IPAddressOrRange
          03 02 00 0a            addressPrefix    10/8
                         IPAddressOrRange
          03 03 04 ac10          addressPrefix    172.16/12
                       } -- addressesOrRanges
                     } -- IPAddressFamily
      30 07            IPAddressFamily {
        04 03 0001 02        addressFamily: IPv4 Multicast
                       IPAddressChoice
        05 00              hérité du producteur
                     } -- IPAddressFamily
      30 0f            IPAddressFamily {
        04 02 0002           addressFamily: IPv6
                       IPAddressChoice
        30 09              addressesOrRanges {
                         IPAddressOrRange
          03 07 00 200100000002    addressPrefix   2001:0:2/47
                       } -- addressesOrRanges
                     } -- IPAddressFamily
                   } -- IPAddrBlocks
                 } -- extnValue
               } -- Extension
```

Appendice C -- Exemple d'extension de délégation d'un identifiant d'AS

Une extension qui spécifie les numéros d'AS 135, 3000 à 3999, et 5001, et qui hérite de tous les identifiants de domaine d'acheminement du certificat du producteur serait (en hexadécimal) :

```
30 2b                Extension {
  06 08 2b06010505070108   extnID      1.3.6.1.5.5.7.1.8
  01 01 ff             critical
  04 1c                extnValue {
    30 1a              ASIdentifiers {
      a0 14              asnum
                       ASIdentifierChoice
        30 12              asIdsOrRanges {
                         ASIdOrRange
          02 02 0087             ASId
                         ASIdOrRange
          30 08              ASRange {
            02 02 0bb8             min
              02 02 0f9f           max
                         } -- ASRange
                         ASIdOrRange
          02 02 1389             ASId
                       } -- asIdsOrRanges
                     } -- asnum
      a1 02            rdi {
                       ASIdentifierChoice
        05 00              hérité du producteur
```

```
    } -- rdi
   } -- ASIdentifiers
  } -- extnValue
} -- Extension
```

Appendice D – Utilisation de certificats d'attribut X.509

Cet appendice discute les questions qui découlent d'une proposition d'utiliser les certificats d'attributs (AC, comme spécifié dans la [RFC3281]) pour convoyer, des registres Internet régionaux (RIR) aux organisations d'utilisateur final, le "droit d'utilisation" des blocs d'adresses IP ou identifiants d'AS.

Les deux ressources, identifiants d'AS et blocs d'adresses IP, sont actuellement gérées de façon différente. Toutes les organisations avec le droit d'utilisation pour un identifiant d'AS reçoivent l'autorisation directement d'un RIR. Les organisations qui ont un droit d'utilisation pour un bloc d'adresses IP reçoivent l'autorisation soit directement d'un RIR, soit indirectement, par exemple, d'un fournisseur de service en aval, qui peut recevoir son autorisation d'un fournisseur d'accès Internet, qui à son tour obtient son autorisation d'un RIR. Noter que les identifiants d'AS pourraient être sous alloués à l'avenir, de sorte que les mécanismes utilisés ne devraient pas s'appuyer sur une hiérarchie à trois niveaux.

À la Section 1 de la RFC 3281, deux raisons sont données pour préférer l'utilisation des AC à l'utilisation de certificats de clé publique (PKC) avec des extensions qui portent les informations d'autorisation :
"Les informations d'autorisation peuvent être placées dans un PKC d'extension ou placées dans un certificat d'attribut séparé. Le placement des informations d'autorisation dans des PKC est généralement indésirable pour deux raisons. D'abord, les informations d'autorisation n'ont souvent pas la même durée de vie que le lien de l'identité et de la clé publique. Quand les informations d'autorisation sont placées dans un PKC d'extension, le résultat général est le raccourcissement de la durée de vie utile du PKC. Ensuite, le producteur de PKC n'est généralement pas d'autorité pour les informations d'autorisation. Il en résulte des étapes supplémentaires pour que le producteur de PKC obtienne les informations d'autorisation de la source d'autorité."

"Pour ces raisons, il est souvent meilleur de séparer les informations d'autorisation du PKC. Déjà, les informations d'autorisation ont aussi besoin d'être liées à une identité. Un AC fournit ce lien ; c'est simplement une identité signée numériquement (ou certifiée) et un ensemble d'attributs."

Dans le cas des autorisations d'adresse IP et identifiant d'AS, ces raisons ne s'appliquent pas. D'abord, les certificats de clé publique sont produits exclusivement pour l'autorisation, de sorte que la durée de vie du certificat correspond exactement à la durée de vie de l'autorisation, qui est souvent liée à une relation contractuelle entre le producteur et l'entité qui a reçu l'autorisation. Les noms de sujet et de producteur ne sont utilisés que pour le chaînage durant la validation du chemin de certification, et les noms n'ont pas besoin de correspondre à une entité physique. Le nom de sujet dans les PKC peut en fait être alloué au hasard par la CA productrice, permettant un anonymat limité au détenteur de la ressource. Ensuite, la hiérarchie de certificats est construite de telle sorte que le producteur de certificat soit d'autorité pour les informations d'autorisation.

Donc les deux points dans le premier paragraphe cité ci-dessus ne sont pas vrais dans le cas d'allocations de numéro d'AS et de bloc d'adresses IP. Le point du second paragraphe cité n'est aussi pas applicable car les ressources ne sont pas liées à une identité mais au détenteur de la clé privée correspondant à la clé publique dans le PKC.

La RFC 3281 spécifie plusieurs exigences qu'un certificat d'attribut conforme doit satisfaire. En relation avec S-BGP, les exigences les plus significatives sont :

1 D'après la section 1 : "cette spécification NE RECOMMANDE PAS l'utilisation de chaînes d'AC. D'autres (futures) spécifications pourront traiter de l'utilisation de chaînes d'AC."

   L'allocation de l'IANA aux RIR aux FAI aux DSP et l'affectation aux organisations finales exigerait l'utilisation de chaînes, au moins pour les blocs d'adresses IP. Une description de comment l'AC supérieur devrait être situé et comment il devrait être traité devrait être fournie. Les lecteurs du présent document sont encouragés à proposer des moyens pour éviter le chaînage.

2 D'après le paragraphe 4.2.9 : "Le paragraphe 4.3 définit les extensions qui PEUVENT être utilisées avec ce profil, et si elles peuvent ou non être marquées comme critiques. Si une autre extension critique est utilisée, l'AC ne se conforme pas au présent profil. Cependant, si aucune autre extension non critique n'est utilisée, l'AC se conforme au présent profil."

Cela signifie que les extensions de délégation définies dans cette spécification, qui sont critiques, ne pourraient pas être simplement placées dans un AC. Elles pourraient être utilisées si elles n'étaient pas marquées critiques, mais l'utilisation prévue exige que les extensions soient critiques afin que les certificats qui les contiennent ne puissent pas être utilisés comme des certificats d'identité par une application insouciante.

3 D'après le paragraphe 4.5 : "un producteur d'AC, NE DOIT PAS aussi être un producteur de PKC. C'est-à-dire, un producteur d'AC ne peut pas être aussi une CA."
Cela signifie que pour chaque producteur d'AC il est nécessaire d'avoir une CA séparée pour produire le PKC qui contient la clé publique du détenteur d'AC. Le producteur d'AC ne peut pas produire le PKC du détenteur, et le producteur de PKC ne peut pas signer l'AC. Donc, chaque entité dans la PKI aurait besoin de faire fonctionner un producteur d'AC en plus de sa CA. Il y aurait deux fois plus de producteurs de certificats et de CRL à traiter pour prendre en charge les certificats d'attribut que ce qui est nécessaire si des PKC sont utilisés. La possibilité de discordances survient aussi lorsque deux producteurs produisent des certificats pour un seul objet.
Le modèle d'AC de la RFC 3281 implique que le détenteur d'AC présente l'AC au vérificateur d'AC quand le détenteur veut appliquer un attribut ou une autorisation. L'usage prévu pour les extensions défini ici n'a pas d'interaction directe entre un vérificateur d'AC (un NOC) et les producteurs d'AC (tous les RIR et les NOC). Avec une signature sur un objet de droit d'utilisation revendiqué, le "vérificateur d'AC" peut localiser le PKC du détenteur d'AC, mais il n'y a pas de moyen direct de localiser le ou les AC de sujet.

4 D'après la Section 5 : "4. Le producteur d'AC DOIT être directement de confiance comme producteur d'AC (par configuration ou autrement)."
Ceci n'est pas vrai dans le cas d'un droit d'utilisation pour un bloc d'adresses IP, qui est alloué à travers une hiérarchie. La validation du chemin de certification de l'AC va exiger un chaînage à travers la hiérarchie de délégation. Avoir à configurer chaque consommateur d'assertions (NOC) à "faire confiance" à chaque autre NOC n'est pas adaptable, et une telle "confiance" a résulté en des échecs que les mécanismes de sécurité proposés sont destinés à empêcher. Une seule PKI avec une racine de confiance est utilisée, pas des milliers de producteurs d'AC individuellement de confiance par FAI.
La quantité de travail nécessaire pour valider correctement un AC est plus grande que pour le mécanisme qui place les extensions de certificat définies dans le présent document dans les PKC. Il y aurait deux fois plus de certificats à valider, en plus des AC. Cela serait un accroissement considérable de la charge de gestion nécessaire pour prendre en charge les AC.

Références

Références normatives

[IANA-AFI] http://www.iana.org/assignments/address-family-numbers .

[IANA-SAFI] http://www.iana.org/assignments/safi-namespace .

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

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[X.690] Recommandation UIT-T X.690 | ISO/CEI 8825-1:2002, "Technologies de l'information - Règles de codage de l'ASN.1 : Spécification des règles de codage de base (BER), règles de codage canoniques (CER) et règles de codage distinctives (DER)", (07/2002).

Références pour information

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, septembre 1981.

[RFC1142] D. Oran, "Protocole d'acheminement intra domaine IS-IS de l'OSI", janvier 1990. *(Historique, voir* RFC7142 ; voir ISO/CEI 10589:2002, seconde édition)

[RFC1771] Y. Rekhter, T. Li , "Protocole de routeur frontière v. 4 (BGP-4)", mars 1995. *(Obsolète, voir* RFC4271) *(D.S.)*

[RFC1930] J. Hawkinson, T. Bates, "Lignes directrices pour la création, sélection, et enregistrement d'un système autonome (AS)", mars 1996. (BCP0006)

[RFC2050] K. Hubbard, M. Kosters, D. Conrad, D. Karrenberg, J. Postel, "Lignes directrices pour l'allocation des adresses IP par les registraires Internet", novembre 1996. *(Remplace* RFC1466) (BCP0012) *(Remplacée par* RFC7020)

[RFC3281] S. Farrell et R. Housley, "Profil de certificat d'attribut Internet pour l'autorisation", avril 2002. *(Obsolète, voir* RFC5755)

[RFC3513] R. Hinden et S. Deering, "Architecture d'adressage du protocole Internet version 6 (IPv6)", avril 2003. (*Obs. voir* RFC4291)

[S-BGP] S. Kent, C. Lynn, and K. Seo, "Secure Border Gateway Protocol (S-BGP)," IEEE JSAC Special Issue on Network Security, avril 2000.

Adresse des auteurs

Charles Lynn
BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA
téléphone : +1 (617) 873-3367
mél : CLynn@BBN.Com

Stephen Kent
BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA
téléphone : +1 (617) 873-3988
mél : Kent@BBN.Com

Karen Seo
BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA
téléphone : +1 (617) 873-3152
mél : KSeo@BBN.Com

Déclaration complète de droits de reproduction

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