Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 8209
RFC mise à jour : 6487
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

M. Reynolds, IPSw
S. Turner, sn3rd
S. Kent, BBN
septembre 2017
Traduction Claude Brière de L'Isle

Profil pour les certificats de routeur BGPsec, listes de révocation de certificat, et demandes de certificat

Résumé
Le présent document définit un profil standard pour les certificats X.509 utilisés pour permettre la validation des chemins de systèmes autonomes (AS, *Autonomous System*) dans le protocole de routeur frontière (BGP, *Border Gateway Protocol*) au titre d'une extension à ce protocole connue sous le nom de BGPsec. BGP est la norme pour l'acheminement inter domaines dans l'Internet ; c'est la "colle" qui tient ensemble l'Internet. BGPsec est développé comme un des composants d'une solution qui vise l'exigence d'assurer la sécurité de BGP. Le but de BGPsec est de fournir la pleine validation du chemin d'AS fondée sur l'utilisation de fortes primitives cryptographiques. Les certificats d'entité d'extrémité (EE) spécifiés par ce profil sont produits aux routeurs au sein d'un AS. Chacun de ces certificats est produit sous un certificat d'une autorité de certification (CA, *Certification Authority*) de l'infrastructure de clé publique de ressource (RPKI, *Resource Public Key Infrastructure*). Ces certificats de CA et d'EE contiennent tous deux l'extension Ressource d'AS. Un certificat d'EE de ce type affirme que le ou les routeurs qui détiennent la clé privée correspondante sont autorisés à émettre des annonces de route sûres au nom de ou des AS spécifiés dans le certificat. Le présent document profile aussi le format des demandes de certification et spécifie les procédures de validation de chemin de certificat de consommateur d'assertions (RP, *Relying Party*) pour ces certificats d'EE. Le présent document étend la RPKI ; donc, le présent document met à jour le profil de certificat de ressource RPKI (RFC 6487).

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc8209

Table des matières

1. Introduction

Le présent document définit un profil pour les certificats X.509 d'entité d'extrémité (EE) [RFC5280] à utiliser dans le contexte de certification des chemins de systèmes autonomes (AS, *Autonomous System*) dans le protocole BGPsec. Ces certificats sont appelés "certificats de routeur BGPsec". Le détenteur de la clé privée associée au certificat de routeur BGPsec est autorisé à envoyer des annonces de route sûres (BGPsec UPDATE) au nom des AS désignés dans le certificat. Un routeur qui détient la clé privée est autorisé à envoyer des annonces de routes (à ses homologues) identifiant le numéro d'AS (ASN) comme source des annonces. Une propriété clé fournie par BGPsec est que chaque AS le long du chemin d'AS peut vérifier que les autres AS le long du chemin ont autorisé l'annonce de la route en question (au prochain AS le long du chemin d'AS).

Le présent document est un profil de la [RFC6487], qui est un profil de la [RFC5280] ; donc, le présent document met à jour la [RFC6487]. Il établit les exigences imposées à un certificat de ressource qui est utilisé comme certificat de routeur BGPsec, c'est-à-dire qu'il définit des contraintes pour que les champs du certificat et les extensions du certificat soient valides dans ce contexte. Le présent document profile aussi les demandes de certification utilisées pour acquérir les certificats de routeur BGPsec. Finalement, le présent document spécifie les procédures de validation du chemin de certificat du consommateur d'assertions (RP, *Relying Party*) pour ces certificats.

1.1 Terminologie

Le lecteur est supposé être familiarisé avec les termes et concepts décrits dans "Profil pour les certificats de ressource X.509 PKIX" [RFC6487], "Spécification du protocole BGPsec" [RFC8205], "Protocole de routeur frontière version 4 (BGP-4)" [RFC4271], "Analyse des faiblesses de la sécurité de BGP" [RFC4272], "Considérations sur la validation de chemin dans BGP" [RFC5123], et "Annonces de capacités avec BGP-4" [RFC5492].

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], [RFC8174] quand, et seulement quand ils apparaissent tout en majuscules, comme montré ci-dessus.

2. Description de ressources dans les certificats

La Figure 1 dépeint certaines des entités de l'infrastructure de clé publique de ressource (RPKI, *Resource Public Key Infrastructure*) et certains des produits générés par les entités RPKI.

L'IANA produit un certificat d'autorité de certification (CA, *Certification Authority*) à chaque registraire régional de l'Internet (RIR, *Regional Internet Registry*).

Le RIR à son tour produit un certificat de CA à un fournisseur d'accès Internet (FAI).

Le FAI à son tour produit des certificats d'EE à lui-même pour permettre la vérification des signatures sur les objets signés de la RPKI.

La CA génère aussi des listes de révocation de certificat (CRL, *Certificate Revocation List*).

Ces certificats de CA et d'EE sont appelés des "Certificats de ressource" et sont profilés dans la [RFC6487]. La [RFC6480] envisageait d'utiliser ces certificats de ressource pour permettre la vérification des manifestes [RFC6486] et des autorisations d'origine de chemin (ROA, *Route Origin Authorization*) [RFC6482]. Les ROA et les manifestes incluent les certificats de ressource utilisés pour les vérifier.

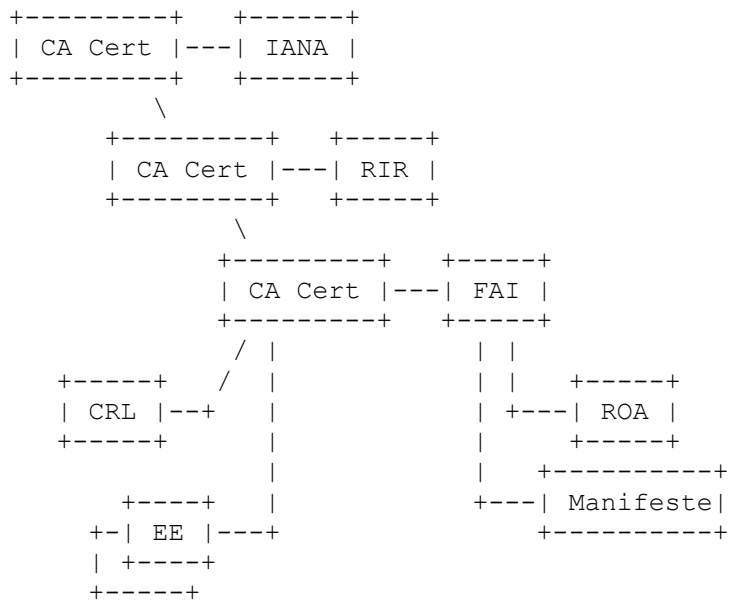

Figure 1

Le présent document définit un autre type de certificat de ressource, qui est appelé un "certificat de routeur BGPsec". L'objet de ce certificat expliqué à la Section 1 entre dans le domaine des utilisations appropriées définies dans la [RFC6484]. La production de certificats de routeur BGPsec a un impact minimal sur les CA RPKI parce que le profil de certificat de CA RPKI et de CRL reste inchangé (c'est-à-dire, il est comme spécifié dans la [RFC6487]). De plus, les algorithmes utilisés pour générer les certificats de CA RPKI qui produisent les certificats de routeur BGPsec et les CRL nécessaires pour vérifier la validité des certificcats de routeur BGPsec restent inchangés (c'est-à-dire, ils sont comme spécifié dans la [RFC7935]). Le seul impact est que les CA RPKI vont devoir être capables de traiter une demande de certificat profilée (voir au paragraphe 3.2) signée avec les algorithmes qui se trouvent dans la [RFC8208]. Les certificats de routeur BGPsec ne sont utilisés que pour vérifier la signature sur la demande de certificat BGPsec (seules les CA les traitent) et la signature sur un message BGPsec UPDATE [RFC8205] (seuls les routeurs BGPsec les traitent) ; les certificats de routeur BGPsec ne sont pas utilisés pour traiter les manifestes et les ROA ou vérifier les signatures sur les certificats ou les CRL.

Le présent document énumère seulement les différences entre ce profil et le profil de la [RFC6487]. Noter que les certificats de routeur BGPsec sont des certificats d'EE, et à ce titre il n'y a pas d'impact sur la procédure d'agilité d'algorithme décrite dans la [RFC6916].

3. Mises à jour de la RFC 6487

3.1 Champs de certificat de routeur BGPsec

Un certificat de routeur BGPsec est cohérent avec le profil de la [RFC6487] comme modifié par les spécifications de cette section. À ce titre, c'est un certificat de clé publique X.509 valide cohérent avec le profil PKIX [RFC5280]. Les différences entre ce profil et celui de la [RFC6487] sont spécifiées dans cette section.

3.1.1 Sujet

Les options de codage qui sont prises en charge pour le nom commun sont printableString *(chaîne imprimable)* et UTF8String *(chaîne UTF8)*. Pour les certificats de routeur BGPsec, il est RECOMMANDÉ que l'attribut de nom commun contienne la chaîne littérale "ROUTER-" suivie par l'ASN de 32 bits [RFC3779] codé comme huit chiffres hexadécimaux et que l'attribut de numéro de série contienne l'identifiant BGP de 32 bits [RFC4271] (c'est-à-dire, l'identifiant de routeur) codé comme huit chiffres hexadécimaux. Si il y a plus d'un ASN, le choix duquel inclure dans le nom commun est à la discrétion du producteur. Si le même certificat est produit à plus d'un routeur (et donc si la clé privée est partagée par ces routeurs) le choix de l'identifiant de routeur utilisé dans ce nom est à la discrétion du producteur.

3.1.2 Informations de clé publique sujette

Se référer au paragraphe 3.1 de la [RFC8208].

3.1.3 Champs d'extension de certificat de routeur BGPsec version 3

3.1.3.1 Contraintes de base

Les locuteurs BGPsec sont des EE ; donc, l'extension BasicConstraints ne doit pas être présente, conformément à la [RFC6487].

3.1.3.2 Usage de clé étendu

Les certificats de routeur BGPsec DOIVENT inclure l'extension Usage de clé étendu (EKU, *Extended Key Usage*). Comme spécifié dans la [RFC6487], cette extension ne doit pas être marquée critique. Le présent document définit un EKU pour les certificats de routeur BGPsec :

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

IDENTIFIANT D'OBJET id-kp-bgpsec-router ::= { id-kp 30 }

Un routeur BGPsec DOIT exiger l'extension EKU dans tout certificat de routeur BGPsec qu'il reçoit. Si plusieurs valeurs de KeyPurposeId sont inclues, les routeurs BGPsec n'ont pas besoin de les reconnaître tous, pour autant que la valeur exigée de KeyPurposeId soit présente. Les routeurs BGPsec DOIVENT rejeter les certificats qui ne contiennent pas l'EKU de routeur BGPsec même si ils incluent l'OID anyExtendedKeyUsage défini dans la [RFC5280].

3.1.3.3 Accès aux informations de sujet

Cette extension n'est pas utilisée dans les certificats de routeur BGPsec. Elle DOIT être omise.

3.1.3.4 Ressources IP

Cette extension n'est pas utilisée dans les certificats de routeur BGPsec. Elle DOIT être omise.

3.1.3.5 Ressources d'AS

Chaque certificat de routeur BGPsec DOIT inclure l'extension Ressources d'AS, comme spécifié au paragraphe 4.8.11 de la [RFC6487]. L'extension Ressources d'AS DOIT inclure un ou plusieurs ASN, et l'élément "hérité" NE DOIT PAS être spécifié.

3.2 Profil de demande de certificat de routeur BGPsec

Se reporter à la Section 6 de la [RFC6487]. Les seules différences entre ce profil et celui de la [RFC6487] sont les suivantes :

- Extension Contraintes de base : Si elle est incluse, la CA NE DOIT PAS honorer le booléen cA si il est réglé à VRAI.
- Extension EKU : Si elle est incluse, id-kp-bgpsec-router DOIT être présent (voir au paragraphe 3.1.3.2). Si elle est incluse, la CA DOIT honorer la demande pour id-kp-bgpsec-router.
- Extension Accès aux informations du sujet (SIA, *Subject Information Access*) : Si elle est incluse, la CA NE DOIT PAS honorer la demande d'inclure l'extension.
- Le champ SubjectPublicKeyInfo est spécifié dans la [RFC8208].
- La demande est signée avec les algorithmes spécifiés dans la [RFC8208].

3.3 Validation de certificat de routeur BGPsec

La procédure de validation utilisée pour les certificats de routeur BGPsec est identique à la procédure de validation décrite à la Section 7 de la [RFC6487] (et toute RFC qui met à jour cette procédure) comme modifié ci-dessous. Par exemple, à l'étape 3 (des critères énumérés au paragraphe 7.2 de la [RFC6487]) "Le certificat contient tous les champs qui DOIVENT être présents" se réfère aux champs qui sont exigés par la présente spécification.

Les différences sont les suivantes :
- o les certificats de routeur BGPsec DOIVENT inclure l'EKU de routeur BGPsec défini au paragraphe 3.1.3.2,
- o les certificats de routeur BGPsec NE DOIVENT PAS inclure l'extension SIA,
- o les certificats de routeur BGPsec NE DOIVENT PAS inclure l'extension Ressources IP,
- o les certificats de routeur BGPsec DOIVENT inclure l'extension Ressources d'AS,
- o les certificats de routeur BGPsec DOIVENT inclure le champ subjectPublicKeyInfo décrit dans la [RFC8208].

Note : Les RP BGPsec vont devoir prendre en charge les algorithmes de la [RFC8208], qui sont utilisés pour valider les signatures BGPsec, ainsi que les algorithmes de la [RFC7935], qui sont nécessaires pour valider les signatures sur les certificats BGPsec, les certificats de CA RPKI, et les CRL RPKI.

3.4 Certificats de routeur et fonctions de signature dans la RPKI

Comme décrit à la Section 1, la principale fonction des certificats de routeur BGPsec dans la RPKI est une utilisation dans le contexte de la certification des chemins d'AS dans le protocole BGPsec.

La clé privée associée à un certificat EE de routeur peut être utilisée plusieurs fois pour générer des signatures dans plusieurs instances de segments de signature d'attribut BGPsec_PATH [RFC8205]. C'est-à-dire que le certificat de routeur BGPsec est utilisé pour valider plusieurs signatures.

Les certificats de routeur BGPsec sont mémorisés dans le répertoirte de la CA productrice, où un répertoire conforme à la [RFC6481] DOIT utiliser une extension de nom de fichier ".cer" pour le fichier de certificat.

4. Notes sur la conception

Le profil de certificat de routeur BGPsec se fonde sur le profil de certificat de ressource spécifié dans la [RFC6487]. Par suite, beaucoup des choix de conception sont ici un reflet des choix de conception du travail précédent. Le lecteur est renvoyé à la [RFC6484] pour une discussion plus complète de ces choix.

Les CA sont requises par la politique de certificat (CP, *Certificate Policy*) [RFC6484] de produire des certificats de routeur BGPsec correctement formés sans considération de ce qui est présent dans la demande de certificat, de sorte qu'il y a une certaine souplesse permise dans les demandes de certificats :
- o les certificats de routeur BGPsec sont toujours des certificats de EE ; donc, les demandes de production d'un certificat de CE résultent en des certificats de EE ;
- o les certificats de routeur BGPsec sont toujours des certificats de EE ; donc, les demandes de valeurs d'extension d'usage de clé keyCertSign et cRLSign résultent en des certificats sans aucune de ces valeurs ;
- o les certificats de routeur BGPsec incluent toujours la valeur de EKU de routeur BGPsec ; donc, les demandes sans la valeur résultent en des certificats avec la valeur ; et,
- o les certificats de routeur BGPsec n'incluent jamais l'extension SIA ; donc, les demandes avec cette extension résultent en des certificats sans l'extension.

Noter que ce comportemnt est similaire à ce que la CA inclue l'extension Ressources d'AS dans les certificats de routeur BGPsec produits, en dépit du fait qu'elle n'est pas présente dans la demande.

5. Considérations de mise en œuvre

Le présent document permet à l'opérateur d'inclure une liste d'ASN dans un certificat de routeur BGPsec. Dans ce cas, le certificat de routeur va devenir invalide si un des ASN est retiré d'un certificat de CA supérieure le long du chemin d'une

ancre de confiance. Les opérateurs pourraient choisir d'éviter cette possibilité en produisant un certificat de routeur BGPsec séparé pour chaque ASN distinct, afin que les certificats de routeur pour les ASN qui sont conservés dans le certificat de CA supérieure restent valides.

6. Considérations sur la sécurité

Les considérations sur la sécurité de la [RFC6487] s'appliquent.

Un certificat de routeur BGPsec va échouer à la validation RPKI comme défini dans la [RFC6487] parce que les algorithmes de chifrement utilisés sont différents. Par conséquent, un RP a besoin d'identifier l'EKU pour déterminer la contrainte de validation appropriée.

Un certificat de routeur BGPsec est une extension de la RPKI [RFC6480] pour englober les routeurs. C'est un élément constitutif de BGPsec qui est utilisé pour valider l'origine des signatures sur le segment de signature BGPsec des segments de chemin signés [RFC8205]. Donc, sa fonction de sécurité essentielle est la liaison sécurisée d'un ou plusieurs ASN à une clé publique, en cohérence avec la hiérarchie d'allocation/affectation de la RPKI.

Les fonctions de hachage [RFC8208] sont utilisées lors de la génération des deux extensions d'identifiant de clé (c'est-à-dire, Identifiant de clé sujette et Identifiant de clé de producteur) incluses dans les certificats BGPsec. Cependant, comme le note la [RFC6818], la résistance à la collision n'est pas une propriété requise des fonctions de hachage unidirectionnelles quand elles sont utilisés pour générer des identifiants de clés. Néanmoins, les collisions de hachage sont peu probables, mais elles sont possibles, et si il en est détecté, un opérateur devrait être alerté. Une collision d'identifiant de clé sujette pourrait causer le choix du certificat incorrect dans l'antémémoire, résultant en l'échec de la validation de signature.

7. Considérations relatives à l'IANA

Le présent document utilise deux OID dans le registre SMI pour PKIX. Un est pour le module ASN.1 [X680], [X690] dans l'Appendice A, et il vient du registre "Sécurité du SMI pou identifiant de module PKIX" de l'IANA (id-mod-bgpsec-eku). L'autre est pour l'EKU de routeur BGPsec défini au paragraphe 3.1.3.2 et à l'Appendice A, et il vient du registre "Sécurité du SMI pour les besons de clé PKIX étendue" de l'IANA (id-kp-bgpsec-router). Ces OID ont été alloués avant que la gestion de l'arc PKIX soit passée à l'IANA. Les références dans ces registres ont été mises à jour pour pointer sur le présent document.

8. Références

8.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", DOI 10.17487/RFC2119, BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3779] C. Lynn, S. Kent, K. Seo, "ExtensionsX.509 pour les adresses IP et les identifiants d'AS", juin 2004. DOI 10.17487/RFC3779, *(P.S.)*

[RFC4271] Y. Rekhter, T. Li et S. Hares, "Protocole de routeur frontière version 4 (BGP-4)", janvier 2006. DOI 10.17487/RFC4271, *(D.S. MàJ par* RFC6608, RFC8212)

[RFC5280] D. Cooper et autres, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", mai 2008. DOI 10.17487/RFC5271, (*Remplace les* RFC3280, RFC4325, RFC4630) *(P.S. ; MàJ par* RFC8398, 8399)

[RFC6481] G. Huston, R. Loomans, G. Michaelson, "Profil pour structure de répertoire de certificats de ressource", février 2012. DOI 10.17487/RFC6481, *(P.S.)*

[RFC6486] R. Austein et autres, "Manifestes pour l'infrastructure de clé publique de ressource (RPKI)", février 2012. DOI 10.17487/RFC6486, *(P.S.)*

[RFC6487] G. Huston, G. Michaelson, R. Loomans, "Profil pour les certificats de ressource X.509 PKIX", février 2012. DOI 10.17487/RFC6487, *(P.S. ; MàJ par* RFC8209)

[RFC7935] G. Huston, G. Michaelson, "Profil des algorithmes et tailles de clé à utiliser dans l'infrastructure de clé publique de ressource (RPKI)", août 2016. DOI 10.17487/RFC7935, *(P.S., MàJ par* RFC8208, RFC8608)

[RFC8174] B. Leiba, "Ambiguïté des mots clés en majuscules ou minuscules dans la RFC2119", mai 2017. BCP14. DOI 10.17487/RFC8174, *(MàJ* 2119)

[RFC8205] M. Lepinski, K. Sriram, "Spécification du protocole BGPsec", septembre 2017. DOI 10.17487/RFC8205, *(P.S. ; MàJ par* RFC8206)

[RFC8208] S. Turner, O. Borchert, "Algorithmes, formats de clé et de signature pour BGPsec", septembre 2017. DOI 10.17487/RFC8208, *(P.S. ; MàJ* RFC7935 *; rendue obsolète par* RFC8608*)*

[X680] Recommandation UIT-T X.680, ISO/CEI 8824-1, "Technologie de l'information – Notation de syntaxe abstraite n° 1 (ASN.1) : Spécification de la notation de base", août 2015, <https://www.itu.int/rec/T-REC-X.680/fr >.

[X690] Recommandation UIT-T X.690, ISO/CEI 8825-1, " Technologie de l'information – règles de codage ASN.1 : Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER)", août 2015, <https://www.itu.int/rec/T-REC-X.690/fr >.

8.2 Références pour information

[RFC4272] S. Murphy, "Analyse des faiblesses de la sécurité de BGP", janvier 2006. DOI 10.17487/RFC4272, *(Information)*

[RFC5123] R. White, B. Akyol, "Considérations sur la validation de chemin dans BGP", février 2008. DOI 10.17487/RFC51235, *(Information)*

[RFC5492] J. Scudder, R. Chandra, "Annonces de capacités avec BGP-4", février 2009. DOI 10.17487/RFC5492, (*Remplace* 3392) *(D.S. ; MàJ par* 8810*)*

[RFC6480] M. Lepinski, S. Kent, "Infrastructure pour la prise en charge de l'acheminement Internet sécurisé", février 2012. DOI 10.17487/RFC6480, *(Info.)*

[RFC6482] M. Lepinski, S. Kent, D. Kong, "Profil d'autorisations d'origine de chemin (ROA)", février 2012. DOI 10.17487/RFC6482, *(P.S.)*

[RFC6484] S. Kent, D. Kong, K. Seo, R. Watro, "Politique de certificat (CP) pour l'infrastructure de clé publique de ressources de numéro de l'Internet (RPKI)", BCP0173, février 2012. DOI 10.17487/RFC6484.

[RFC6818] P. Yee, "Mise à jour du profil de certificat d'infrastructure de clé publique Internet X.509 et de liste de révocation de certificat (CRL)", janvier 2013. DOI 10.17487/RFC6818,

[RFC6916] R. Gagliano, S. Kent, S. Turner, "Procédure d'agilité d'algorithme pour l'infrastructure de clé publique de ressource (RPKI)", BCP0182, avril 2013. DOI 10.17487/RFC6916.

Appendix A. Module ASN.1

BGPSECEKU { iso(1) identified-organization(3) dod(6) internet(1)security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-bgpsec-eku(84) }

ÉTIQUETTES EXPLICITES DE DÉFINITIONS ::=

DÉBUT

```
-- EXPORTE TOUT --

-- IMPORTE RIEN --

-- Arc d'OID --

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

-- Usage de clé étendue de routeur BGPsec --

IDENTIFIANT D'OBJET id-kp-bgpsec-router ::= { id-kp 30 }

FIN
```

Remerciements

Nous tenons à remercier Geoff Huston, George Michaelson, et Robert Loomans de leur travail sur la [RFC6487], sur lequel est fondé celui-ci. De plus, les efforts de Matt Lepinski ont été décisifs pour la préparation de ce travail. Nous souhaitons aussi remercier Rob Austein, Roque Gagliano, Richard Hansen, Geoff Huston, David Mandelberg, Sandra Murphy, et Sam Weiler de leur relecture et commentaires.

Adresse des auteurs

Mark Reynolds
Island Peak Software
328 Virginia Road
Concord, MA 01742
United States of America
mèl : mcr@islandpeaksoftware.com

Sean Turner
sn3rd
mél : sean@sn3rd.com

Stephen Kent
Raytheon BBN Technologies
10 Moulton St.
Cambridge, MA 02138
United States of America
mèl :kent@alum.mit.edu