Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 8608
Remplace la RFC 8208
RFC mise à jour : 7935
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

S. Turner, sn3rd
O. Borchert, NIST

juin 2019

Traduction Claude Brière de L'Isle

Algorithmes, formats de clé, et formats de signature BGPsec

Résumé
Le présent document spécifie les algorithmes, les paramètres d'algorithmes, les formats de clés asymétriques, les tailles de clés asymétriques, et les formats de signature utilisés dans la sécurité du protocole de routeur frontière (BGPsec, *Border Gateway Protocol Security*). Le présent document met à jour la RFC 7935 ("Profil pour les algorithmes et tailles de clé à utiliser dans l'Infrastructure de clé publique de ressource") et rend obsolète la RFC 8208 ("Algorithmes, formats de clé, et formats de signature BGPsec") en ajoutant les identifiants de documentation et d'algorithmes d'expérimentation, en corrigeant la gamme des identifiants d'algorithmes non alloués pour remplir la gamme complète, et en restructurant le document pour en améliorer la lecture.

Le présent document inclut aussi des exemples de messages BGPsec UPDATE ainsi que des clés privées utilisées pour générer les messages et les certificats nécessaires pour valider ces signatures.

Statut de ce mémoire
Ceci est un document de l'Internet en cours de 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/rfc8608

Table des matières

1. Introduction

Le présent document spécifie :
- l'algorithme et les paramètres de signature numérique,
- l'algorithme et les paramètres de hachage,
- l'allocation et la classification de l'identifiant d'algorithme,
- les formats de clé publique et privée,
- les formats de signature,

utilisés par les autorités de certification (CA, *Certification Authority*) de l'infrastructure de clé publique de ressource (RPKI, *Resource Public Key Infrastructure*) et les locuteurs de la sécurité du protocole de routeur frontière (BGPsec, *Border Gateway Protocol Security*) (c'est-à-dire, les routeurs). Les CA utilisent ces algorithmes pour traiter les demandes de certificats de routeur BGPsec [RFC8209]. Des exemples de quand les routeurs BGPsec utilisent ces algorithmes incluent de demander des certificats BGPsec [RFC8209], de signer des messages BGPsec UPDATE [RFC8205], et de vérifier les signatures sur les messages BGPsec UPDATE [RFC8205].

Le présent document met à jour la [RFC7935] et ajoute la prise en charge de a) un algorithme différent pour les demandes de certificatBGPsec, qui ne sont produites que par des locuteurs BGPsec ; b) un format différent d'informations de clé publique sujette pour les certificats BGPsec, qui est nécessaire pour l'algorithme de signature BGPsec spécifié ; et c) différents formats de signature pour les signatures BGPsec, qui sont nécessaires pour l'algorithme de signature BGPsec spécifié. Les certificats BGPsec sont différenciés des autres certificats RPKI par l'utilisation de l'usage de clé étendue BGPsec comme défini dans la [RFC8209]. BGPsec utilise un algorithme différent [RFC6090] [DSS] du reste de la RPKI pour fournir une sécurité similaire avec de plus petites clés, rendant les certificats plus courts ; ces algorithmes résultent aussi en de plus petites signatures, ce qui rend les PDU plus courtes.

L'Appendice A (non normatif) contient des exemples de messages BGPsec UPDATE ainsi que des clés privées utilisées pour générer les messages et les certificats nécessaires pour valider les signatures.

1.1 Terminologie

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.

1.2 Changements par rapport à la RFC 8208

Ce paragraphe décrit les changements significatifs entre la [RFC8208] et le présent document.

- Ajout du paragraphe 2.1 contenant les types d'identifiants d'algorithmes. L'interprétation de ces identifiants est aussi décrite.

- Restructuration des Sections 2 et 3 pour les aligner avec la valeur correspondante d'identifiant de suite d'algorithme.

- Correction de la gamme des valeurs d'identifiant de suite d'algorithmes non allouées.

- Ajout des valeurs d'identifiant de suite d'algorithme de documentation.

- Ajout des valeurs d'identifiant de suite d'algorithme d'expérimentation.

- Changement du prochain bond IP dans l'exemple IPv6 de l'Appendice A pour utiliser une adresse IPv6 d'usage privé.

2. Algorithmes

Les algorithmes utilisés pour calculer les signatures sur les certificats de CA, les certificats de routeur BGPsec, et les listes de révocation de certificat (CRL, *Certificate Revocation List*) sont comme spécifié à la Section 2 de la [RFC7935]. Cette section traite des algorithmes utilisés par BGPsec [RFC8205] [DSS]. Par exemple, ces algorithmes sont utilisés par les routeurs BGPsec pour signer et vérifier les messages BGPsec UPDATE. Pour identifier quel algorithme est utilisé, le message BGPsec UPDATE contient l'identifiant d'algorithme correspondant dans chaque bloc de signature du message BGPsec UPDATE.

2.1 Types d'identifiant d'algorithmes

Les algorithmes dans les messages BGPsec UPDATE sont identifiés par le champ Identifiant de suite d'algorithme (identifiant d'algorithme) au sein du bloc de signature (voir au paragraphe 3.2 de la [RFC8205]).

Le présent document spécifie cinq types d'identifiants d'algorithme :

- Identifiant d'algorithme réservé : les identifiants d'algorithme réservés sont les valeurs 0x00 (0) et 0xFF (255). Ces identifiants NE DOIVENT PAS être utilisés dans un bloc de signature, et si il en rencontre, le routeur DOIT traiter les messages BGPsec UPDATE comme mal formés [RFC4271].

- Identifiant d'algorithme de signature : ce sont les algorithmes de signature définis au paragraphe 2.2 du présent document. Le traitement de la signature et de la validation de BGPsec UPDATE en utilisant les algorithmes de signature est décrit en détails aux paragraphes 4.2 et 5.2 de la [RFC8205].

- Identifiant d'algorithme non alloué : ce type d'identifiant d'algorithme est libre pour de futures allocations et NE DOIT PAS être utilisé tant qu'un algorithme n'est pas officiellement alloué (voir la Section 7). Si un routeur rencontre un identifiant d'algorithme non alloué dans un des blocs de signature d'un message BGPsec UPDATE, il DEVRAIT traiter le bloc de signature comme un algorithme non pris en charge, comme spécifié au paragraphe 5.2 de la [RFC8205].

- Identifiant d'algorithme d'expérimentation : les identifiants d'algorithmes d'expérimentation s'étendent de 0xF7 (247) à 0xFA (250). Pour permettre à une expérimentation de décrire avec précision des exemples de déploiement, l'utilisation des identifiants d'algorithme alloués publiquement est inappropriée, et une liste réservée de blocs d'identifiants d'algorithmes d'expérimentation est nécesaire. Cela assure que l'expérimentation n'entre pas en conflit avec des identifiants d'algorithme alloués dans les réseaux déployés et atténue les risques à l'intégrité opérationnelle du réseau découlant de l'utilisation inappropriée de l'expérimentation pour effectuer une configuration littérale des éléments d'acheminement sur les systèmes de production. Un routeur qui rencontre un identifiant d'algorithme de ce type en dehors d'un réseau expérimental DEVRAIT le traiter de la même façon qu'un algorithme non pris en charge comme spécifié au paragraphe 5.2 de la [RFC8205].

- Identifiant d'algorithme de documentation : ils s'étendent de 0xFB (251) à 0xFE (254). Pour permettre que la documentation décrive précisément les exemples de déploiement, l'utilisation d'identifiants d'algorithmes alloués publiquement est inappropriée, et un bloc réservé d'identifiants d'algorithme de documentation est nécessaire. Cela assure que la documentation n'entre pas en conflit avec les identifiants d'algorithme alloués dans les réseaux déployés et atténue les risques pour l'intégrité opérationnelle des réseaux découlant d'une utilisation inappropriée de la documentation pour effectuer une configuration littérale des éléments d'acheminement sur les systèmes de production. Un routeur qui rencontre un identifiant d'algorithme de ce type DEVRAIT le traiter de la même façon qu'un algorithme non pris en charge, comme spécifié au paragraphe 5.2 de la [RFC8205].

2.2 Algorithmes de signature

2.2.1 Identifiant d'agorithme 0x01 (1) - (ECDSA P-256)

- L'algorithme de signature utilisé DOIT être l'algorithme de signature numérique à courbe elliptique (ECDSA, *Elliptic Curve Digital Signature Algorithm*) avec la courbe P-256 [RFC6090], [DSS].

- L'algorithme de hachage utilisé DOIT être SHA-256 [SHS].

Les algorithmes de hachage ne sont pas identifiés par eux-mêmes dans les certificats ou les messages BGPsec UPDATE. Ils sont représentés par un OID qui combine l'algorithme de hachage avec l'algorithme de signature numérique comme suit :

- L'OID ecdsa-with-SHA256 [RFC5480] DOIT apparaître dans le champ signatureAlgorithm de la norme de chiffrement à clé publique n° 10 (PKCS #10, *Public-Key Cryptography Standards #10*) [RFC2986] ou dans le champ d'algorithme POPOSigningKey du format de message de demande de certificat (CRMF, C*ertificate Request Message Format*) [RFC4211] ; la place de l'OID dépend du format de demande de certificat généré.

- Dans les messages BGPsec UPDATE, l'ECDSA avec la valeur de suite d'algorithme SHA-256 de 0x01 (1) (voir la Section 7) est inclus dans le champ Identifiant de suite d'algorithme de la liste de blocs de signature.

3. Formats de paire de clés asymétriques

Les formats de clés utilisés pour calculer les signatures sur les certificats de CA, les certificats de routeur BGPsec, et les CRL sont comme spécifié à la Section 3 de la [RFC7935]. Cette section vise les formats de clés qui se trouvent dans les demandes de certificat de routeur BGPsec et dans les certificats de routeur BGPsec.

3.1 Paire de clés asymétriques pour l'identifiant d'algorithme 0x01 (1) - (ECDSA P-256)

Les clés privées ECDSA utilisées pour calculer les signatures des demandes de certificat et des messages BGPsec UPDATE DOIVENT être associées aux paramètres de domaine de courbe elliptique P-256 [RFC5480]. La paire de clés publiques DOIT utiliser la forme non compressée.

3.1.1 Format de clé publique

La clé publique de sujet est incluse dans subjectPublicKeyInfo [RFC5280]. Elle a deux sous champs : algorithm et subjectPublicKey. Les valeurs pour les structures et leurs sous structures sont :

- algorithm (un type AlgorithmIdentifier) : l'OID id-ecPublicKey DOIT être utilisé dans le champ algorithm, comme spécifié au paragraphe 2.1.1 de la [RFC5480]. La valeur des paramètres associés DOIT être secp256r1, comme spécifié au paragraphe 2.1.1.1 de la [RFC5480].

- subjectPublicKey : ECPoint DOIT être utilisé pour coder le champ subjectPublicKey du certificat, comme spécifié au paragraphe 2.2 de la [RFC5480].

3.1.2 Format de clé privée

La politique locale détermine le format de clé privée.

4. Formats de signature

La structure pour les champs de certificat et de CRL DOIT être comme spécifié à la Section 4 de la [RFC7935] ; c'est le même format qu'utilisé par les autres certificats de RPKI. La structure pour le champ Signature de demande de certification et de message BGPsec UPDATE DOIT être comme spécifié au paragraphe 2.2.3 de la [RFC3279].

5. Exigences supplémentaires

Il est prévu que BGPsec va exiger l'adoption de tailles de clé mises à jour et d'un jeu différent d'algorithmes de signature et de hachage au fil du temps, afin de conserver un niveau acceptable de sécurité cryptographique. Ce profil devrait être mis à jour pour spécifier ces futures exigences, quand ce sera approprié.

Les procédures recommandées pour mettre en œuvre une telle transition de tailles de clé et d'algorithmes sont spécifiées dans la [RFC6916].

6. Considérations sur la sécurité

Les considérations sur la sécurité des [RFC3279], [RFC5480], [RFC6090], [RFC7935], et [RFC8209] s'appliquent aux certificats. Les considérations sur la sécurité des [RFC3279], [RFC6090], [RFC7935], et [RFC8209] s'appliquent aux demandes de certification. Les considérations sur la sécurité des [RFC3279], [RFC6090], et [RFC8205] s'appliquent aux messages BGPsec UPDATE. Aucune nouvelle considération sur la sécurité n'est introduite par suite de cette spécification.

7. Considérations relatives à l'IANA

L'autorité d'allocations des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*) a créé le registre "BGPsec Algorithm Suites" dans le groupe Infrastructure de clé publique de ressource (RPKI, *Resource Public Key Infrastructure*). Les identifiants de suite d'algorithme de un octet alloués par l'IANA identifient l'algorithme de résumé et l'algorithme de signature utilisés dans le champ Identifiant de suite d'algorithmes de la liste des blocs de signature BGPsec.

Conformément à la [RFC8208], l'IANA a enregistré un seul identifiant de suite d'algorithme pour l'algorithme de résumé SHA-256 [SHS] et pour l'algorithme de signature ECDSA sur la courbe P-256 [RFC6090], [DSS]. Cet identifiant est toujours valide, et l'IANA a mis à jour l'enregistrement pour se référer au présent document.

L'IANA a modifié la gamme de l'espace d'adresses "Non allouées" de "0x2-0xEF" à "0x02-0xF6" :

Identifiant de suite d'algorithme	Algorithme de résumé	Algorithme de signature	Pointeur de spécification
0x02-0xF6	Non alloué	Non alloué	

De plus, l'IANA a enregistré les espaces d'adresses suivants pour "Experimentation" et "Documentation":

Identifiant de suite d'algorithme	Algorithme de résumé	Algorithme de signature	Pointeur de spécification
0xF7-0xFA	Experimentation	Experimentation	ce document
0xFB-0xFE	Documentation	Documentation	ce document

Le registre "Suites d'algorithmes BGPsec" dans le groupe RPKI contient maintenant les valeurs suivantes :

Identifiant de suite d'algorithme	Algorithme de résumé	Algorithme de signature	Pointeur de spécification
0x00	Réservé	Réservé	ce document
0x01	SHA-256	ECDSA P-256	[SHS] [DSS] [RFC6090] ce document
0x02-0xF6	non alloué	non alloué	
0xF7-0xFA	Expérimentation	Expérimentation	ce document
0xFB-0xFE	Documentation	Documentation	ce document
0xF	Réservé	Réservé	ce document

De futures allocations seront faites en utilisant le processus d'action de normalisation défini dans la [RFC8126]. Les allocations consistent en la valeur d'identifiant de suite d'algorithme de un octet et du nom de l'algorithme de résumé et du nom de l'algorithme de signature associés.

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)

[RFC2986] M. Nystrom, B. Kaliski, "PKCS n° 10 : Spécification de la syntaxe de demande de certification, version 1.7", novembre 2000, DOI 10.17487/RFC2986, *(Information)*

[RFC3279] L. Bassham, W. Polk et R. Housley, "Algorithmes et identifiants pour le profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002, DOI 10.17487/RFC3972.

[RFC4211] J. Schaad, "Format de message de demande de certificat d'infrastructure de clé publique X.509 pour l'Internet", septembre 2005, DOI 10.17487/RFC4211, (*Remplace* RFC2511) *(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/RFC5280, (*Remplace les* RFC3280, RFC4325, RFC4630) *(P.S. ; MàJ par* RFC8398, 8399)

[RFC5480] S. Turner et autres, "Syntaxe et sémantique du champ subjectPublicKeyInfo dans la cryptographie à courbe elliptique", mars 2009, DOI 10.17487/RFC5480, (*MàJ* RFC3279) *(P. S.)*

[RFC6090] D. McGrew, K. Igoe, M. Salter, "Algorithmes fondamentaux de cryptographie par courbe élliptique", février 2011, DOI 10.17487/RFC6090,. *(Info.)*

[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.

[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)

[RFC8126] M. Cotton, B. Leiba, T. Narten, "Lignes directrices pour la rédaction d'une section de considérations relatives à l'IANA dans les RFC", juin 2017. BCP 26, DOI 10.17487/RFC8126, *(Remplace* RFC5226)

[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*)*

[RFC8209] M. Reynolds, S. Turner, S. Kent, "Profil pour les certificats de routeur, les listes de révocation de certificat, et les demandes de certification BGPsec", septembre 2017, DOI 10.17487/RFC8209, *(P.S. ; MàJ* RFC6487*)*

[DSS] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", NIST FIPS Publication 186-4, DOI 10.6028/NIST.FIPS.186-4, July 2013, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf >.

[SHS] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", NIST FIPS Publication 180-4,DOI 10.6028/NIST.FIPS.180-4, août 2015, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf >.

8.2 Références pour information

[RFC5398] G. Huston, "Réservation de numéro de système autonome (AS) à usage documentaire", décembre 2008, DOI 10.17487/RFC5398, *(Information)*

[RFC6979] T. Pornin, "Utilisation déterministe de l'algorithme de signature numérique (DSA) et de l'algorithme de signature numérique à courbe elliptique (ECDSA)", août 2013, DOI 10.17487/RFC6979, *(Information)*

Appendice A. Exemples

A.1 Topologie et description d'expérience

Topologie :

AS(64496)----AS(65536)----AS(65537)

Annonce de préfixe : AS(64496), 192.0.2.0/24, 2001:db8::/32

L'algorithme de signature utilisé dans cet exemple est ECDSA P-256, en utilisant l'identifiant de suite d'algorithmes 0x01 (1) comme spécifié à la Section 7 du présent document.

A.2 Clés

Pour cet exemple, l'algorithme ECDSA a reçu un k statique pour rendre le résultat déterministe .

Le k utilisé pour toutes les opérations de signature a été tiré de la [RFC6979], Appendice A.2.5, "Signatures avec SHA-256, message = 'sample'".

Note : Bien que les certificats ci-dessous soient expirés, ils sont toujours utiles dans le contexte de ce document.

k = A6E3C57DD01ABE90086538398355DD4C3B17AA873382B0F24D6129493D8AAD60

Clés de AS64496 :
==========
ski: AB4D910F55CAE71A215EF3CAFE3ACC45B5EEC154

clé privée :
x = D8AA4DFBE2478F86E88A7451BF075565709C575AC1C136D081C540254CA440B9

clé publique :
Ux = 7391BABB92A0CB3BE10E59B19EBFFB214E04A91E0CBA1B139A7D38D90F77E55A
Uy = A05B8E695678E0FA16904B55D9D4F5C0DFC58895EE50BC4F75D205A25BD36FF5

Exemple de certificat de clé de routeur utilisant OpenSSL 1.0.1e-fips 11 février 2013

Certificat :
Données :
Version : 3 (0x2)
Numéro de série : 38655612 (0x24dd67c)
Algorithme de signature : ecdsa-with-SHA256
Producteur : CN=ROUTER-0000FBF0
Validité
Pas avant : Jan 1 05:00:00 2017 GMT
Pas après : Jul 1 05:00:00 2018 GMT
Sujet : CN=ROUTER-0000FBF0
Informations de clé publique sujette :
Algorithme de clé publique : id-ecPublicKey
Clé publique : (256 bit)
pub:
04:73:91:ba:bb:92:a0:cb:3b:e1:0e:59:b1:9e:bf:
fb:21:4e:04:a9:1e:0c:ba:1b:13:9a:7d:38:d9:0f:
77:e5:5a:a0:5b:8e:69:56:78:e0:fa:16:90:4b:55:
d9:d4:f5:c0:df:c5:88:95:ee:50:bc:4f:75:d2:05:
a2:5b:d3:6f:f5
OID ASN1 : prime256v1
Extensions X509v3 :
Usage de clé X509v3 :
Signature numérique

```
            Identifiant de clé sujette X509v3 :
               AB:4D:91:0F:55:CA:E7:1A:21:5E:F3:CA:FE:3A:CC:45:B5:EE:C1:54
            Usage de clé étendue  X509v3 : 1.3.6.1.5.5.7.3.30
            sbgp-autonomousSysNum : critique
               Numéro de système autonome : 64496
               Identifiants de domaine d'acheminement : hérite

      Algorithme de signature : ecdsa-with-SHA256
           30:44:02:20:07:b7:b4:6a:5f:a4:f1:cc:68:36:39:03:a4:83:
           ec:7c:80:02:d2:f6:08:9d:46:b2:ec:2a:7b:e6:92:b3:6f:b1:
           02:20:00:91:05:4a:a1:f5:b0:18:9d:27:24:e8:b4:22:fd:d1:
           1c:f0:3d:b1:38:24:5d:64:29:35:28:8d:ee:0c:38:29

-----DÉBUT DE CERTIFICAT-----
MIIBiDCCAS+gAwIBAgIEAk3WfDAKBggqhkjOPQQDAjAaMRgwFgYDVQQDDA9ST1VU
RVItMDAwMEZCRjAwHhcNMTcwMTAxMDUwMDAwWhcNMTgwNzAxMDUwMDAwWjAaMRgw
FgYDVQQDDA9ST1VURVItMDAwMEZCRjAwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNC
AARzkbq7kqDLO+EOWbGev/shTgSpHgy6GxOafTjZD3flWqBbjmlWeOD6FpBLVdnU
9cDfxYiV7lC8T3XSBaJb02/1o2MwYTALBgNVHQ8EBAMCB4AwHQYDVR0OBBYEFKtN
kQ9VyucaIV7zyv46zEW17sFUMBMGA1UdJQQMMAoGCCsGAQUFBwMeMB4GCCsGAQUF
BwEIAQH/BA8wDaAHMAUCAwD78KECBQAwCgYIKoZIzj0EAwIDRwAwRAIgB7e0al+k
8cxoNjkDpIPsfIAC0vYInUay7Cp75pKzb7ECIACRBUqh9bAYnSck6LQi/dEc8D2xOCRdZCk1KI3uDDgp
-----FIN DE CERTIFICAT-----

Clés de AS(65536):
==================
ski: 47F23BF1AB2F8A9D26864EBBD8DF2711C74406EC

clé privée :
x = 6CB2E931B112F24554BCDCAAFD9553A9519A9AF33C023B60846A21FC95583172

clé publique :
Ux = 28FC5FE9AFCF5F4CAB3F5F85CB212FC1E9D0E0DBEAEE425BD2F0D3175AA0E989
Uy = EA9B603E38F35FB329DF495641F2BA040F1C3AC6138307F257CBA6B8B588F41F

Exemple de certificat de clé de routeur utilisant OpenSSL 1.0.1e-fips 11 février 2013
---------------------------------------------------------------------
Certificat :
   Données :
      Version : 3 (0x2)
      Numéro de série : 3752143940 (0xdfa52c44)
     Algorithme de signature : ecdsa-with-SHA256
        Producteur : CN=ROUTER-00010000
        Validité
            Pas avant : Jan  1 05:00:00 2017 GMT
            Pas après : Jul  1 05:00:00 2018 GMT
         Suje t : CN=ROUTER-00010000
         Informations de clé publique sujette :
            Algorithme de clé publique : id-ecPublicKey
               Clé publique : (256 bits)
               pub:
                  04:28:fc:5f:e9:af:cf:5f:4c:ab:3f:5f:85:cb:21:
                  2f:c1:e9:d0:e0:db:ea:ee:42:5b:d2:f0:d3:17:5a:
                  a0:e9:89:ea:9b:60:3e:38:f3:5f:b3:29:df:49:56:
                  41:f2:ba:04:0f:1c:3a:c6:13:83:07:f2:57:cb:a6:b8:b5:88:f4:1f
               OID ASN1 : prime256v1

     Extensions X509v3 :
        Usage de clé X509v3 : Signature numérique
        Identifiant de clé sujette X509v3 :
           47:F2:3B:F1:AB:2F:8A:9D:26:86:4E:BB:D8:DF:27:11:C7:44:06:EC
```

```
        Usage de clé étendue X509v3 : 1.3.6.1.5.5.7.3.30
        sbgp-autonomousSysNum : critique
           Numéro de système autonome : 65536
            Identifiants de domaine d'acheminement : hérite

    Algorithme de signature : ecdsa-with-SHA256
         30:45:02:21:00:8c:d9:f8:12:96:88:82:74:03:a1:82:82:18:
         c5:31:00:ee:35:38:e8:fa:ae:72:09:fe:98:67:01:78:69:77:
         8c:02:20:5f:ee:3a:bf:10:66:être:28:d3:b3:16:a1:6b:db:66:
         21:99:ed:a6:e4:ad:64:3c:ba:bf:44:fb:cb:b7:50:91:74

-----DÉBUT DE CERTIFICAT-----
MIIBijCCATCgAwIBAgIFAN+lLEQwCgYIKoZIzj0EAwIwGjEYMBYGA1UEAwwPUk9V
VEVSLTAwMDEwMDAwMB4XDTE3MDEwMTA1MDAwMFoXDTE4MDcwMTA1MDAwMFowGjEY
MBYGA1UEAwwPUk9VVEVSLTAwMDEwMDAwMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcD
QgAEKPxf6a/PX0yrP1+FyyEvwenQ4Nvq7kJb0vDTF1qg6Ynqm2A+OPNfsynfSVZB
8roEDxw6xhODB/JXy6a4tYj0H6NjMGEwCwYDVR0PBAQDAgeAMB0GA1UdDgQWBBRH
8jvxqy+KnSaGTrvY3ycRx0QG7DATBgNVHSUEDDAKBggrBgEFBQcDHjAeBggrBgEF
BQcBCAEB/wQPMA2gBzAFAgMBAAChAgUAMAoGCCqGSM49BAMCA0gAMEUCIQCM2fgS
loiCdAOhgoIYxTEA7jU46Pqucgn+mGcBeGl3jAIgX+46vxBmvijTsxaha9tmIZntpuStZDy6v0T7y7dQkXQ=
-----FIN DE CERTIFICAT-----
```

A.3 BGPsec IPv4

UPDATE BGPsec IPv4 de l'AS(65536) à l'AS(65537):

```
==================================================
Forme binaire de BGPsec UPDATE (TCP-DUMP) :
FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF 01 03 02 00 00 00 EC 40 01 01 02 80 04 04 00 00
 00 00 80 0E 0D 00 01 01  04 C6 33 64 64 00 18 C0 00 02 90 1E 00 CD 00 0E 01 00 00 01 00 00 01 00
 00 00 FB F0 00 BF 01 47  F2 3B F1 AB 2F 8A 9D 26 86 4E BB D8 DF 27 11 C7 44 06 EC 00 48 30 46 02
 21 00 EF D4 8B 2A AC B6  A8 FD 11 40 DD 9C D4 5E 81 D6 9D 2C 87 7B 56 AA F9 91 C3 4D 0E A8 4E AF
 37 16 02 21 00 90 F2 C1  29 AB B2 F3 9B 6A 07 96 3B D5 55 A8 7A B2 B7 33 3B 7B 91 F1 66 8F D8 61
 8C 83 FA C3 F1 AB 4D 91  0F 55 CA E7 1A 21 5E F3 CA FE 3A CC 45 B5 EE C1 54 00 48 30 46 02 21 00
 EF D4 8B 2A AC B6 A8 FD  11 40 DD 9C D4 5E 81 D6 9D 2C 87 7B 56 AA F9 91 C3 4D 0E A8 4E AF 37 16
 02 21 00 8E 21 F6 0E 44  C6 06 6C 8B 8A 95 A3 C0 9D 3A D4 37 95 85 A2 D7 28 EE AD 07 A1 7E D7 AA 05 5E CA

Signature de l'AS(64496) à l'AS(65536) :
---------------------------------------
Résumé : 21 33 E5 CA A0 26 BE 07   3D 9C 1B 4E FE B9 B9 77
          9F 20 F8 F5 DE 29 FA 98   40 00 9F 60 47 D0 81 54
Signature : 30 46 02 21 00 EF D4 8B   2A AC B6 A8 FD 11 40 DD
          9C D4 5E 81 D6 9D 2C 87   7B 56 AA F9 91 C3 4D 0E
          A8 4E AF 37 16 02 21 00   8E 21 F6 0E 44 C6 06 6C
          8B 8A 95 A3 C0 9D 3A D4   37 95 85 A2 D7 28 EE AD   07 A1 7E D7 AA 05 5E CA

Signature de l'AS(65536) à l'AS(65537):
---------------------------------------
Résumé :  01 4F 24 DA E2 A5 21 90   B0 80 5C 60 5D B0 63 54
            22 3E 93 BA 41 1D 3D 82   A3 EC 26 36 52 0C 5F 84
Signature : 30 46 02 21 00 EF D4 8B   2A AC B6 A8 FD 11 40 DD
             9C D4 5E 81 D6 9D 2C 87   7B 56 AA F9 91 C3 4D 0E
             A8 4E AF 37 16 02 21 00   90 F2 C1 29 AB B2 F3 9B
             6A 07 96 3B D5 55 A8 7A   B2 B7 33 3B 7B 91 F1 66   8F D8 61 8C 83 FA C3 F1
```

Le résultat lisible par l'homme est produit en utilisant bgpsec-io, un générateur de trafic BGPsec qui utilise une impression de type Wireshark.

```
Envoie le message UPDATE
   +--marqueur : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
   +--longueur : 259
```

```
+--type : 2 (UPDATE)
+--longueur de routes retirées : 0
+--longueur totale d'attributs de chemin : 236
   +--ORIGINE : INCOMPLETE (4 octets)
   |  +--Fanions : 0x40 (Bien connu, Transitif, Complet)
   |  +--Code de type : ORIGINE (1)
   |  +--Longueur : 1 octet
   |  +--Origine : INCOMPLETE (1)
   +--MULTI_EXIT_DISC (7 octets)
   |   +--Fanions : 0x80 (Optionnel, Non transitif, Complet)
   |   +--Code de type : MULTI_EXIT_DISC (4)
   |   +--Longueur : 4 octets
   |   +--données : 00 00 00 00
   +--MP_REACH_NLRI (16 octets)
   |   +--Fanions : 0x80 (Optionnel, Non transitif, Complet)
   |   +--Code de type : MP_REACH_NLRI (14)
   |   +--Longueur : 13 octets
   |   +--Famille d'adresses : IPv4 (1)
   |   +--Identifiant de famille d'adresses suivante : Unicast (1)
   |   +--adresse du réseau de prochain bond : (4 octets)
   |   |  +--Prochain bond : 198.51.100.100
   |   +--Points de rattachement de sous réseau : 0
   |   +--Informations d'accessibilité de couche réseau : (4 octets)
   |      +--192.0.2.0/24
   |      +--Longueur de préfixe MP Reach NLRI : 24
   |      +--Préfixe IPv4 MP Reach NLRI : 192.0.2.0
   +--Attribut de chemin BGPSEC (209 octets)
      +--Fanions : 0x90 (Optionnel, Complet, Longueur étendue)
      +--Code de type : Attribut de chemin BGPSEC (30)
      +--Longueur : 205 octets
      +--Chemin sûr (14 octets)
      |   +--Longueur : 14 octets
      |   +--Segment de chemin sûr : (6 octets)
      |   |   +--pCount : 1
      |   |   +--Fanions : 0
      |   |   +--Numéro d'AS : 65536 (1.0)
      |   +--Segment de chemin sûr : (6 octets)
      |    +--pCount : 1
      |    +--Fanions : 0
      |    +--Numéro d'AS : 64496 (0.64496)
      +--Bloc de signature (191 octets)
         +--Longueur : 191 octets
         +--Identifiant d'algorithme : 1
         +--Segment de signature : (94 octets)
         |  +--SKI: 47F23BF1AB2F8A9D26864EBBD8DF2711C74406EC
         |  +--Longueur : 72 octets
         |  +--Signature : 3046022100EFD48B   2AACB6A8FD1140DD
         |                 9CD45E81D69D2C87   7B56AAF991C34D0E
         |                A84EAF3716022100   90F2C129ABB2F39B
         |                6A07963BD555A87A   B2B7333B7B91F166
         |                8FD8618C83FAC3F1
         +--Segment de signature : (94 octets)
            +--SKI: AB4D910F55CAE71A215EF3CAFE3ACC45B5EEC154
            +--Longueur : 72 octets
            +--Signature : 3046022100EFD48B   2AACB6A8FD1140DD
                           9CD45E81D69D2C87   7B56AAF991C34D0E
                           A84EAF3716022100   8E21F60E44C6066C
                           8B8A95A3C09D3AD4   379585A2D728EEAD
                           07A17ED7AA055ECA
```

A.4 BGPsec IPv6

UPDATE BGPsec IPv6 de l'AS(65536) à l'AS(65537) :
==========

Forme binaire de BGP/BGPsec UPDATE (TCP-DUMP) :
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 01 10 02 00 00 00 F9 40 01 01 02 80 04 04 00 00
00 00 80 0E 1A 00 02 01 10 FD 00 00 00 00 00 00 00 00 00 00 00 00 C6 33 64 64 00 20 20 01 0D B8 90
1E 00 CD 00 0E 01 00 00 01 00 00 01 00 00 00 FB F0 00 BF 01 47 F2 3B F1 AB 2F 8A 9D 26 86 4E BB
D8 DF 27 11 C7 44 06 EC 00 48 30 46 02 21 00 EF D4 8B 2A AC B6 A8 FD 11 40 DD 9C D4 5E 81 D6 9D
2C 87 7B 56 AA F9 91 C3 4D 0E A8 4E AF 37 16 02 21 00 D1 B9 4F 62 51 04 6D 21 36 A1 05 B0 F4 72
7C C5 BC D6 74 D9 7D 28 E6 1B 8F 43 BD DE 91 C3 06 26 AB 4D 91 0F 55 CA E7 1A 21 5E F3 CA FE 3A
CC 45 B5 EE C1 54 00 48 30 46 02 21 00 EF D4 8B 2A AC B6 A8 FD 11 40 DD 9C D4 5E 81 D6 9D 2C 87
7B 56 AA F9 91 C3 4D 0E A8 4E AF 37 16 02 21 00 E2 A0 2C 68 FE 53 CB 96 93 4C 78 1F 5A 14 A2 97
19 79 20 0C 91 56 ED F8 55 05 8E 80 53 F4 AC D3

Signature de l'AS(64496) à l'AS(65536) :

Résumé : 8A 0C D3 E9 8E 55 10 45 82 1D 80 46 01 D6 55 FC 52 11 89 DF 4D B0 28 7D 84 AC FC 77 55 6D 06 C7
Signature : 30 46 02 21 00 EF D4 8B 2A AC B6 A8 FD 11 40 DD
9C D4 5E 81 D6 9D 2C 87 7B 56 AA F9 91 C3 4D 0E
A8 4E AF 37 16 02 21 00 E2 A0 2C 68 FE 53 CB 96
93 4C 78 1F 5A 14 A2 97 19 79 20 0C 91 56 ED F8 55 05 8E 80 53 F4 AC D3

Signature de l'AS(65536) à l'AS(65537) :

Résumé : 44 49 EC 70 8D EC 5C 85 00 C2 17 8C 72 FE 4C 79 FF A9 3C 95 31 61 01 2D EE 7E EE 05 46 AF 5F D0
Signature : 30 46 02 21 00 EF D4 8B 2A AC B6 A8 FD 11 40 DD
9C D4 5E 81 D6 9D 2C 87 7B 56 AA F9 91 C3 4D 0E
A8 4E AF 37 16 02 21 00 D1 B9 4F 62 51 04 6D 21
36 A1 05 B0 F4 72 7C C5 BC D6 74 D9 7D 28 E6 1B 8F 43 BD DE 91 C3 06 26

Le résultat lisible par l'homme est produit en utilisant bgpsec-io, un générateur de trafic BGPsec qui utilise une impression de type Wireshark.

Message UPDATE envoyé
+--marqueur : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
+--longueur : 272
+--type : 2 (UPDATE)
+--longueur de routes retirées : 0
+--longueur totale des attributs de chemin : 249
+--ORIGINE : INCOMPLETE (4 octets)
| +--Fanions : 0x40 (Bien connu, Transitif, Complet)
| +--Code de type : ORIGINE (1)
| +--Longueur : 1 octet
| +--Origine : INCOMPLETE (1)
+--MULTI_EXIT_DISC (7 octets)
| +--Fanions : 0x80 (Optionnel, Non transitif, Complet)
| +--Code de type : MULTI_EXIT_DISC (4)
| +--Longueur : 4 octets
| +--données : 00 00 00 00
+--MP_REACH_NLRI (29 octets)
| +--Fanions : 0x80 (Optionnel, Non transitif, Complet)
| +--Code de type : MP_REACH_NLRI (14)
| +--Longueur : 26 octets
| +--Famille d'adresses : IPv6 (2)
| +--Identifiant de famille d'adresses suivante : Unicast (1)
| +--Adresse du réseau de prochain bond : (16 octets)
| | +--Prochain bond : fd00:0000:0000:0000:0000:0000:c633:6464
| +--Points de rattachement de sous réseau : 0
| +--Informations d'accessibilité de couche réseau : (5 octets)
| +--2001:db8::/32

```
|    +--Longueur de préfixe MP Reach NLRI : 32
|    +--Préfixe IPv6 MP Reach NLRI : 2001:db8::
+--Attribut de chemin BGPSEC (209 octets)
   +--Fanions : 0x90 (Optionnel, Complet, Longueur étendue)
   +--Code de type : Attribut de chemin BGPSEC (30)
   +--Longueur : 205 octets
   +--Chemin sûr (14 octets)
    |  +--Longueur : 14 octets
    |  +--Segment de chemin sûr : (6 octets)
    |       +--pCount : 1
    |       +--Fanions : 0
    |       +--Numéro d'AS : 65536 (1.0)
    |  +--Segment de chemin sûr : (6 octets)
    |       +--pCount : 1
    |       +--Fanions : 0
    |       +--Numéro d'AS : 64496 (0.64496)
   +--Bloc de signature (191 octets)
      +--Longueur : 191 octets
      +--Identifiant d'algorithme : 1
      +--Segment de signature : (94 octets)
       |  +--SKI : 47F23BF1AB2F8A9D26864EBBD8DF2711C74406EC
       |  +--Longueur : 72 octets
       |  +--Signature : 3046022100EFD48B   2AACB6A8FD1140DD
       |                 9CD45E81D69D2C87   7B56AAF991C34D0E
       |                 A84EAF3716022100   D1B94F6251046D21
       |                 36A105B0F4727CC5   BCD674D97D28E61B   8F43BDDE91C30626
      +--Segment de signature : (94 octets)
         +--SKI : AB4D910F55CAE71A215EF3CAFE3ACC45B5EEC154
         +--Longueur : 72 octets
         +--Signature : 3046022100EFD48B   2AACB6A8FD1140DD
                        9CD45E81D69D2C87   7B56AAF991C34D0E
                        A84EAF3716022100   E2A02C68FE53CB96
                        934C781F5A14A297   1979200C9156EDF8   55058E8053F4ACD3
```

Remerciements

Les auteurs souhaitent remercier Geoff Huston et George Michaelson qui ont produit la [RFC7935], sur laquelle se fonde entièrement le présent document. Les auteurs remercient aussi Roque Gagliano, David Mandelberg, Tom Petch, Sam Weiler, et Stephen Kent de leur relecture et commentaires. Mehmet Adalier, Kotikalapudi Sriram, et Doug Montgomery ont développé les vecteurs d'essai de l'Appendice A. De plus, nous voulons remercier Geoff Huston, auteur de la [RFC5398] à laquelle nous avons emprunté le texte du paragraphe 2.1 du présent document.

Adresse des auteurs

Sean Turner
sn3rd
mèl : sean@sn3rd.com

Oliver Borchert
NIST
100 Bureau Drive
Gaithersburg, MD 20899
United States of America
mèl : oliver.borchert@nist.gov