Groupe de travail Réseau
**Request for Comments : 4109**
**Met à jour la RFC2409**
Catégorie : Sur la voie de la normalisation

P. Hoffman, VPN Consortium
mai 2005

Traduction Claude Brière de L'Isle

# Algorithmes pour l'échange de clé Internet version 1 (IKEv1)



**Résumé**
Les algorithmes exigés et suggérés dans la spécification originale d'échange de clés Internet version 1 (IKEv1, *Internet Key Exchange version 1*) ne reflètent pas la réalité actuelle des exigences du marché pour IPsec. La spécification originale permet une sécurité faible et suggère des algorithmes qui ne sont que peu mis en œuvre. Le présent document met à jour la RFC 2409, la spécification d'origine, et est destinée à toutes les mises en œuvre de IKEv1 déployées à ce jour.

## 1. Introduction

La définition originale de IKEv1, la [RFC2409], a un ensemble d'exigences de niveau DOIT et DEVRAIT qui ne correspond pas aux besoins des utilisateurs de IPsec. Le présent document met à jour la RFC 2409 en changeant les exigences pour les algorithmes qui y sont définis.

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. Anciennes exigences pour les algorithmes

La RFC 2409 a les exigences de niveau DOIT et DEVRAIT suivantes :
- DES pour le chiffrement DOIT être pris en charge.
- MD5 et SHA-1 pour le hachage et les fonctions HMAC DOIVENT être pris en charge.
- Les secrets pré-partagés pour l'authentification DOIVENT être pris en charge.
- Le groupe 1 MODP Diffie-Hellman (logarithme discret à 768 bits) DOIT être pris en charge.
- TripleDES pour le chiffrement DEVRAIT être pris en charge.
- Tiger pour le hachage DEVRAIT être pris en charge.
- DSA et RSA pour l'authentification avec signatures DEVRAIT être pris en charge.
- RSA pour l'authentification avec chiffrement DEVRAIT être pris en charge.
- Le groupe 2 MODP Diffie-Hellman (logarithme discret à 1024 bits) DEVRAIT être pris en charge.

La RFC 2409 donne deux niveaux d'exigence contradictoires pour les groupe MODP Diffie-Hellman à courbe elliptique. La Section 4 de cette spécification dit que "les mises en œuvre de IKE ... PEUVEN prendre en charge les groupes ECP et EC2N", mais les paragraphes 6.3 et 6.4 disent que les groupes MODP 3 et 4 pour les groupes EC2N DEVRAIENT être pris en charge.

## 3. Nouvelles exigences pour les algorithmes

On donne ici la liste des nouvelles exigences pour IKEv1. Noter que certaines des exigences sont les mêmes que celles de la RFC 2409, tandis que d'autres ont changé :
- TripleDES pour le chiffrement DOIT être pris en charge.

- AES-128 en mode CBC [RFC3602] pour le chiffrement DEVRAIT être pris en charge.
- SHA-1 pour le hachage et les fonctions HMAC DOIVENT être pris en charge.
- Les secrets pré partagés pour l'authentification DOIVENT être pris en charge.
- AES-128 en mode XCBC pour les fonctions PRF ([RFC3566] et [RFC3664]) DEVRAIT être pris en charge.
- Le groupe 2 MODP Diffie-Hellman (logarithme discret à 1024 bits) DOIT être pris en charge.
- Le groupe 14 MODP Diffie-Hellman (logarithme discret à 2048 bits) [RFC3526] DEVRAIT être pris en charge.
- RSA pour l'authentification avec signatures DEVRAIT être pris en charge.

Si des mises à jour supplémentaires sont faites à IKEv1 à l'avenir, il est alors très probable que la mise en œuvre de AES-128 en mode CBC pour le chiffrement deviendra obligatoire.

Les autres algorithmes qui figuraient sur la liste aux niveaux DOIT et DEVRAIT dans la RFC 2409 sont maintenant au niveau PEUT. Cela inclut DES pour le chiffrement, MD5 et Tiger pour le hachage, le groupe 1 MODP Diffie-Hellman, les groupes MODP Diffie-Hellman avec courbes elliptiques, DSA pour l'authentification avec signatures, et RSA pour l'authentification avec chiffrement.

DES pour le chiffrement, MD5 pour le hachage, et le groupe 1 MODP Diffie-Hellman sont rétrogradés au niveau PEUT à cause de leur faiblesse cryptographique.

Tiger pour le hachage, les groupes MODP Diffie-Hellman avec courbes elliptiques, DSA pour l'authentification avec signatures, et RSA pour l'authentification avec chiffrement sont abandonnés à cause de l'absence de déploiements significatifs et du manque d'interopérabilité.

## 4. Résumé

| **Algorithme** | **RFC 2409** | **Le présent document** |
|---|---|---|
| DES pour chiffrement | DOIT | PEUT (faiblesse cryptographique) |
| TripleDES pour chiffrement | DEVRAIT | DOIT |
| AES-128 pour chiffrement | N/A | DEVRAIT |
| MD5 pour hachage et HMAC | DOIT | PEUT (faiblesse cryptographique) |
| SHA1 pour hachage et HMAC | DOIT | DOIT |
| Tiger pour hachage | DEVRAIT | PEUT (manque de déploiement) |
| AES-XCBC-MAC-96 pour PRF | N/A | DEVRAIT |
| Secrets pré partagés | DOIT | DOIT |
| RSA avec signatures | DEVRAIT | DEVRAIT |
| DSA avec signatures | DEVRAIT | PEUT (manque de déploiement) |
| RSA avec chiffrement | DEVRAIT | PEUT (manque de déploiement) |
| D-H groupe 1 (768) | DOIT | PEUT (faiblesse cryptographique) |
| D-H groupe 2 (1024) | DEVRAIT | DOIT |
| D-H groupe 14 (2048) | N/A | DEVRAIT |
| D-H à courbes elliptiques | DEVRAIT | PEUT (manque de déploiement) |

## 5. Considérations sur la sécurité

Le présent document est entièrement sur la sécurité. Tous les algorithmes qui sont soit de niveau DOIT, soit de niveau DEVRAIT dans la section "Nouvelles exigences pour les algorithmes" du présent document sont estimés assez robustes et sûrs au moment de cette rédaction.

## 6. Références normatives

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

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

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

[RFC3566] S. Frankel, H. Herbert, "L'algorithme AES-XCBC-MAC-96 et son utilisation avec IPsec", septembre 2003. *(P.S.)*

[RFC3602] S. Frankel, R. Glenn, S. Kelly, "Algorithme de chiffrement AES-CBC et utilisation avec IPsec", septembre 2003. *(P.S.)*

[RFC3664] P. Hoffman, "Algorithme AES-XCBC-PRF-128 pour le protocole d'échange de clés Internet (IKE)", janvier 2004. (*Obsolète, voir* RFC4434) *(P.S.)*

## Adresse de l'auteur

Paul Hoffman
VPN Consortium
127 Segre Place
Santa Cruz, CA 95060
US

mél : paul.hoffman@vpnc.org

## Déclaration complète de droits de reproduction



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