Groupe de travail Réseau
Request for Comments : 4945
Catégorie : sur la voie de la normalisation
Traduction Claude Brière de L'Isle

B. Korver, Network Resonance, Inc.
août 2007

Profil Internet de PKI de sécurité IP de IKEv1/ISAKMP, IKEv2, et PKIX

Statut du présent mémoire

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

Résumé

Les profils de certificat de l'échange de clé Internet (IKE, *Internet Key Exchange*) et de l'infrastructure de clé publique pour X.509 (PKIX, *Public Key Infrastructure for X.509*) fournissent tous deux des cadres qui doivent être profilés pour l'utilisation dans une application. Le présent document fournit un profil de IKE et de PKIX qui définit les exigences pour l'utilisation de la technologie PKI dans le contexte de IKE/IPsec. Le document complète les spécifications de protocole telles que IKEv1 et IKEv2, qui supposent l'existence de certificats de clé publique et des matériaux de chiffrement en rapport, mais qui ne s'adressent pas explicitement aux questions de PKI. Le présent document traite ces problèmes. L'audience visée est celle des mises en œuvre de PKI pour IPsec.

Table des matières

1. Introduction....2
2. Termes et définitions....2
3. Utilisation des certificats dans la RFC 2401 et dans IKEv1/ISAKMP....2
   3.1 Charge utile Identification....2
   3.2 Charge utile Demande de certificat....7
   3.3 Charge utile Certificat....10
4. Utilisation de certificats dans la RFC 4301 et IKEv2....13
   4.1 Charge utile Identification....13
   4.2 Charge utile Demande de certificat....13
   4.3 Charge utile Certificat....14
5. Profil de certificat pour IKEv1/ISAKMP et IKEv2....14
   5.1 Certificats X.509....14
   5.2 Listes de révocation de certificat X.509....19
   5.3 Force des algorithmes de hachage de signature....20
6. Conventions d'échange des données de configuration....20
   6.1 Certificats....21
   6.2 CRL et ARL....21
   6.3 Clés publiques....21
   6.4 Demandes de signature de certificat PKCS n° 10....21
7. Considérations sur la sécurité....21
   7.1 Charge utile Demande de certificat....21
   7.2 Mode principal IKEv1....21
   7.3 Désactivation des vérifications de certificat....21
8. Remerciements....22
9. Références....22
   9.1 Références normatives....22
   9.2 Références pour information....22
Appendice A. Dangers possibles des CRL delta....23
Appendice B. Compléments sur les CERTREQ vides....23
Adresse de l'auteur....24
Déclaration complète de droits de reproduction....24

1. Introduction

IKE [RFC2409], ISAKMP [RFC2408], et IKEv2 [RFC4306] fournissent un mécanisme d'échange de clés sécurisé à utiliser avec IPsec [RFC2401], [RFC4301]. Dans de nombreux cas, les homologues s'authentifient en utilisant des certificats numériques comme spécifié dans PKIX [RFC3280]. Malheureusement, la combinaison de ces normes conduit à un ensemble sous spécifié d'exigences pour l'utilisation des certificats dans le contexte de IPsec.

ISAKMP fait référence au profil de certificat PKIX mais, dans de nombreux cas, spécifie simplement le contenu de divers messages sans spécifier leur syntaxe ou sémantique. Pendant ce temps, le profil de certificat PKIX fournit un large ensemble de mécanismes de certificat qui sont généralement applicables pour les protocoles Internet, mais avec peu d'instructions spécifiques pour IPsec. Comme de nombreux choix sont sous spécifiés, l'interopérabilité est mise en danger si toutes les mises en œuvre ne font pas des choix similaires, ou au moins ne peuvent pas prendre en compte les mises en œuvre qui ont fait des choix différents.

Ce profil des cadres de IKE et PKIX est destiné à fournir un standard accepté pour l'utilisation de la technologie de PKI dans le contexte de IPsec en profilant le cadre PKIX pour l'utilisation avec IKE et IPsec, et en documentant le contenu des charges utiles IKE pertinentes et en spécifiant mieux leur signification.

En plus de fournir un profil de IKE et PKIX, le présent document tente d'incorporer les leçons tirées de l'expérience récente avec la mise en œuvre et le déploiement, ainsi que de l'état actuel des protocoles et technologies qui s'y rapportent.

Le matériel provenant de ISAKMP, IKEv1, IKEv2, ou PKIX n'est pas répété ici, et le lecteur du présent document est supposé avoir lu et compris ces documents. Les exigences et les aspects de ces documents sont aussi pleinement pertinents pour le présent document.

Le document est organisé comme suit : la Section 2 définit la terminologie particulière utilisée dans le reste du document, la Section 3 donne le profil de IKEv1/ISAKMP, la Section 4 donne un profil de IKEv2, et la Section 5 le profil de PKIX. La Section 6 couvre les conventions pour l'échange hors bande des matériels de chiffrement pour la configuration.

2. Termes et définitions

Sauf pour les termes qui sont définis immédiatement ci-dessous, tous les termes utilisés dans ce document sont définis dans les documents PKIX [RFC3280], ISAKMP [RFC2408], IKEv1 [RFC2409], IKEv2 [RFC4306], ou de domaine d'interprétation (DOI) [RFC2407].

- Adresse de source d'homologue : adresse de source dans les paquets provenant d'un homologue. Cette adresse peut être différente de toute adresse affirmée comme "identité" de l'homologue.

- FQDN *(Fully qualified domain name)* nom de domaine plainement qualifié.

- ID_USER_FQDN : IKEv2 a rebaptisé ID_USER_FQDN en ID_RFC822_ADDR. tous deux sont appelés ID_USER_FQDN dans le présent document.

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].

3. Utilisation des certificats dans la RFC 2401 et dans IKEv1/ISAKMP

3.1 Charge utile Identification

La charge utile Identification (ID) indique l'identité revendiquée par l'envoyeur. Le receveur peut alors utiliser le ID comme clé de recherche pour la politique et les recherches de certificat dans tout magasin ou répertoire de certificats qui lui est disponible. L'objectif principal de cette section est de profiler la charge utile ID pour qu'elle puisse être utilisée en toute sécurité pour générer ou rechercher la politique. IKE rend obligatoire l'utilisation de la charge utile ID dans la phase 1.

Le DOI [RFC2407] définit les 11 types de données d'identification qui peuvent être utilisés et spécifie la syntaxe de ces types. Ils sont discutés en détails ci-dessous.

Les exigences de charge utile ID dans ce document couvrent seulement la portion des vérifications explicites de politique qui traitent spécifiquement de la charge utile Identification. Par exemple, dans le cas où ID ne contient pas une adresse IP, des vérifications comme celle que l'adresse de source de l'homologue est permise par la politique pertinente ne sont pas traitées ici, car elles sortent du domaine d'application de ce document.

Les mises en œuvre DEVRAIENT remplir l'ID avec les informations d'identité qui sont contenues dans le certificat d'entité d'extrémité. Remplir l'ID avec les informations d'identité provenant du certificat d'entité d'extrémité permet aux receveurs d'utiliser l'ID comme clé de recherche pour trouver le certificat d'entité d'extrémité homologue. Le seul cas où les mises en œuvre peuvent remplir l'ID avec des informations qui ne sont pas contenues dans le certificat d'entité d'extrémité est quand l'ID contient l'adresse de source de l'homologue (une seule adresse, pas un sous réseau ou une gamme).

Parce que les mises en œuvre peuvent utiliser l'ID comme clé de recherche pour déterminer quelle politique utiliser, toutes DOIVENT être particulièrement attentives à vérifier la véracité du contenu en vérifiant qu'il correspond à du métériel de chiffrement dont on peut démontrer qu'il appartient à l'homologue.

Manquer à le faire peut résulter en l'utilisation d'une politique inappropriée ou non sûre. Les paragraphes qui suivent décrivent les méthodes pour effectuer ce lien.

Le tableau qui suit résume le lien de la charge utile Identification avec le contenu des certificats d'entité d'extrémité et des informations d'identité avec la politique. Chaque type d'identification est traité plus en détails dans les paragraphes suivants

Type d'ID	Prise en charge à l'envoi	Attribut PKIX correspondant	Corresp. de certif	Règles de recherche SPD
IP*_ADDR	DOIT [a]	SubjAltName iPAddress	DOIT [b]	[c], [d]
FQDN	DOIT [a]	SubjAltName dNSName	DOIT [b]	[c], [d]
USER_FQDN	DOIT [a]	SubjAltName rfc822Name	DOIT [b]	[c], [d]
Gamme IP	NE DOIT PAS	n/a	n/a	n/a
DN	DOIT [a]	EntireSubject, comparaison au bit près	DOIT [b]	DOIT prendre en charge la recherche sur toute combinaison de C, CN, O, ou OU
GN	NE DOIT PAS	n/a	n/a	n/a
KEY_ID	NE DOIT PAS	n/a	n/a	n/a

[a] = la mise en œuvre DOIT avoir l'opttion de configuration pour envoyer ce type d'ID dans la charge utile ID. Si le type d'ID est utilisé est l'affaire de la configuration locale.

[b] = l'ID dans la charge utile ID DOIT correspondre exactement au contenu du champ correspondant (mentionné) dans le certificat, avec aucune autre recherche. Le ID correspondant PEUT être utilisé pour une recherche dans la base de données de politique de sécurité (SPD, *Security Policy Database*) mais n'est pas obligé d'être utilisé pour cela.

[c] = au minimum, la mise en œuvre DOIT être capable d'être configurée à effectuer une correspondance exacte du contenu de la charge utile ID à une entrée dans la SPD locale.

[d] = en plus, la mise en œuvre PEUT aussi être configurable à effectuer des correspondances de sous chaîne ou de caractère générique du contenu de la charge utile ID avec des entrées de la SPD locale. (Voir au paragraphe 3.1.5.)

Lors de l'envoi d'un IPV4_ADDR, IPV6_ADDR, FQDN, ou USER_FQDN, les mises en œuvre DOIVENT être capables d'être configurées à envoyeur la même chaîne que celle qui apparaît dans l'extension SubjectAltName correspondante. Le présent document RECOMMANDE que les déployeurs utilisent cette option de configuration. Tous ces types d'ID sont traités de la même façon : comme des chaînes qui peuvent être comparées aisément et rapidement à une chaîne correspondante dans une valeur explicite dans le certificat. Parmi ces types, FQDN et USER_FQDN sont RECOMMANDÉS plutôt que les adresses IP (voir la discussion au paragraphe 3.1.1).

Lors de l'envoi d'un nom distinctif (DN, *Distinguished Name*) comme ID, les mises en œuvre DOIVENT envoyer le DN entier dans l'ID. Aussi, les mises en œuvre DOIVENT prendre en charge au moins les attributs C, CN, O, et OU pour la correspondance de SPD. Voir au paragraphe 3.1.5 les détails sur le DN, incluant la correspondance de SPD.

Les receveurs DOIVENT être capables d'effectuer la correspondance de SPD sur le contenu exact de l'ID, et cela

DEVRAIT être le réglage par défaut. De plus, les mises en œuvre PEUVENT utiliser des sous chaînes ou des caractères génériques dans la configuration de la politique locale pour faire la comparaison de la SPD avec le contenu de l'ID. En d'autres termes, les mises en œuvre DOIVENT être capables de faire des confrontations exactes de ID à la SPD, mais PEUVENT ausi être configurables à faire des confrontations de sous chaîne ou caractères génériques de ID à la SPD.

3.1.1 ID_IPV4_ADDR et ID_IPV6_ADDR

Les mises en œuvre DOIVENT prendre en charge au moins le type d'ID ID_IPV4_ADDR ou ID_IPV6_ADDR, selon que la mise en œuvre prend en charge IPv4, IPv6, ou les deux. Ces adresses DOIVENT être codées dans "l'ordre des octets du réseau", comme spécifié dans IP [RFC0791] : le bit de moindre poids (LSB, *least significant bit*) de chaque octet est le LSB de l'octet correspondant dans l'adresse réseau. Pour le type ID_IPV4_ADDR, la charge utile DOIT contenir exactement quatre octets [RFC0791]. Pour le type ID_IPV6_ADDR, la charge utile DOIT contenir exactement seize octets [RFC2460].

Les mises en œuvre NE DEVRAIENT PAS remplir la charge utile ID avec des adresses IP à cause de problèmes d'interopérabilité comme les problèmes de traversée de traducteur d'adresse réseau (NAT, *Network Address Translator*) et de comportement de vérification IP.

Les déploiements peuvent vouloir seulement envisager d'utiliser l'adresse IP comme ID si tout ce qui suit est vrai :
- o l'adresse IP de l'homologue est statique, ne changeant pas dynamiquement ;
- o l'homologue N'EST PAS derrière un NAT ;
- o l'administrateur veut que la mise en œuvre vérifie que l'adresse de source de l'homologue corresponde à l'adresse IP dans l'ID reçu, et à celle dans le champ Adresse IP dans l'extension SubjectAltName du certificat de l'homologue.

Les mises en œuvre DOIVENT être capables de vérifier que l'adresse IP présentée dans l'ID correspond via une comparaison au bit près à l'adresse IP présente dans le champ iPAddress du certificat de l'extension SubjectAltName. Les mises en œuvre DOIVENT effectuer cette vérification par défaut. Lors de la comparaison pour égalité du contenu de l'ID avec le champ iPAddress dans l'extension SubjectAltName, une comparaison binaire DOIT être effectuée. Noter que les certificats peuvent contenir plusieurs types d'identité d'adresse -- dans ce cas, au moins une doit correspondre à la source IP. Si la vérification par défaut est activée, alors une discordance entre les deux adresses DOIT être traitée comme une erreur, et l'établissement de l'association de sécurité DOIT être interrompu. Cet événement DEVRAIT pouvoir faire l'objet d'un examen. Les mises en œuvre PEUVENT fournir une option de configuration (c'est-à-dire que la configuration de politique locale peut activer) pour sauter cette étape de vérification, mais cette option DOIT être désactivée par défaut. On inclut l'option de "sauter la validation" afin de permettre une meilleure interopérabilité car les mises en œuvre courantes varient largement dans la façon de se comporter sur ce sujet.

De plus, les mises en œuvre DOIVENT être capables de vérifier que l'adresse contenue dans l'ID est la même que l'adresse contenue dans l'en-tête IP. Les mises en œuvre DEVRAIENT être capables de vérifier l'adresse dans l'en-tête le plus externe ou le plus interne et PEUVENT fournir une option de configuration pour specifier laquelle va être vérifiée. Si il n'y a pas d'option de configuration fournie, une mise en œuvre DEVRAIT vérifier l'adresse de source de l'homologue contenue dans l'en-tête le plus externe (comme c'est la pratique de la plupart des mises en œuvre actuelles). Si l'ID est d'un des types d'adresse IP, alors les mises en œuvre DOIVENT effectuer cette vérification par défaut. Si ce comportement par défaut est activé, alors une discordance DOIT être traitée comme une erreur, et l'établissement de l'association de sécurité DOIT être interrompu. Cette événement DEVRAIT pouvoir faire l'objet d'un examen. Les mises en œuvre PEUVENT fournir une option de configuration (c'est-à-dire que la configuration de politique locale peut activer) pour sauter cette étape de vérification, mais cette option DOIT être désactivée par défaut. On inclut l'option de "sauter la validation" afin de permettre une meilleure interopérabilité car les mises en œuvre courantes varient largement dans la façon de se comporter sur le sujet de la vérification de la source IP.

Si le comportement par défaut pour les deux vérifications ci-dessus est activé, alors, par la propriété de transitivité, la mise en œuvre va aussi vérifier que l'adresse IP de source de l'homologue correspond via une comparaison au bit près du contenu du champ iPAddress dans l'extension SubjectAltName dans le certificat. De plus, les mises en œuvre PEUVENT permettre aux administrateurs de configurer une politique locale qui exige explicitement que l'adresse IP de source de l'homologue corresponde via une comparaison au bit près du contenu du champ iPAddress dans l'extension SubjectAltName dans le certificat. Les mises en œuvre DEVRAIENT permettre aux administrateurs de configurer une politique locale qui saute cette vérification de validation.

Les mises en œuvre PEUVENT prendre en charge une sous chaîne, caractère générique , ou expression régulière correspondant au contenu de l'ID pour chercher la politique dans la SPD, et ceci serait une affaire de configuration de politique de sécurité locale.

Les mises en œuvre PEUVENT utiliser l'adresse IP trouvée dans l'en-tête des paquets reçus de l'homologue pour chercher la politique, mais de telles mises en œuvre DOIVENT quand même effectuer la vérification de la charge utile d'ID. Bien que les adresses IP de paquet soient par nature indignes de confiance et doivent donc être vérifiées de façon indépendante, il est souvent utile d'utiliser l'adresse IP apparente de l'homologue pour localiser la classe générale de politiques qui vont être utilisées jusqu'à ce que la recherche obligatoire de politique fondée sur l'identité puisse être effectuée.

Par exemple, si l'adresse IP de l'homologue n'est pas reconnue, un appareil de passerelle de VPN pourrait charger une politique générale "de guerrier de la route" qui spécifie une autorité de certification (CA, *Certification Authority*) particulière qui est de confiance pour fournir des certificats contenant un rfc822Name valide, qui peut être utilisé par cette mise en œuvre pour effectuer une autorisation fondée sur des listes de contrôle d'accès (ACL, *Access Control List*) après que le certificat de l'homologue a été validé. Le rfc822Name peut alors être utilisé pour déterminer la politique qui fournit une autorisation spécifique d'accès aux ressources (comme les adresses IP, les accès, et ainsi de suite).

Dans un autre exemple, si l'adresse IP de l'homologue est reconnue pour être un point d"extrémité connu de VPN homologue, la politique peut être déterminée en utilisant cette adresse, mais jusqu'à ce que l'identité (adresse) soit validée par la validation du certificat de l'homologue, la politique NE DOIT PAS être utilisée pour autoriser du trafic IPsec.

3.1.2 ID_FQDN

Les mises en œuvre DOIVENT prendre en charge le type d'ID ID_FQDN, généralement pour prendre en charge des listes de contrôle d'accès fondées sur l'hôte pour les hôtes sans adresse IP fixe. Cependant, les mises en œuvre NE DEVRAIENT PAS utiliser le DNS pour transposer le FQDN en adresse IP pour l'entrée dans des décisions de politique, sauf si cette transposition est connue pour être sûre, par exemple, si DNSSEC [RFC4033] a été employé pour ce FQDN.

Si l'ID contient un ID_FQDN, les mises en œuvre DOIVENT être capables de vérifier que l'identité contenue dans la charge utile ID correspond aux informations d'identité contenues dans le certificat d'entité d'extrémité de l'homologue, dans le champ dNSName dans l'extension SubjectAltName. Les mises en œuvre DOIVENT effectuer cette vérification par défaut. Quand elles comparent pour égalité le contenu de l'ID avec le champ dNSName dans l'extension SubjectAltName, une comparaison de chaîne insensible à la casse DOIT être effectuée.

Noter que la comparaison de chaîne insensible à la casse fonctionne aussi sur les noms de domaine internationalisés (IDN, *Internationalized Domain Name*) (voir IDN [RFC3490]). La comparaison de sous chaîne, de caractères génériques, ou d'expression régulière NE DOIT PAS être effectuée pour cette comparaison. Si le comportement par défaut est activé, alors une discordance DOIT être traitée comme une erreur, et l'établissement d'association de sécurité DOIT être interrompu. Cet événement DEVRAIT pouvoir faire l'objet d'un examen. Les mises en œuvre PEUVENT fournir une option de configuration (c'est-à-dire, la configuration de politique locale peut activer) de sauter l'étape de vérification, mais cette option DOIT être désactivée par défaut. On inclut "l'option de sauter la validation" afin de permettre une meilleure interopérabilité, car les mises en œuvre courantes varient largement dans leur comportement sur ce sujet.

Les mises en œuvre PEUVENT prendre en charge la correspondance de sous chaîne, caractère générique, ou expression régulière du contenu de l'ID pour chercher la politique dans la SPD, et ce serait une affaire de configuration de politique de sécurité locale.

3.1.3 ID_USER_FQDN

Les mises en œuvre DOIVENT prendre en charge le type d'ID ID_USER_FQDN, généralement pour prendre en charge des listes de contrôle d'accès fondées sur l'utilisateur pour les utilisateurs sans adresse IP fixe. Cependant, les mises en œuvre NE DEVRAIENT PAS utiliser le DNS pour transposer la portion FQDN en adresse IP pour toutes décisions de politique, sauf si la transposition est connue pour être sûre, par exemple, si DNSSEC [RFC4033] était employé pour ce FQDN.

Les mises en œuvre DOIVENT être capables de vérifier que l'identité contenue dans la charge utile ID correspond aux informations d'identité contenues dans le certificat d'entité d'extrémité de l'homologue, dans le champ rfc822Name dans l'extension SubjectAltName. Les mises en œuvre DOIVENT effectuer cette vérification par défaut. Lors de la comparaison pour égalité du contenu de l'ID avec le champ rfc822Name dans l'extension SubjectAltName, une comparaison de chaîne insensible à la casse DOIT être effectuée. Noter que la comparaison de chaîne insensible à la casse fonctionne aussi sur les noms de domaine internationalisés (IDN, *Internationalized Domain Name*) (voir IDN [RFC3490]). La comparaison de sous chaîne, de caractères génériques, ou d'expression régulière NE DOIT PAS être effectuée pour cette comparaison. Si ce comportement par défaut est activé, alors une discordance DOIT être traitée comme une erreur, et l'établissement d'association de sécurité DOIT être interrompu. Cet événement DEVRAIT pouvoir faire l'objet d'un examen. Les mises en

œuvre PEUVENT fournir une option de configuration (c'est-à-dire, la configuration de politique locale peut activer) de sauter l'étape de vérification, mais cette option DOIT être désactivée par défaut. On inclut "l'option de sauter la validation" afin de permette une meilleure interopérabilité, car les mises en œuvre courantes varient largement dans leur comportement sur ce sujet.

Les mises en œuvre PEUVENT prendre en charge la correspondance de sous chaîne, caractère générique, ou expression régulière du contenu de l'ID pour chercher la politique dans la SPD, et ce serait une affaire de configuration de politique de sécurité locale.

3.1.4 ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, ID_IPV6_ADDR_RANGE

Noter que la [RFC3779] définit des blocs d'adresses utilisant l'extension de certificat identifiée par :

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

bien que l'utilisation de cette extension dans IKE soit considérée comme expérimentale pour l'instant.

3.1.5 ID_DER_ASN1_DN

Les mises en œuvre DOIVENT prendre en charge la réception du type d'ID ID_DER_ASN1_DN. Les mises en œuvre DOIVENT être capables de générer ce type, et la décision de le faire sera une affaire de configuration de politique de sécurité locale. Quand elles génèrent ce type, les mises en œuvre DOIVENT remplir le contenu de l'ID avec le champ Subject provenant du certificat de l'entité d'extrémité, et DOIVENT le faire de telle façon qu'une comparaison binaire des deux réussisse. Si il n'y a pas de correspondance, cela DOIT être traité comme une erreur, et l'établissement de l'association de sécurité DOIT être interrompu. Cet événement DEVRAIT pouvoir faire l'objet d'un examen.

Les mises en œuvre NE DOIVENT PAS remplir l'ID avec le Subject provenant du certificat d'entité d'extrémité si il est vide, même si un certificat Subject vide est explicitement permis dans la section "Subject" du profil de certificat PKIX.

Concernant la confrontation à la SPD, les mises en œuvre DOIVENT être capables de l'effectuer sur la base d'une comparaison au bit près dans le DN entier avec l'ID dans son entrée de SPD. Cependant, l'expérience du fonctionnement a montré qu'utiliser le DN entier dans la configuration locale est difficile, en particulier dans les déploiements à grande échelle. Donc, les mises en œuvre DOIVENT aussi être capables d'effectuer la confrontation de la SPD de toute combinaison d'un ou plusieurs attributs C, CN, O, OU au sein du DN Subject dans l'ID avec la même dans la SPD. Les mises en œuvre PEUVENT prendre en charge une confrontation en utilisant des attributs de DN supplémentaires dans toute combinaison, bien que l'interopérabilité soit loin d'être certaine et même douteuse. Les mises en œuvre PEUVENT aussi prendre en charge d'effectuer une confrontation de sous chaîne, caractère générique, ou expression régulière pour tous ses attributs de DN pris en charge d'ID, dans toute combinaison, à la SPD. Une telle souplesse permet aux déployeurs de créer une entrée de SPD sur la passerelle pour un département entier d'une entreprise (par exemple, O=Foobar Inc., OU=Ingénierie) tout en leur permettant quand même de tirer d'autres détails du DN (par exemple, CN=John Doe) pour les besoins d'examen. Tout ceci est une affaire de mise en œuvre locale et de définition de politique locale et de capacité d'application, et non des bits sur le réseau, mais aura un grand impact sur l'interopérabilité.

3.1.6 ID_DER_ASN1_GN

Les mises en œuvre NE DOIVENT PAS générer ce type, parce que le receveur ne saura probablement pas comment l'utiliser.

3.1.7 ID_KEY_ID

Le type ID_KEY_ID est utilisé pour spécifier des clés pré partagées et sort donc du domaine d'application de ce document.

3.1.8 Choix d'une identité à partir d'un certificat

Les mises en œuvre DOIVENT prendre en charge les certificats qui contiennent plus d'une seule identité, comme quand le champ Subject et l'extension SubjectAltName sont tous deux remplis, ou que l'extension SubjectAltName contient plusieurs identités sans considération de si le Subject est vide. Dans de nombreux cas, un certificat va contenir une identité, comme une adresse IP, dans l'extension SubjectAltName en plus d'un Subject non vide.

Les mises en œuvre devraient remplir l'ID avec toute identité qui a des chances d'être nommée dans la politique de l'homologue. En pratique, cela signifie généralement un FQDN, ou USER_FQDN, mais cette information peut aussi être disponible à l'administrateur par des moyens hors bande. En l'absence de telles informations de configuration hors bande, l'identité avec laquelle une mise en œuvre choisit de remplir la charge utile ID est une affaire locale.

3.1.9 Subject seulement pour DN

Si un FQDN est destiné à être traité comme une identité pour les besoins de correspondance d'ID, il DOIT être placé dans le champ dNSName de l'extension SubjectAltName. Les mises en œuvre NE DOIVENT PAS remplir le Subject avec un FQDN au lieu de remplir le champ dNSName de l'extension SubjectAltName.

Bien que rien n'empêche un FQDN, USER_FQDN, ou une adresse IP d'apparaître quelque part dans le contenu de Subject, de telles entrées NE DOIVENT PAS être interprétées comme des informations d'identité pour les besoins de confrontation avec l'ID ou pour la recherche de politique.

3.1.10 Lien d'identité à la politique

En présence de certificats qui contiennent plusieurs identités, les mises en œuvre devraient choisir l'identité la plus appropriée dans le certificat et en remplir l'ID. Le receveur DOIT utiliser l'identité envoyée comme première clé quand il choisit la politique. Le receveur DOIT aussi utiliser la politique la plus spécifique dans cette base de données si il y a des politiques qui se chevauchent à cause de caractères génériques (ou parce que la mise en œuvre peut décorréler la base de données de politiques afin qu'il n'y ait pas de chevauchement d'entrées, ou elle peut aussi interdire la création de recouvrements de politiques et laisser le processus de décorrélation à l'administrateur, mais, comme cela déplace le problème à l'administrateur, cela n'est PAS RECOMMANDÉ).

Par exemple, imaginons qu'une mise en œuvre soit configurée avec un certificat qui contient à la fois un Subject non vide et un dNSName. La politique de l'envoyeur peut spécifier lequel utiliser, et elle indique la politique à l'autre extrémité en envoyant cet ID. Si le receveur a une politique spécifique pour le dNSName pour cet hôte et une règle de caractère générique pour certains attributs présents dans le champ Subject, il va correspondre à une politique différente selon l'ID envoyé. Comme l'envoyeur sait pourquoi il voulait se connecter à l'homologue, il sait aussi quelle identité il devraient utiliser pour correspondre à la politique dont il a besoin pour l'opération qu'il essaye d'effectuer ; il est le seul à pouvoir choisir l'ID de façon adéquate.

Dans le cas où la politique ne peut pas être trouvée dans la SPD du receveur en utilisant l'ID envoyé, le receveur PEUT alors utiliser les autres identités du certificat quand il tente de correspondre à une politique convenable. Par exemple, si le certificat contient un champ Subject non vide, un dNSName et une iPAddress. Si une iPAddress est envoyée dans l'ID mais qu'il n'existe pas d'entrée spécifique pour l'adresse dans la base de données de politique, le receveur PEUT chercher dans la SPD sur la base du Subject ou du dNSName contenu dans le certificat.

3.2 Charge utile Demande de certificat

La charge utile Demande de certificat (CERTREQ) permet à une mise en œuvre de demander qu'un homologue fournisse un certain ensemble de certificats ou de listes de révocation de certificat (CRL, C*ertificate Revocation List*). Il n'est pas clair dans ISAKMP comment exactement cet ensemble devrait être spécifié ou comment l'homologue devrait répondre. On décrit la sémantique pour les deux côtés.

3.2.1 Type de certificat

Le champ Type de certificat identifie pour l'homologue le type de matériel de chiffrement de certificat qui est désiré. ISAKMP définit 10 types de données de certificat qui peuvent être demandés et spécifie la syntaxe de ces types. Pour les besoins du présent document, seuls les types suivants sont pertinents :

- Certificat X.509 - Signature
- Listes de révocation (CRL et ARL)
- Certificat X.509 enveloppé dans PKCS n° 7

L'utilisation des autres types sort du comaine d'application de ce document :

- Certificat X.509 - échange de clés

- o Certificat PGP *(Pretty Good Privacy)*
- o Clé signée DNS
- o Jetons Kerberos
- o Certificat SPKI *(Simple Public Key Infrastructure)*
- o Attribut de certificat X.509.

3.2.2 Certificat X.509 - Signature

Ce type demande que le certificat d'entité d'extrémité soit un certificat utilisé pour signer.

3.2.3 Listes de révocation (CRL et ARL)

ISAKMP ne prend pas en charge des tailles de charge utile de certificat de plus d'environ 64K, ce qui est trop petit pour de nombreuses CRL, et la fragmentation UDP va probablement se produire à des tailles bien inférieures. Donc, l'acquisition du matériel de révocation doit être traité hors bande pour IKE. Pour cette raison et d'autres, les mises en œuvre NE DEVRAIENT PAS générer des CERTREQ où le type de certificat est "Liste de révocation de certificat (CRL)" ou "Liste d'autorité de révocation (ARL)". Les mises en œuvre qui génèrent de telles CERTREQ NE DOIVENT PAS exiger que le receveur réponde avec une CRL ou ARL, et NE DOIVENT PAS échouer quand elles n'en reçoivent pas. À réception d'une telle CERTREQ, les mises en œuvre PEUVENT ignorer la demande.

Au lieu d'échanger les listes de révocation dans la bande, un pointeur sur la vérification de révocation DEVRAIT être mentionné dans les extensions de certificat CRLDistributionPoints (CDP) ou AuthorityInfoAccess (AIA) (voir les détails à la Section 5). Sauf si d'autres méthodes pour obtenir les informations de révocation sont disponibles, les mises en œuvre DEVRAIENT être capables de traiter ces attributs, et à partir d'eux, être capables d'identifier le matériel de révocation en antémémoire, ou de restituer le matériel de révocation pertinent à partir d'un URL, pour le traitement de validation. De plus, les mises en œuvre DOIVENT avoir la capacité de configurer les informations de vérification de validation pour chaque autorité de certification. Sans considération de la méthode (CDP, AIA, ou configuration statique) l'acquisition du matériel de révocation DEVRAIT se faire en dehors de IKE. Noter cependant, que l'incapacité d'accéder aux données d'état de révocation par des moyens hors bande fait peser une potentielle vulnérabilité de la sécurité qui pourrait être exploitée par un attaquant.

3.2.4 Certificat X.509 enveloppé dans PKCS n° 7

Ce type d'ID définit un codage particulier (pas un type particulier de certificat) ; certaines mises en œuvre actuelles peuvent ignorer les CERTREQ qu'elles reçoivent qui contiennent ce type d'ID, et les éditeurs ne connaissent aucune mise en œuvre qui génère de tels messages CERTREQ. Donc, l'utilisation de ce type est déconseillée. Les mises en œuvre NE DEVRAIENT PAS exiger de CERTREQ qui contienne ce type de certificat. Les mises en œuvre qui reçoivent des CERTREQ qui contiennent ce type d'ID PEUVENT traiter ces charges utiles comme synonymes de "Certificat X.509 - Signature".

3.2.5 Localisation des charges utiles Demande de certificat

Dans le mode principal IKEv1, la charge utile CERTREQ DOIT être dans les messages 4 et 5.

3.2.6 Présence ou absence des charges utiles Demande de certificat

Quand un échange dans la bande de matériel de chiffrement de certificat est désiré, les mises en œuvre DOIVENT en informer l'homologue en envoyant au moins une CERTREQ. En d'autres termes, une mise en œuvre qui n'envoie aucune CERTREQ durant un échange NE DEVRAIT PAS s'attendre à recevoir de charge utile CERT.

3.2.7 Demandes de certificat

3.2.7.1 Spécification des autorités de certification

Quand elles demandent l'échange du matériel de chiffrement dans la bande, les mises en œuvre DEVRAIENT générer des CERTREQ pour chaque ancre de confiance d'homologue que la politique locale estime explicitement de confiance durant un certain échange. Les mises en œuvre DEVRAIENT remplir le champ Autorité de certification avec le champ Subject de

l'ancre de confiance, de telle façon que la comparaison binaire du Subject et de l'autorité de certification réussisse.

À réception d'une CERTREQ, les mises en œuvre DOIVENT répondre en envoyant au moins le certificat d'entité d'extrémité correspondant à l'autorité de certification mentionnée dans la CERTREQ sauf si la configuration de politique de sécurité locale spécifie que le matériel de chiffrement doit être échangé hors bande. Les mises en œuvre PEUVENT envoyer des certificats autres que le certificat de l'entité d'extrémité (voir la discussion au paragraphe 3.3).

Noter que dans le cas où plusieurs certificats d'entité d'extrémité peuvent être disponibles qui s'enchaînent à des ancres de confiance différentes, les mises en œuvre DEVRAIENT s'en remettre à des heuristiques locales pour déterminer quelle ancre de confiance est d'utilisation la plus appropriée pour générer le CERTREQ. De telles heuristiques sortent du domaine d'application de ce document.

3.2.7.2 Champ Autorité de certification vide

Les mises en œuvre DEVRAIENT générer des CERTREQ où le type de certificat est "Certificat X.509 - Signature" et où le champ Autorité de certification n'est pas vide. Cependant, les mises en œuvre PEUVENT générer des CERTREQ avec un champ Autorité de certification vide dans des conditions particulières. Bien que PKIX interdise les certificats avec un champ Issuer vide, il existe bien un cas d'utilisation où le faire est approprié, et porte une signification spéciale dans le contexte de IKE. C'est devenu une convention dans les essais d'interopérabilité et l'espace d'usage de IKE, et donc son utilisation est spécifiée, et expliquée ici pour les besoins de l'interopérabilité.

Cas d'utilisation : on considère le cas rare où on a une passerelle avec plusieurs politiques pour un grand nombre d'homologues IKE : certains de ces homologues sont des partenaires d'affaires, certains sont des employés distants, certains font du télétravail, certains sont des bureaux locaux, et/ou la passerelle peut servir simultanément de nombreus consommateurs (par exemple, des routeurs virtuels). Le nombre total de certificats, et des ancres de confiance correspondantes, est très élevé -- disons, des centaines. Chacune de ces politiques est configurée avec une ou plusieurs ancres de confiance acceptables, de sorte qu'au total, la passerelle a cent (100) ancres de confiance qui pourraient être utilisées pour authentifier une connexion entrante. Supposons que beaucoup de ces connexions proviennent d'hôtes/passerelles avec des adresses IP allouées dynamiquement, de sorte que la source IP de l'initiateur IKE n'est pas connue de la passerelle, ni l'identité de l'initiateur (jusqu'à ce qu'elle soit révélée dans le message 5 de mode principal). Dans le message 4 de mode principal IKE, la passerelle qui répond va avoir besoin d'envoyer une CERTREQ à l'initiateur. Dans cet exemple, la passerelle n'a aucune idée de à laquelle des cent autorités de certification possibles elle devrait envoyer la CERTREQ. Envoyer à toutes les autorités de certification possibles causerait des délais de traitement significatifs, de la consommation de bande passante, et de la fragmentation UDP, de sorte que cette tactique est exclue.

Dans un tel déploiement, la mise en œuvre de passerelle qui répond devraient être capable de faire tout ce qu'elle peut pour indiquer une autorité de certification dans la CERTREQ. Cela signifie que celui qui répond DEVRAIT d'abord vérifier dans la SPD pour voir si elle peut correspondre à la source IP, et trouver une indication de quelle CA est associée à cet IP. Si cela échoue (parce que la source IP n'est pas familière, comme dans le cas ci-dessus) alors celui qui répond DEVRAIT avoir une option de configuration spécifiant quelles CA sont les CA par défaut à indiquer dans la CERTREQ durant de telles connexions ambigües (par exemple, envoyer la CERTREQ avec ces N CA si il y a une source IP inconnue). Si un tel comportement de repli n'est pas configuré ou est impraticable dans un certain scénario de déploiement, alors celui qui répond DEVRAIT avoir les deux options de configuration suivantes :

- o envoyer une charge utile CERTREQ avec un champ Autorité de certification vide, ou
- o terminer la négociation avec un message d'erreur approprié et une entrée de journal d'événements.

Recevoir une charge utile CERTREQ avec un champ Autorité de certification vide indique que le receveur devrait envoyer tous les certificats d'entité d'extrémité qu'il a, sans considération de l'ancre de confiance. L'initiateur devraient avoir connaissance de la politique et de l'identité qu'il va utiliser, car il a initié la connexion sur une politique, et peut donc répondre avec le certificat approprié.

Si, après l'envoi d'une CERTREQ vide dans un message 4 du mode principal, celui qui répond reçoit un certificat dans le message 5 qui s'enchaîne à une ancre de confiance que celui qui répond soit (a) NE prend PAS en charge, soit (b) n'était pas configuré pour la politique (cette politique à laquelle il peut maintenant être confronté puisque le certificat de l'initiateur est présent) ceci DOIT être traité comme une erreur, et l'établissement de l'association de sécurité DOIT être interrompu. Cet événement DEVRAIT pouvoir faire l'objet d'un examen.

Au lieu d'envoyer une CERTREQ vide, la mise en œuvre qui répond PEUT être configurée à terminer la négociation sur la base d'un conflit avec la politique de sécurité configurée en local.

La décision sur laquelle configurer est une affaire de politique de sécurité locale ; le présent document RECOMMANDE que les deux options soient présentées aux administrateurs.

Plus d'exemples et d'explications de cette question sont inclus dans l'Appendice B "Compléments sur les CERTREQ vides".

3.2.8 Robustesse

3.2.8.1 Types de certificat non reconnus ou non pris en charge

Les mises en œuvre DOIVENT être capables de traiter la réception de CERTREQ avec des types de certificat non pris en charge. En l'absence de types de CERTREQ reconnus et pris en charge, les mises en œuvre PEUVENT les traiter comme si ils étaient d'un type pris en charge avec le champ Autorité de certification laissé vide, selon la politique locale. Le paragraphe 5.10 de ISAKMP [RFC2408] "Traitement de la charge utile Demande de certificat", spécifie les détails du traitement *(voir maintenant le paragraphe 3.7 de la RFC7296)*.

3.2.8.2 Champ Autorité de certification indécodable

Les mises en œuvre DOIVENT être capables de traiter la réception des CERTREQ avec un champ Autorité de certification indécodable. Les mises en œuvre PEUVENT ignorer de telles charges utiles, selon leur politique locale. ISAKMP spécifie d'autres actions qui peuvent être entreprises.

3.2.8.3 Ordre des charges utiles Demande de certificat

Les mises en œuvre NE DOIVENT PAS supposer que les CERTREQ sont dans un ordre quelconque.

3.2.9 Optimizations

3.2.9.1 Charges utiles Demande de certificat dupliquées

Les mises en œuvre NE DEVRAIENT PAS envoyer de CERTREQ dupliquées durant un échange.

3.2.9.2 Nomination des autorités de certification Lowest 'Common' Authorities

Quand le matériel de chiffrement de certificat de l'homologue a été mis en antémémoire, une mise en œuvre peut envoyer un conseil à l'homologue pour élider certains des certificats que l'homologue incluerait normalement dans la réponse. En plus de l'ensemble normal de CERTREQ qui sont envoyées en spécifiant les ancres de confiance, une mise en œuvre PEUT envoyer des CERTREQ qui spécifient les certificats d'entité d'extrémité pertinents en antémémoire. Quand elle envoie ces conseils, il est quand même nécessaire d'envoyer l'ensemble normal de CERTREQ d'ancre de confiance parce que les conseils ne portent pas les informations suffisantes nécessaires à l'homologue. Précisément, soit l'homologue ne peut pas prendre en charge cette optimisation, soit il peut y avoir des chaînes supplémentaires qui pourraient être utilisées dans ce contexte mais ne le seront pas si seul le certificat d'entité d'extrémité est spécifié.

Aucun traitement particulier n'est exigé de la part du receveur d'une telle CERTREQ, et le certificats d'entité d'extrémité va quand même être envoyé. Par ailleurs, le receveur PEUT choisir d'élider les certificats sur la base des conseils reçus.

Les CERTREQ doivent contenir des informations qui identifient un certificat d'autorité de certification, ce qui a pour résultat que l'homologue envoie toujours au moins le certificat d'entité d'extrémité. Envoyer toujours le certificat d'entité d'extrémité permet aux mises en œuvre de déterminer sans ambiguïté quand un nouveau certificat est utilisé par un homologue (peut-être parce que le certificat précédent vient d'expirer) ce qui peut provoquer un échec à cause d'un nouveau certificat de CA intermédiaire qui pourrait n'être pas disponible pour valider le nouveau certificat d'entité d'extrémité). Les mises en œuvre qui utilisent cette optimisation DOIVENT reconnaître quand le certificat d'entité d'extrémité a changé et y répondre en n'effectuant pas cette optimisation si l'échange doit être reessayé afin que tout les matériaux de chiffrement manquants soient envoyés durant le nouvel essai.

3.2.9.3 Exemple

Imaginons qu'une mise en œuvre de IKEv1 ait précédemment reçu et mis en antémémoire la chaîne de certificats de

l'homologue TA->CA1->CA2->EE. Si, durant un échange suivant cette mise en œuvre envoie une CERTREQ contenant le champ Subject dans un certificat TA, cette mise en œuvre demande que l'homologue envoie au moins trois certificats : CA1, CA2, et EE. Par ailleurs, si cette mise en œuvre envoie aussi une CERTREQ contenant le champ Subject de CA2, la mise en œuvre fournit le conseil qu'un seul certificat a besoin d'être envoyé : EE. Noter que dans cet exemple, le fait que TA soit une ancre de confiance ne devrait pas être conçu comme impliquant que TA est un certificat auto-signé.

3.3 Charge utile Certificat

La charge utile Certificat (CERT) permet à l'homologue de transmettre un seul certificat ou CRL. Plusieurs certificats devraient être transmis dans plusieurs charges utiles. Pour la rétro compatibilité, les mises en œuvre PEUVENT envoyer des certificats de CA intermédiaires en plus du ou des certificats d'entité d'extrémité appropriés, mais NE DEVRAIENT PAS envoyer de CRL, ARL, ou ancres de confiance. Échanger des ancres de confiance et en particulier des CRL et des ARL dans IKE augmenterait la probabilité de fragmentation UDP, rendrait l'échane IKE plus complexe, et consommerait plus de bande passante du réseau.

Noter, cependant, que bien que l'envoyeur des charges utiles CERT NE DEVRAIT PAS envoyer de certificats qu'il considère comme des ancres de confiance, il est possible que le receveur puisse considérer tout certificat de CA intermédiaire comme étant celui d'une ancre de confiance. Par exemple, imaginons que l'envoyeur ait la chaîne de certificats TA1->CA1->EE1 tandis que le receveur a la chaîne de certificats TA2->EE2 où TA2 = CA1. L'envoyeur inclut simplement un certificat de CA intermédiaire, alors que le receveur reçoit une ancre de confiance.

Cependant, toutes les formes de certificat légales dans le profil de certificat PKIX ont du sens dans le contexte de IPsec. La question de comment représenter les formes de nom signicatives pour IKE dans un certificat est particulièrement problématique. Le présent document fournit un profil pour un sous ensemble du profil de certificat PKIX qui a un sens pour IKEv1/ISAKMP.

3.3.1 Type de certificat

Le champ Type de certificat identifie à l'homologue le type de matériel de chiffrement de certificat inclus. ISAKMP définit dix types de données de certificat qui peuvent être envoyées et spécifie la syntaxe de ces types. Pour les besoins du présent document, seuls les types suivants sont pertinents :

- Certificat X.509 - Signature
- Liste de révocation (CRL et ARL)
- Certificat X.509 enveloppé dans PKCS n° 7

L'utilisation des autres types sort du domaine d'application de ce document :

- Certificat X.509 - échange de clés
- Certificat PGP
- Clé signée du DNS
- Jetons Kerberos
- Certificat SPKI
- Attribut de certificat X.509.

3.3.2 Certificat X.509 - Signature

Ce type spécifie que les données de certificat contiennent un certificat utilisé pour signer.

3.3.3 Listes de révocation (CRL et ARL)

Ces types spécifient que les données de certificat contiennent une CRL ou ARL X.509. Ces types NE DEVRAIENT PAS être envoyés dans IKE. Voir la discussion au paragraphe 3.2.3.

3.3.4 Certificat X.509 enveloppé dans PKCS n° 7

Ce type définit un codage particulier, pas un type de certificat particulier. Les mises en œuvre NE DEVRAIENT PAS générer des CERT qui contiennent ce type de certificat. Les mises en œuvre DEVRAIENT accepter les CERT qui contiennent ce type de certificat parce que plusieurs mises en œuvre sont connues pour les générer. Noter que ces mises en œuvre incluent parfois des hiérarchies de certificat entières dans une seule charge utile PKCS n° 7 de CERT, ce qui viole

l'exigence spécifiée dans ISAKMP que cette charge utile contienne un seul certificat.

3.3.5 Localisation des charges utiles de certificat

En mode principal IKEv1, la charge utile CERT DOIT être dans les messages 5 et 6.

3.3.6 Charges utiles de certificat non obligatoires

Une mise en œuvre qui ne reçoit aucune CERTREQ durant un échange NE DEVRAIT PAS envoyer de charge utile CERT, sauf quand elle est explicitement configurée à envoyer de façon proactive des charges utiles CERT afin d'interopérer avec les mises en œuvre non conformes qui échouent à envoyer des CERTREQ même quand des certificats sont désirés. Dans ce cas, une mise en œuvre PEUT envoyer la chaîne de certificats (sans inclure d'ancre de confiance) associée au certificat d'entité d'extrémité. Ceci NE DOIT PAS être le comportement par défaut de la mise en œuvre.

Les mises en œuvre dont la configuration de politique de sécurité locale attend qu'un homologue reçoive les certificats par des moyens hors bande DEVRAIT ignorer tout message CERTREQ reçu. Cette condition est connue pour se produire en présence de mises en œuvre non conformes ou bogués.

Les mises en œuvre qui reçoivent d'un homologue des CERTREQ qui contiennent seulement des CA non reconnues PEUVENT choisir de terminer l'échange, afin d'éviter un traitement cryptographique inutile et potentiellement coûteux, dans des attaques de déni de service (privation de ressources).

3.3.7 Réponse à une proposition des plusieurs autorités de certification

En réponse à plusieurs CERTREQ qui contiennent des identités d'autorité de certification différentes, les mises en œuvre PEUVENT utiliser un certificat d'entité d'extrémité qui s'enchaîne à une CA correspondant à une des identités fournies par l'homologue.

3.3.8 Utilisation des matériaux de chiffrement locaux

Les mises en œuvre PEUVENT choisir de sauter l'analyse ou autrement de décoder un certain ensemble de CERT si les mêmes matériels de chiffrement sont disponibles via un moyen préférable, comme dans le cas où des certificats d'un échange précédent ont été mis en antémémoire.

3.3.9 Plusieurs certificats d'entité d'extrémité

Les mises en œuvre NE DEVRAIENT PAS envoyer plusieurs certificats d'entité d'extrémité et les receveurs NE DEVRAIENT PAS être supposés itérer sur plusieurs certificats d'entité d'extrémité.

Si plusieurs certificats d'entité d'extrémité sont envoyés, ils DOIVENT avoir la même clé publique ; autrement, celui qui répond ne va pas savoir quelle clé a été utilisée dans le message 5 de mode principal.

3.3.10 Robustesse

3.3.10.1 Types de certificat non reconnus ou non pris en charge

Les mises en œuvre DOIVENT être capables de traiter la réception de CERT avec des types de certificat non reconnus ou non pris en charge. Les mises en œuvre PEUVENT éliminer de telles charges utiles, selon la politique locale. Le paragraphe 5.10 "Traitement de la charge utile Demande de certificat", spécifie les détails du traitement *(voir maintenant le paragraphe 3.7 de la RFC7296)*.

3.3.10.2 Champs de données de certificat indécodables

Les mises en œuvre DOIVENT être capables de traiter la réception de CERT avec des champs de données de certificat indécodables. Les mises en œuvre PEUVENT éliminer de telles charges utiles, selon la politique locale. ISAKMP spécifie les autres actions qui peuvent être faites.

3.3.10.3 Ordre des charges utiles de certificat

Les mises en œuvre NE DOIVENT PAS supposer que les CERT sont ordonnés d'une façon ou d'une autre.

3.3.10.4 Charges utiles de certificat dupliquées

Les mises en œuvre DOIVENT prendre en charge la réception de plusieurs CERT identiques durant un échange.

3.3.10.5 Certificats non pertinents

Les mises en œuvre DOIVENT être prêtes à recevoir des certificats et des CRL qui ne sont pas pertinents pour l'échange en cours. Les mises en œuvre PEUVENT éliminer de tels certificats et CRL étrangers.

Les mises en œuvre PEUVENT envoyer des certificats qui ne sont pas pertinents pour un échange. Une raison d'inclure des certificats qui ne sont pas pertinents pour un échange est de minimiser la menace de laisser fuir des informations d'identification dans des échanges où le CERT n'est pas chiffré dans IKEv1. On devrait noter cependant que cela ne fournit qu'une protection assez minimale contre la fuite de l'identité.

Une autre raison pour inclure des certificats qui semblent non pertinents pour un échange est qu'il peut y avoir deux chaînes de l'autorité de certification à l'entité d'extrémité, chacune n'étant valide qu'avec certains paramètres de validation (comme de politiques acceptables). Comme l'entité d'extrémité ne sait pas quels paramètres utilise l'autre partie, elle devrait envoyer les certificats nécessaires pour les deux chaînes (même si il n'y a qu'une CERTREQ).

Les mises en œuvre NE DEVRAIENT PAS envoyer plusieurs certificats d'entité d'extrémité et les receveurs NE DEVRAIENT PAS être supposés itérer sur plusieurs certificats d'entité d'extrémité.

3.3.11 Optimisations

3.3.11.1 Charges utiles de certificat dupliquées

Les mises en œuvre NE DEVRAIENT PAS envoyer de CERT dupliqués durant un échange. De telles charges utiles devraient être supprimées.

3.3.11.2 Envoi des plus bas certificats 'communs'

Quand plusieurs CERTREQ sont reçues qui spécifient des autorités de certification au sein de la chaîne de certificats d'entité d'extrémité, les mises en œuvre PEUVENT envoyer la plus courte chaîne possible. Cependant, les mises en œuvre DEVRAIENT toujours envoyer le certificat d'entité d'extrémité. Voir au paragraphe 3.2.9.2 la discussion de cette optimisation.

3.3.11.3 Ignorer les charges utiles de certificat dupliquées

Les mises en œuvre PEUVENT employer des moyens locaux pour reconnaître les CERT qui ont déjà été reçus et DEVRAIENT éliminer ces CERT dupliqués.

3.3.11.4 Cgarge utile Hachage

IKEv1 spécifie l'utilisation facultative de la charge utile Hachage pour porter un pointeur sur un certificat dans l'un des modes de chiffrement de clé publique de phase 1. Ce pointeur est utilisé par une mise en œuvre pour localiser le certificat d'entité d'extrémité qui contient la clé publique qu'un homologue devrait utiliser pour le chiffrement des charges utiles durant l'échange.

Les mises en œuvre DEVRAIENT inclure cette charge utile chaque fois que la portion publique de la paire de clés a été placée dans un certificat.

4. Utilisation de certificats dans la RFC 4301 et IKEv2

4.1 Charge utile Identification

La base de données d'autorisation d'homologue (PAD, *Peer Authorization Database*) décrite dans la [RFC4301] décrit l'utilisation de la charge utile ID dans IKEv2 et fournit un modèle formel pour le lien de l'identité à la politique en plus de fournir des services qui traitent plus spécifiquement lcs détails de l'application de la politique, qui sortent généralement du domaine d'application du présent document. La PAD est destinée à fournir un lien entre la SPD et la gestion d'association de sécurité dans des protocoles comme IKE. Voir plus de détails au paragraphe 4.4.3 de la [RFC4301].

Noter que IKEv2 ajoute une charge utile IDr facultative dans le second échange que l'initiateur peut envoyer à celui qui répond afin de spécifier laquelle des multiples identités de celui qui répond devrait être utilisée. Celui qui répond PEUT choisir d'envoyer un IDr dans le troisième échange qui diffère par son type ou son contenu de l'IDr généré par l'initiateur. L'initiateur DOIT être capable de recevoir un IDr généré par celui qui répond qui est d'un type différent de celui généré par l'initiateur.

4.2 Charge utile Demande de certificat

4.2.1 Listes de révocation (CRL et ARL)

IKEv2 ne prend pas en charge les tailles de charge utile de certificat au dessus de approximativement 64 K. Voir au paragraphe 3.2.3 les problèmes que cela peut causer.

4.2.1.1 Hachage de IKEv2 et URL de certificat X.509

Ce type d'identifiant définit une demande que l'homologue envoie un hachage et l'URL de son certificat X.509, au lieu du certificat réel lui-même. Ceci est un mécanisme particulièrement utile quand l'homologue est un appareil avec peu de mémoire et une faible bande passante, par exemple, un téléphone mobile ou un appareil électronique de consommateur.

Si la mise en œuvre IKEv2 accepte les recherches d'URL, et préfère un tel URL à recevoir les certificats réels, alors la mise en œuvre va vouloir envoyer une notification de type HTTP_CERT_LOOKUP_SUPPORTED *(recherche de certificat HTTP prise en charge)*. D'après le paragraphe 3.10.1 de IKEv2 [RFC4306], "cette notification PEUT être incluse dans tout message qui peut inclure une charge utile CERTREQ et indique que l'envoyeur est capable de chercher les certificats sur la base d'un URL fondé sur HTTP (et donc va probablement préférer recevoir les spécifications de certificat dans ce format)". Si une notification HTTP_CERT_LOOKUP_SUPPORTED est envoyée, l'envoyeur DOIT prendre en charge le schéma http. Voir au paragraphe 4.3.1 la discussion de HTTP_CERT_LOOKUP_SUPPORTED.

4.2.1.2 Localisation des charges utiles Demande de certificat

Dans IKEv2, la charge utile CERTREQ doit être dans les messages 2 et 3. Noter que dans IKEv2, il est possible d'avoir un côté qui s'authentifie avec des certificats tandis que l'autre côté s'authentifie avec des clés pré partagées.

4.3 Charge utile Certificat

4.3.1 Hachage de IKEv2 et URL de certificat X.509

Ce type spécifie que les données de certificat contiennent un hachage et l'URL d'un répertoire où un certificat X.509 peut être restitué.

Une mise en œuvre qui envoie une notification HTTP_CERT_LOOKUP_SUPPORTED DOIT prendre en charge le schéma http et PEUT prendre en charge le schéma ftp, et NE DOIT PAS exiger une forme spécifique du chemin d'url, et elle DEVRAIT prendre en charge d'avoir des parties nom d'utilisateur, mot de passe, et accès dans l'URL. Voici des exemples de formes obligatoires :

- o http://certs.exemple.com/certificate.cer
- o http://certs.exemple.com/certs/cert.pl?u=foo;a=pw;valid-to=+86400
- o http://certs.exemple.com/%0a/../foo/bar/zappa

tandis que voici un exemple d'une forme qui DEVRAIT être prise en charge :

o http://user:password@certs.exemple.com:8888/certificate.cer

FTP PEUT être pris en charge, et si il l'est, voici un exemple du schéma ftp qui DOIT être pris en charge :
o ftp://ftp.exemple.com/pub/certificate.cer

4.3.2 Localisation des charges utiles Certificat

Dans IKEv2, la charge utile CERT DOIT être dans les messages 3 et 4. Noter que dans IKEv2, il est possible d'avoir un côté qui s'authentifie avec des certificats tandis que l'autre côté s'authentifie avec des clés pré partagées.

4.3.3 Ordre des charges utiles Certificat

Pour IKEv2, les mises en œuvre NE DOIVENT PAS supposer que, sauf la première CERT, les autres suivent un ordre quelconque. IKEv2 spécifie que la première CERT contient un certificat d'entité d'extrémité qui peut être utilisé pour authentifier l'homologue.

5. Profil de certificat pour IKEv1/ISAKMP et IKEv2

Sauf lorsque déclaré spécifiquement dans le présent document, les mises en œuvre DOIVENT se conformer aux exigences du profil de certificat PKIX [RFC3280].

5.1 Certificats X.509

Les utilisateurs qui déploient IKE et IPsec avec des certificats ont souvent peu de contrôle sur les capacités des CA qui leur sont disponibles. Les mises en œuvre de la présente spécification peuvent inclure des boutons de configuration pour désactiver les vérifications exigées par la présente spécification afin de permettre son utilisation avec des CA non flexibles et/ou non conformes. Cependant, toutes les vérifications sur les certificats existent pour une raison spécifique qui implique la sécurité de tout le système. Donc, toutes les vérifications DOIVENT être activées par défaut. Les administrateurs et utilisateurs devraient comprendre les objetifs de sécurité des diverses vérifications, et être clairs sur la sécurité qui va être perdue en désactivant la vérification.

5.1.1 Versions

Bien que PKIX déclare que "les mises en œuvre DEVRAIENT être prêtes à accepter toute version de certificat", en pratique, ce profil exige certaines extensions qui nécessitent l'utilisation de certificats de version 3 pour tous les certificats sauf les certificats auto-signés utilisés comme ancres de confiance. Les mises en œuvre qui se conforment au présent document PEUVENT donc rejeter les certificats de version 1 et version 2 dans tous les autres cas.

5.1.2 Subject

Les mises en œuvre d'autorité de certification DOIVENT être capables de créer des certificats avec des champs Subject ayant au moins les quatre attributs suivants : CN, C, O, et OU. Les mises en œuvre PEUVENT aussi prendre en charge d'autres attributs Subject. Le contenu de ces attributs DEVRAIT être configurable certificat par certificat, car ces champs seront probablement utilisés par les mises en œuvre de IKE pour correspondre à la politique de la SPD.

Voir au paragraphe 3.1.5 les détails de la façon dont les mises en œuvre de IKE doivent être capables de traiter le champ d'attributs Subject pour la recherche de politique de la SPD.

5.1.2.1 Nom de Subject vide

Les mises en œuvre de IKE DOIVENT accepter les certificats qui contiennent un champ Subject vide, comme spécifié dans le profil de certificat PKIX. Les informations d'identité dans ces certificats vont être entièrement contenues dans l'extension SubjectAltName.

5.1.2.2 Spécification d'hôtes et non de FQDN dans le nom de sujet

Les mises en œuvre qui désirent placer des noms d'hôte qui ne sont pas destinés à être traités par les receveurs comme des FQDN (par exemple "Routeur passerelle") dans le champ Subject DOIVENT utiliser l'attribut commonName.

5.1.2.3 EmailAddress

Comme spécifié dans le profil de certificat PKIX, les mises en œuvre NE DOIVENT PAS remplir les noms distinctifs X.500 avec l'attribut emailAddress.

5.1.3 Extensions de certificat X.509

Les mises en œuvre conformes de IKE DOIVENT reconnaître les extensions qui doivent ou peuvent être marquées comme critiques en accord avec la présente spécification. Ces extensions sont : KeyUsage, SubjectAltName, et BasicConstraints.

Les mises en œuvre d'autorité de certification DEVRAIENT générer des certificats tels que les bits critiques de l'extension soient établis en accord avec le profil de certificat PKIX et le présent document. Par rapport à la conformité au profil de certificat PKIX, les mises en œuvre de IKE qui traitent des certificats PEUVENT ignorer la valeur du bit de criticité pour les extensions qui sont prises en charge par cette mise en œuvre, mais DOIVENT prendre en charge le bit de criticité pour les extensions qui ne sont pas prises en charge par cette mise en œuvre. C'est-à-dire, la partie utilisatrice DEVRAIT traiter toutes les extensions dont elle sait si le bit est vrai ou faux -- le bit dit ce qui arrive quand la partie utilisatrice ne peut pas traiter une extension.

Met en œuvre	Bit dans le cert.	Obligatoire dans PKIX	Comportement
oui	vrai	vrai	ok
oui	vrai	faux	ok ou rejet
oui	faux	vrai	ok ou rejet
oui	faux	faux	ok
non	vrai	vrai	rejet
non	vrai	faux	rejet
non	faux	vrai	rejet
non	faux	faux	ok

5.1.3.1 AuthorityKeyIdentifier et SubjectKeyIdentifier

Les mises en œuvre NE DEVRAIT PAS assumer de prendre en charge les extensions AuthorityKeyIdentifier ou SubjectKeyIdentifier. Donc, les mises en œuvre d'autorité de certification ne devraient pas générer de hiérarchies de certificat qui soient trop complexes à traiter en l'absence de ces extensions, comme celles qui exigent de vérifier une signature sur un grand nombre de certificats de CA de nom similaire afin de trouver le certificat de CA qui contient la clé utilisée pour générer la signature.

5.1.3.2 KeyUsage

IKE utilise un certificat d'entité d'extrémité dans le processus d'authentification. Le certificat d'entité d'extrémité peut être utilisé pour plusieurs applications. À ce titre, la CA peut imposer des contraintes à la manière dont une clé publique devrait être utilisée. Les extensions KeyUsage (KU) et ExtendedKeyUsage (EKU) s'appliquent dans cette situation.

Comme on parle d'utiliser la clé publique pour valider une signature, si l'extension KeyUsage est présente, alors au moins un des bits de digitalSignature ou nonRepudiation dans l'extension KeyUsage DOIT être établi (les deux peuvent l'être aussi). C'est aussi très bien que d'autres bits de KeyUsage soient établis.

Un résumé du flux logique de la validation de certificat de l'homologue suit :

- Si il n'y a pas d'extension KU, continuer.
- Si KU est présente et ne mentionne pas digitalSignature ou nonRepudiation (les deux, en plus d'autres KU, est bien aussi) rejeter le certificat.
- Si il n'y a aucun des deux ci-dessus, continuer.

5.1.3.3 PrivateKeyUsagePeriod

Le profil de certificat PKIX recommande de ne pas utiliser cette extension. L'extension Utilisation de clé privée est destinée à être utilisée quand des signatures vont devoir être vérifiées longtemps après le moment où les signatures utilisant la paire de clés privées peuvent être générées. Comme les associations de sécurité (SA, *Security Association*) IKE ont une durée de vie courte par rapport à l'utilisation prévue de cette extension en plus du fait que chaque signature est validée une seule fois, l'utilité de cette extension dans le contexte de IKE n'est pas clair. Donc, les mises en œuvre d'autorité de certification NE DOIVENT PAS générer de certificats qui contiennent l'extension PrivateKeyUsagePeriod. Si une mise en œuvre IKE reçoit un certificat avec cette extension, elle DEVRAIT l'ignorer.

5.1.3.4 CertificatePolicies

De nombreuses mises en œuvre de IKE ne prennent pas en charge actuellement l'extension CertificatePolicies. Donc, les mises en œuvre d'autorité de certification qui génèrent des certificats contenant cette extension NE DEVRAIENT PAS marquer l'extension comme critique. Comme c'est le cas avec toutes les extensions de certificat, une partie intéressée qui reçoit cette extension mais qui peut la traiter NE DEVRAIT PAS rejeter le certificat parce qu'il contient l'extension.

5.1.3.5 PolicyMappings

De nombreuses mises en œuvre de IKE ne prennent pas en charge l'extension PolicyMappings *(transpositions de politique)*. Donc, les mises en œuvre qui génèrent des certificats contenant cette extension NE DEVRAIENT PAS marquer l'extension comme critique.

5.1.3.6 SubjectAltName

Les déploiements qui ont l'intention d'utiliser un identifiant de FQDN, USER_FQDN, IPV4_ADDR, ou IPV6_ADDR DOIVENT produire des certificats avec les champs SubjectAltName correspondants remplis des mêmes données. Les mises en œuvre DEVRAIENT générer seulement les choix de GeneralName suivants dans l'extension SubjectAltName, car ces choix se transposent en des types légaux de charge utile d'identification IKEv1/ISAKMP/ IKEv2 : rfc822Name, dNSName, ou iPAddress. Bien qu'il soit possible de spécifier tout choix de GeneralName dans la charge utile Identification en utilisant le type d'identifiant ID_DER_ASN1_GN, les mises en œuvre NE DEVRAIENT PAS prendre en charge une telle fonction, et NE DEVRAIENT PAS générer de certificats qui le fassent.

5.1.3.6.1 dNSName

Si le type d'identifiant IKE est FQDN, alors ce champ DOIT contenir un nom de domaine pleinement qualifiié. Si le type d'identifiant IKE est FQDN, alors le champ dNSName DOIT correspondre à son contenu. Les mises en œuvre NE DOIVENT PAS générer des noms qui contiennent des caractères génériques. Les mises en œuvre PEUVENT traiter les certificats qui contiennent des caractères génériques dans ce champ comme syntaxiquement invalides.

Bien que ce champ soit de la forme d'un FQDN, les mises en œuvre de IKE NE DEVRAIENT PAS supposer que ce champ contient un FQDN qui va se résoudre via le DNS, sauf si cela est connu par un mécanisme hors bande. Un tel mécanisme sort du domaine d'application de ce document. Les mises en œuvre NE DEVRAIENT PAS traiter l'échec de résolution comme une erreur.

5.1.3.6.2 iPAddress

Si le type d'identifiant IKE est IPV4_ADDR ou IPV6_ADDR, alors le champ iPAddress DOIT correspondre à son contenu. Noter que bien que PKIX permette la notation de CIDR [RFC4632] dans l'extension "Contraintes de nom", le profil de certificat PKIX interdit explicitement d'utiliser la notation de CIDR pour porter des informations d'identité. En d'autres termes, la notation de CIDR NE DOIT PAS être utilisée dans l'extension SubjectAltName.

5.1.3.6.3 rfc822Name

Si le type d'identifiant IKE est USER_FQDN, alors le champ rfc822Name DOIT correspondre à son contenu. Bien que ce champ soit sous la forme d'une adresse de messagerie Internet, les mises en œuvre de IKE NE DEVRAIENT PAS supposer que ce champ contient une adresse de messagerie valide, sauf si cela est connu par un mécanisme hors bande. Un tel mécanisme sort du domaine d'application de ce document.

5.1.3.7 IssuerAltName

Les mises en œuvre d'autorité de certification NE DEVRAIENT PAS supposer que les autres mises en œuvre prennent en charge l'extension IssuerAltName, et en particulier ne devraient pas supposer que les informations contenues dans cette extension vont être affichées aux utilisateurs finaux.

5.1.3.8 SubjectDirectoryAttributes

L'extension SubjectDirectoryAttributes est destinée à porter les attributs d'identification du sujet. Les mises en œuvre de IKE PEUVENT ignorer cette extension quand elle est marquée non critique, comme y oblige le profil de certificat PKIX.

5.1.3.9 BasicConstraints

Le profil de certificat PKIX exige que les certificats de CA contiennent cette extension et qu'elle soit marquée comme critique. Les mises en œuvre de IKE DEVRAIENT rejeter les certificats de CA qui ne contiennent pas cette extension. Pour la rétro compatibilité, les mises en œuvre peuvent accepter ces certificats si elles sont explicitement configurées à le faire, mais le comportement par défaut pour ce réglage DOIT être de rejeter ces certificats.

5.1.3.10 NameConstraints

De nombreuses mises en œuvre de IKE ne prennent pas en charge l'extension NameConstraints. Comme le profil de certificat PKIX exige que cette extension soit marquée comme critique quand elle est présente, les mises en œuvre d'autorité de certification qui sont intéressées à une interopérabilité maximale pour IKE NE DEVRAIENT PAS générer de certificats qui contiennent cette extension.

5.1.3.11 PolicyConstraints

De nombreuses mises en œuvre de IKE ne prennent pas en charge l'extension PolicyConstraints. Comme le profil de certificat PKIX exige que cette extension soit marquée comme critique quand elle est présente, les mises en œuvre d'autorité de certification qui sont intéressées à une interopérabilité maximale pour IKE NE DEVRAIENT PAS générer des certificats qui contiennent cette extension.

5.1.3.12 ExtendedKeyUsage

La CA NE DEVRAIT PAS inclure d'extension ExtendedKeyUsage (EKU) dans les certificats à utiliser avec IKE. Noter que il y avait trois identifiants d'objet en relation avec IPsec dans EKU qui ont été alloués en 1999. La sémantique de ces valeurs n'a jamais été clairement définie. L'utilisation de ces trois valeurs de EKU dans IKE/IPsec est obsolète et explicitement déconseillée par la présente spécification. Les CA NE DEVRAIENT PAS produire de certificats à utiliser avec elles dans IKE. (Pour une référence historique seulement, ces trois valeurs étaient id-kp-ipsecEndSystem, id-kp-ipsecTunnel, et id-kp-ipsecUser.)

La CA NE DEVRAIT PAS marquer l'extension EKU dans les certificats à utiliser avec IKE et une ou plusieurs autres applications. Néanmoins, le présent document définit unkeyPurposeID ExtendedKeyUsage qui PEUT être utilisé pour limiter l'utilisation d'un certificat :

IDENTIFIANT D'OBJET id-kp-ipsecIKE ::= { id-kp 17 }

où id-kp est défini dans la [RFC3280]. Si un certificat est destiné à être utilisé avec IKE et d'autres applications, et si une des autres applications exige l'utilisation d'une valeur de EKU, alors ces certificats DOIVENT contenir le id-kp-ipsecIKE keyPurposeID ou anyExtendedKeyUsage [RFC3280], ainsi que les valeurs de keyPurposeID associées aux autres applications. De même, si une CA produit plusieurs certificats par ailleurs similaires pour plusieurs applications incluant IKE, et si il est prévu que le certificat IKE NE SOIT PAS utilisé avec une autre application, le certificat IKE PEUT contenir une extension EKU mentionnant un keyPurposeID de id-kp-ipsecIKE pour déconseiller son usage avec l'autre application. On se rappellera cependant que les extensions EKU dans les certificats destinés à être utilisés dans IKE NE SONT PAS RECOMMANDÉES.

Les mises en œuvre conformes à IKE ne sont pas obligées de prendre en charge EKU. Si une extension EKU critique apparaît dans un certificat et si EKU n'est pas supporté par la mise en œuvre, la RFC 3280 exige alors que le certificat soit rejeté. Les mises en œuvre qui prennent en charge EKU DOIVENT prendre en charge la logique suivante pour la validation de certificat :

- o Si l'extension est non EKU, continuer.
- o Si EKU est présent ET contient id-kp-ipsecIKE ou anyExtendedKeyUsage, continuer.
- o Autrement, rejeter le certificat.

5.1.3.13 CRLDistributionPoints

Parce que le présent document déconseille l'envoi de CRL dans la bande, l'utilisation de CRLDistributionPoints (CDP) devient très importante si des CRL sont utilisées pour une vérification de révocation (par opposition, disons, au protocole d'état de certificat en ligne (OCSP, *Online Certificate Status Protocol)* [RFC2560]). L'homologue IPsec a besoin d'avoir un URL pour une CRL écrit dans sa configuration locale, ou de l'apprendre du CDP. Donc, les mises en œuvre d'autorité de certification DEVRAIENT produire des certificats avec un CDP rempli.

Manquer à valider la paire CRLDistributionPoints/IssuingDistributionPoint peut résulter en une substitution de CRL où une entité substitue en connaissance de cause une bonne CRL provenant d'un point de distribution différent à la CRL qui est supposée être utilisée, ce qui montrerait l'entité comme étant révoquée. Les mises en œuvre de IKE DOIVENT prendre en charge la validation que le contenu des CRLDistributionPoints correspond à celui du IssuingDistributionPoint pour empêcher la substitution de CRL quand la CA productrice les utilise. Au moins une CA est connue pour revenir par défaut à ce type d'utilisation de CRL. Voir plus d'informations au paragraphe 5.2.2.5.

Les CDP DEVRAIENT être "résolvables". Plusieurs mises en œuvre d'autorité de certification non conformes sont bien connues pour inclure des CDP non résolvables comme http://localhost/path_to_CRL et http:///path_to_CRL qui sont équivalents à échouer à inclure l'extension CDP dans le certificat.

Voir à la page d'acceuil de la Toile des IPR de l'IETF les informations sur les droits de propriété intellectuelle pour CRLDistributionPoints. Noter que les deux extensions CRLDistributionPoints et IssuingDistributionPoint sont RECOMMANDÉES mais pas EXIGÉES par le profil de certificat PKIX, donc il n'est pas exigé d'avoir une licence pour des IPR.

5.1.3.14 InhibitAnyPolicy

De nombreuses mises en œuvre de IKE ne prennent pas en charge l'extension InhibitAnyPolicy. Comme le profil de certificat PKIX exige que cette extension soit marquée comme critique quand elle est présente, les mises en œuvre d'autorité de certification qui sont intéressées à une interopérabilité maximale pour IKE NE DEVRAIENT PAS générer de certificats qui contiennent cette extension.

5.1.3.15 FreshestCRL

Les mises en œuvre de IKE NE DOIVENT PAS supposer que l'extension FreshestCRL va exister dans les certificats de l'homologue. Noter que la plupart des mises en œuvre de IKE ne prennent pas en charge les CRL deltas.

5.1.3.16. AuthorityInfoAccess

Le profil de certificat PKIX définit l'extension AuthorityInfoAccess, qui est utilisée pour indiquer "comment accéder aux informations et services de CA pour le producteur du certificat dans lequel apparaît l'extension". Parce que le présent document déconseille l'envoi de CRL dans la bande, l'utilisation de AuthorityInfoAccess (AIA) devient très importante si OCSP [RFC2560] doit être utilisé pour la vérification de révocation (par opposition à des CRL). L'homologue IPsec a besoin d'avoir un URI pour l'interrogation de OCSP écrit dans sa configuration locale, ou il doit l'apprendre de l'AIA. Donc, les mises en œuvre DEVRAIENT prendre en charge cette extension, en particulier si OCSP va être utilisé.

5.1.3.17 SubjectInfoAccess

Le profil de certificat PKIX définit l'extension de certificat SubjectInfoAccess, qui est utilisée pour indiquer "comment accéder aux informations et services sur le sujet du certificat dans lequel l'extension apparaît". Cette extension n'a pas d'utilisation connue dans le contexte de IPsec. Les mises en œuvre conformes de IKE DEVRAIENT ignorer cette extension

quand elle est présente.

5.2 Listes de révocation de certificat X.509

Quand elles valident des certificats, les mises en œuvre de IKE DOIVENT utiliser les informations de révocation de certificat, et DEVRAIENT prendre en charge ces informations de révocation sous la forme de CRL, sauf si des informations de révocation non CRL sont connues pour être la seule méthode pour transmettre ces informations. Les déploiements qui ont l'intention d'utiliser des CRL pour la révocation DEVRAIENT remplir l'extension CRLDistributionPoints. Donc, les mises en œuvre d'autorité de certification DOIVENT prendre en charge la production de certificats avec ce champ rempli. Les mises en œuvre de IKE PEUVENT fournir une option de configuration pour désactiver l'utilisation de certains types d'informations de révocation, mais cette option DOIT être désactivée par défaut. Cette option est souvent utile dans des environnements de laboratoire d'essais.

5.2.1 Sources multiples d'informations de révocation de certificat

Les mises en œuvre de IKE qui prennent en charge plusieurs sources d'obtention des informations de révocation de certificat DOIVENT agir avec prudence quand les informations fournies par ces sources ne sont pas cohérentes : quand un certificat est rapporté comme révoqué par une source de confiance, le certificat DOIT être considéré comme révoqué.

5.2.2 Extensions Liste de révocation de certificat X.509

5.2.2.1 AuthorityKeyIdentifier

Les mises en œuvre d'autorité de certification NE DEVRAIENT PAS supposer que les mises en œuvre de IKE prennent en charge l'extension AuthorityKeyIdentifier, et donc ne devraient pas générer de hiérarchies de certificats trop complexes à traiter en l'absence de cette extension, comme celles qui exigent de vérifier une signature sur un grand nombre de certificats de CA de nom similaire afin de trouver le certificat de CA qui contient la clé utilisée pour générer la signature.

5.2.2.2 IssuerAltName

Les mises en œuvre d'autorité de certification NE DEVRAIENT PAS supposer que les mises en œuvre de IKE prennent en charge l'extension IssuerAltName, et en particulier ne devraient pas supposer que les informations contenues dans cette extension vont être affichées aux utilisateurs finaux.

5.2.2.3 CRLNumber

Comme déclaré dans le profil de certificat PKIX, tous les producteurs DOIVENT inclure cette extension dans toutes les CRL.

5.2.2.4 DeltaCRLIndicator

5.2.2.4.1 Si les CRL deltas ne sont pas acceptées

Les mises en œuvre de IKE qui ne prennent pas en charge les CRL deltas DOIVENT rejeter les CRL qui contiennent le DeltaCRLIndicator (qui DOIT être marqué comme critique en accord avec le profil de certificat PKIX) et DOIVENT utiliser une CRL de base si elle est disponible. Ces mises en œuvre DOIVENT s'assurer qu'une CRL delta "n'écrase pas" une CRL de base, par exemple, dans la base de données de matériel de chiffrement.

5.2.2.4.2 Recommendations de CRL delta

Comme certaines mises en œuvre de IKE qui ne prennent pas en charge les CRL deltas peuvent se comporter de façon incorrecte ou non sûre quand il se présente des CRL deltas, les administrateurs et déployeurs devraient considérer si produire des CRL deltas augmente la sécurité avant de produire de telles CRL. Et, si tous les éléments dans le VPN et les systèmes de PKI ne prennent pas adéquatement en charge les CRL deltas, leur utilisation devrait alors être mise en question.

Les éditeurs sont avertis que plusieurs mises en œuvre se comportent de manière incorrecte ou non sûre en présence de

CRL delta. Voir à l'Appendice A une description de la question. Donc, la présente spécification RECOMMANDE de ne pas produire de CRL delta pour l'instant. Par ailleurs, manquer à produire des CRL deltas peut exposer une plus grande fenêtre de vulnérabilité si une CRL complète n'est pas produite aussi souvent que le seraient des CRL deltas. Voir une discussion supplémentaire dans la section Considérations sur la sécurité du profil de certificat PKIX [RFC3280]. Les mises en œuvre et les administratzurs sont invités à se pencher sur ces questions.

5.2.2.5 IssuingDistributionPoint

Une CA qui utilise des CRLDistributionPoints peut le faire pour fournir de nombreuses "petites" CRL, chacune seulement valide pour un ensemble particulier de certificats produits par cette CA. Pour associer une CRL à un certificat, la CA place l'extension CRLDistributionPoints dans le certificat, et place le IssuingDistributionPoint dans la CRL. Le champ distributionPointName dans l'extension CRLDistributionPoints DOIT être identique au champ distributionPoint dans l'extension IssuingDistributionPoint. Au moins une CA est connue pour avoir par défaut ce type d'utilisation de CRL. Voir plus d'informations au paragraphe 5.1.3.13.

5.2.2.6 FreshestCRL

Étant données les recommandations contre la génération de CRL delta par les mises en œuvre d'autorité de certification, la présente spécification RECOMMANDE que les mises en œuvre ne remplissent pas les CRL avec l'extension FreshestCRL, qui est utilisée pour obtenir des CRL deltas.

5.3 Force des algorithmes de hachage de signature

Au moment de la rédaction du présent document, les autorités de certification et les logiciels de CA produisent les certificats en utilisant les algorithmes de signature RSA avec SHA1 et RSA avec MD5. Les mises en œuvre DOIVENT être capables de valider les certificats avec l'un ou l'autre de ces algorithmes.

Comme décrit dans la [RFC4270], les deux algorithmes de hachage MD5 et SHA-1 sont plus faibles qu'attendu à l'origine par rapport aux collisions de hachage. Les certificats qui utilisent ces algorithmes de hachage au titre de leurs algorithmes de signature pourraient être soumis à une attaque dans laquelle une CA produit un certificat avec une certaine identité, et le receveur de ce certificat peut créer un certificat valide différent avec une identité différente. Jusqu'à présent, cette attaque est seulement théorique, même avec les faiblesses trouvées dans les algorithmes de hachage.

À cause des attaques récentes, il y a eu un regain d'intérêt pour un large déploiement d'algorithmes de signature supplémentaires. L'algorithme qui a été mentionné le plus souvent est RSA avec SHA256, dont deux types sont décrits en détails dans la [RFC4055]. Il est largement attendu que cet algorithme de signature soit beaucoup plus résilient aux attaques fondées sur la collision que les RSA avec SHA1 et RSA avec MD5 actuels, bien que cela n'ait pas été prouvé. Il y a une discussion active dans la communité du chiffrement sur les meilleures fonctions de hachage qui pourraient être utilisées dans les algorithmes de signature.

Afin d'interopérer, toutes les mises en œuvre doivent être capables de valider les signatures pour tous les algorithmes que les mises en œuvre vont rencontrer. Donc, les mises en œuvre DEVRAIENT être capables d'utiliser des signatures qui utilisent l'algorithme de signature sha256WithRSAEncryption (PKCS n° 1 version 1.5) aussitôt que possible. Au moment de la rédaction du présent document, il y a au moins une CA qui prend en charge la génération de certificats avec l'algorithme de signature sha256WithRSAEncryption, et il est prévu qu'il y aura des déploiements significatifs de cet algorithme dès la fin de 2007.

6. Conventions d'échange des données de configuration

On présente ci-dessous un format commun d'échange des données de configuration. Les mises en œuvre DOIVENT prendre en charge ces formats, DOIVENT prendre en charge la réception d'espaces blanches arbitraires au début et à la fin de toute ligne, DOIVENT prendre en charge la réception de longueurs de ligne arbitraires bien qu'elles DEVRAIENT générer des lignes de moins de 76 caractères, et DOIVENT prendre en charge la réception des trois terminaisons de ligne suivantes : LF (US-ASCII 10), CR (US-ASCII 13), et CRLF.

6.1 Certificats

Les certificats DOIVENT être codés en Base64 [RFC4648] et apparaître entre les délimiteurs suivants :

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

6.2 CRL et ARL

Les CRL et les ARL DOIVENT être codées en Base64 et apparaître entre les délimiteurs suivants :

```
-----BEGIN CRL-----
-----END CRL-----
```

6.3 Clés publiques

Les mises en œuvre de IKE DOIVENT prendre en charge deux formes de clés publiques : les certificats et ce qu'on appelle des clés "brutes". Les certificats devraient être transférés sous la même forme qu'au paragraphe 6.1. Une clé brute est seulement la portion SubjectPublicKeyInfo du certificat, et DOIT être codée en Base64 et apparaître entre les délimiteurs suivants :

```
-----BEGIN PUBLIC KEY-----
-----END PUBLIC KEY-----
```

6.4 Demandes de signature de certificat PKCS n° 10

Une demande de signature de certificat PKCS n° 10 [RFC2986] DOIT être codée en Base64 et apparaître entre les délimiteurs suivants :

```
-----BEGIN CERTIFICATE REQUEST-----
-----END CERTIFICATE REQUEST-----
```

7. Considérations sur la sécurité

7.1 Charge utile Demande de certificat

Les contenus de CERTREQ ne sont pas chiffrés dans IKE. Dans certains environnements, cela peut laisser fuiter des informations privées. Les administrateurs peuvent souhaiter, dans certains environnements, utiliser l'option Autorité de certification vide pour empêcher la fuite de ces informations, au prix des performances.

7.2 Mode principal IKEv1

Des certificats peuvent être inclus dans tout message, et donc les mises en œuvre peuvent souhaiter répondre avec des CERT dans un message qui offre la protection de la confidentialité dans les messages 5 et 6 de mode principal.

Les mises en œuvre peuvent souhaiter ne pas répondre avec des CERT dans le second message, violant ainsi la caractéristique de protection de l'identité du mode principal de IKEv1.

7.3 Désactivation des vérifications de certificat

Il est important de noter que partout où le présent document suggère aux mises en œuvre de fournir aux utilisateurs l'option de configuration de simplifier, modifier, ou désactiver une caractéristique ou étape de vérification, il peut y avoir des conséquences pour la sécurité à faire ainsi. L'expérience des déploiements a montré qu'une telle souplesse peut être nécessaire dans certains environnements, mais faire usage d'une telle souplesse peut être inapproprié dans d'autres environnements. Ces options de configuration DOIVENT par défaut être "activées" et il est approprié de fournir aux utilisateurs des avertissements quand ils désactivent de telles caractéristiques.

8. Remerciements

Les auteurs tiennent à remercier les auteurs du document arrivé à expiration "Profil PKIX pour IKE" (juillet 2000) qui a fourni des matériaux précieux pour le présent document.

Les auteurs remercient particulièrement Eric Rescorla, un des auteurs originaux, en plus de Greg Carter, Steve Hanna, Russ Housley, Charlie Kaufman, Tero Kivinen, Pekka Savola, Paul Hoffman, et Gregory Lebovitz pour leurs précieux commentaires, dont certains ont été incorporés tels quels dans le présent document. Paul Knight a effectué la tâche ardue de convertir le texte au format XML.

9. Références

9.1 Références normatives

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

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

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Protocole Internet d'association de sécurité et gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

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

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

[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)

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC7296)

9.2 Références pour information

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", décembre 1998. *(MàJ par* 5095, 6564 *; D.S ; Remplacée par* RFC8200, STD 86*)*

[RFC2560] M. Myers, R. Ankney, A. Malpani, S. Galperin et C. Adams, "Protocole d'état de certificat en ligne d'infrastructure de clé publique X.509 pour l'Internet - OCSP", juin 1999. *(P.S.) (Remplacée par* RFC6960)

[RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (*Remplacée par les* RFC5890 et 5891, *P.S.*)

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

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005.

[RFC4055] J. Schaad et autres, "Algorithmes et identifiants supplémentaires pour la cryptographie RSA à utiliser dans le profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour

l'Internet", juin 2005.

[RFC4270] P. Hoffman, B. Schneier, "Attaques contre les hachages cryptographiques dans les protocoles Internet", nov. 2005. *(Info.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4632] V. Fuller et T. Li, "Acheminement inter domaine sans classe (CIDR) : Plan d'allocation et d'agrégation des adresses Internet", août 2006. (BCP 122)

[RFC4648] S. Josefsson, "Codages de données Base16, Base32 et Base64", octobre 2006. (*Remplace* RFC3548) *(P.S.)*

Appendice A. Dangers possibles des CRL deltas

Le problème est que l'algorithme de traitement de CRL est parfois écrit incorrectement avec l'hypothèse que toutes les CRL sont des CRL de base et il est supposé que les CRL vont réussir les essais de validité de contenu. Précisément, de telles mises en œuvre échouent à vérifier le certificat contre toutes les CRL possibles : si la première CRL obtenue de la base de données de matériel de chiffrement échoue au décodage, aucun autre essai de révocation ne sera effectué pour le certificat pertinent. Ce problème est compliqué par le fait que les mises en œuvre qui ne comprennent pas les CRL deltas peuvent échouer à décoder de telles CRLs du fait de l'extension critique DeltaCRLIndicator. L'algorithme qui est mis en œuvre dans ce cas est approximativement :

- o aller chercher la CRL la plus récente
- o vérifier la validité de la signature de CRL
- o si la signature de CRL est valide, alors
- o si la CRL ne contient pas d'extension critique non reconnue et si le certificat est sur la CRL, alors régler le statut du certificat à révoqué.

Les auteurs notent qu'un certain nombre d'outils PKI ne fournissent même pas de méthode pour obtenir autre chose que la plus récente CRL, qui en présence de CRL deltas peut en fait être une CRL delta, pas une CRL de base.

Noter que l'algorithme ci-dessus est dangereux de nombreuses façons. Voir dans le profil de certificat PKIX [RFC3280] l'algorithme correct .

Appendice B. Compléments sur les CERTREQ vides

L'envoi de demandes de certificat vides est couramment utilisé dans les mises en œuvre, et dans les réunions d'inter opérabilité IPsec, les fabricants ont généralement accepté l'idée que cela signifie d'envoyer tous les certificats d'entité d'extrémité qu'on a (si plusieurs certificats d'entité d'extrémité sont envoyés, ils doivent avoir la même clé publique, car autrement, l'autre extrémité ne sait pas quelle clé a été utilisée). Dans 99 % des cas, le client a exactement un certificat et clé publique, donc il ne s'en soucie pas vraiment, mais le serveur pourrait en avoir plusieurs ; donc, il a simplement besoin de dire au client d'utiliser tout certificat qu'il a. Si on parle de VPN d'entreprise, etc., même si le client a plusieurs certificats ou clés, tous vont être utilisables quand il s'authentifie auprès du serveur, de sorte que le client peut simplement en prendre un.

Si il y a une différence réelle sur le certificat à utiliser (comme ceux qui donnent des permissions différentes) alors le client doit être configuré de toutes façons, ou il pourrait même demander à l'utilisateur lequel utiliser (l'utilisateur est le seul qui sache si il a besoin des privilèges d'administrateur, et donc a besoin d'utiliser le certificat d'administrateur, ou si les privilèges normaux de messagerie électronique suffisent, et donc d'utiliser seulement le certificat de messagerie).

Dans 99 % des cas, le client a exactement un certificat, donc il va l'envoyer. Dans 90 % du reste des cas, tout certificat convient, car ce sont simplement différents certificats provenant de la même CA, ou de CA différentes pour le même VPN d'entreprise, donc tous conviennent.

L'envoi de demandes de certificat vides est compris comme signifiant "donnez moi votre certificat, quel qu'il soit".

Justification:

- Celui qui répond fait tout ce qu'il peut pour envoyer une CERTREQ avec une CA, vérifier qu'il y a une correspondance IP dans la SPD, avoir un ensemble de CA par défaut à utiliser dans les cas ambigus, etc.
- Envoyer des CERTREQ vides est très courant dans les mises en œuvre actuelles, et est généralement accepté comme signifiant "envoyez moi un certificat, tout certificat qui fonctionne pour vous".
- Épargne à celui qui répond d'envoyer potentiellement des centaines de certificats, les problèmes de fragmentation qui s'ensuivent, etc.
- Dans plus de 90 % des cas d'utilisation, les initiateurs ont exactement un certificat.
- Dans plus de 90 % des cas d'utilisation restants, les multiples certificats qu'il a sont produits par la même CA.
- Dans les cas restants -- si les précédents ne les couvrent pas tous -- l'initiateur va être configuré explicitement avec le certificat à envoyer, donc répondre à une CERTREQ vide est facile.

L'exemple suivant montre pourquoi les initiateurs ont besoin d'avoir une définition de politique suffisante pour savoir quel certificat utiliser pour la connexion qu'ils initient.

Exemple : votre client (initiateur) est configuré avec des politiques de VPN pour les passerelles A et B (représentant peut-être des entreprises partenaires).

Les politiques pour les deux passerelles ressemblent à quelque chose comme :

Politique de la compagnie Acme (passerelle A)
L'ingénierie peut accéder par 10.1.1.0
CA de confiance : CA-A, Utilisateurs de confiance : OU=Ingénierie
Les partenaires peuvent accéder par 20.1.1.0
CA de confiance : CA-B, Utilisateurs de confiance : OU=AcmePartenaires

Politique de la compagnie Bizco (passerelle B)
Les ventes peuvent accéder par 30.1.1.0
CA de confiance : CA-C, Utilisateurs de confiance : OU=ventes
Les partenaires peuvent accéder par 40.1.1.0
CA de confiance : CA-B, Utilisateurs de confiance : OU=BizcoPartenaires

Si vous êtes employé de Acme et qu'on vous produit les certificats suivants :
- De CA-A : CN=JoeUser,OU=Ingénierie
- De CA-B : CN=JoePartner,OU=BizcoPartenaires

Le client DOIT être configuré en local pour savoir quelle CA utiliser quand il se connecte à l'une ou l'autre passerelle. Si votre client n'est pas configuré à savoir les accréditifs locaux à utiliser pour la passerelle distante, ce scénario ne va pas fonctionner non plus. Si vous tentez de vous connecter à Bizco, tout va fonctionner... tant que vous sont présentées des réponses avec un certificat signé par CA-B ou CA-C... car avoir seulement un certificat de CA-B vous convient. Si vous tentez de vous connecter à Acme, vous allez avoir un problème parce que un choix de politique ambigu est présenté. Comme initiateur, vous présentez des demandes de certificat de CA-A et CA-B. Vous avez des certificats produits par les deux CA, mais seulement un des certificats va être utilisable. Comment le client sait il quel certificat il devrait présenter ? Il doit avoir une politique locale suffisamment claire pour spécifier quel accréditif présenter pour la connexion qu'il initie.

Adresse de l'auteur

Brian Korver
Network Resonance, Inc.
2483 E. Bayshore Rd.
Palo Alto, CA 94303
USA

téléphone : +1 650 812 7705
mél : briank@networkresonance.com

Déclaration complète de droits de reproduction

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