

Groupe de travail Réseau  
**Request for Comments : 2528**  
 Catégorie : Information  
 Traduction Claude Brière de L'Isle

R. Housley, SPYRUS  
 W. Polk, NIST  
 mars 1999

## **Infrastructure Internet de clés publiques X.509 : Représentation des clés de l'algorithme d'échange de clés dans les certificats d'infrastructure Internet de clé publique X.509**

### **Statut de ce mémoire**

Le présent mémoire apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune forme de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

### **Notice de copyright**

Copyright (C) The Internet Society (1999). Tous droits réservés.

### **Table des matières**

1. Résumé fonctionnel.....	1
2. Exigences et hypothèses.....	1
2.1 Communication et topologie.....	2
2.2 Critères d'acceptabilité.....	2
2.3 Attentes de l'utilisateur.....	2
2.4 Attentes des administrateurs.....	2
3. Prise en charge de l'algorithme de KEA.....	2
3.1 Informations de clé publique sujette.....	2
3.2 Extension d'usage de clé dans les certificats de KEA.....	3
4. Modules ASN.1.....	3
4.1 Syntaxe de 1988.....	3
4.2 Syntaxe de 1993.....	4
5. Références.....	4
6. Considérations pour la sécurité.....	4
7. Adresse des auteurs.....	5
8. Déclaration complète de droits de reproduction.....	5

### **Résumé**

L'algorithme d'échange de clés (KEA, *Key Exchange Algorithm*) est un algorithme classifié pour échanger des clés. La présente spécification fait le profil du format et de la sémantique des champs dans les certificats X.509 V3 qui contiennent des clés KEA. La spécification traite du champ `subjectPublicKeyInfo` et de l'extension `keyUsage`.

## **1. Résumé fonctionnel**

La présente spécification contient des lignes directrices sur l'utilisation des certificats d'infrastructure Internet de clé publique pour transporter les clés de l'algorithme d'échange de clés (KEA). Cette spécification est un addendum à la RFC2459, "Profil de certificat d'infrastructure de clé publique X.509 et de CRL pour l'Internet". Les mises en œuvre de la présente spécification doivent aussi se conformer à la RFC2459. Les mises en œuvre de la présente spécification ne sont pas obligées de se conformer aux autres parties de cette série.

## **2. Exigences et hypothèses**

L'objectif est d'augmenter le profil de certificat X.509 présenté dans la Partie 1 pour faciliter la gestion des clés KEA pour les groupes qui utilisent cet algorithme.

## 2.1 Communication et topologie

Ce profil, tel que présenté dans la [RFC2459] et augmenté par la présente spécification, prend en charge des utilisateurs sans grosse bande passante, connexité IP en temps réel, ou forte disponibilité de connexion. De plus, le profil permet la présence de pare-feu ou autres filtrages de communication.

Le présent profil ne suppose pas le déploiement d'un système d'annuaire X.500. Le profil n'interdit pas l'utilisation d'un annuaire X.500, mais d'autres moyens de distribution des certificats et des listes de révocation de certificats (CRL, *certificate revocation list*) sont pris en charge.

## 2.2 Critères d'acceptabilité

L'objectif de l'infrastructure de clé publique de l'Internet (PKI, *Public Key Infrastructure*) est de satisfaire les besoins en fonctions de contrôle d'accès déterministes, d'identification automatisée, d'authentification, et d'autorisation. La prise en charge de ces services détermine les attributs contenus dans le certificat aussi bien que les informations de contrôle auxiliaires dans le certificat telles que les données de politique et les contraintes du chemin de certification.

Le but du présent document est de dessiner un profil des certificats de KEA, de spécifier le contenu et la sémantique des attributs qui n'étaient pas pleinement spécifiés par la [RFC2459]. Si ils ne sont pas spécifiquement visés par le présent document, le contenu et la sémantique des champs et extensions doivent être comme décrit dans la [RFC2459].

## 2.3 Attentes de l'utilisateur

Les utilisateurs de PKI Internet sont des personnes et des processus qui utilisent un logiciel client et sont les sujets désignés dans les certificats. Ces utilisateurs incluent des lecteurs et des rédacteurs de messagerie électronique, les clients des navigateurs de la Toile mondiale, les serveurs WWW, et le gestionnaire de clés pour IPSEC au sein d'un routeur. Ce profil reconnaît les limitations des plateformes que ces usagers emploient et la sophistication/attention des utilisateurs eux-mêmes.

Cela se manifeste par la responsabilité minimale de la configuration d'utilisateur (par exemple, les clés racines, les règles) les contraintes explicites d'utilisation de plateforme au sein du certificat, les contraintes du chemin de certification qui masquent à l'utilisateur de nombreuses actions malveillantes, et les applications qui automatisent intelligemment les fonctions de validation.

## 2.4 Attentes des administrateurs

Comme avec les utilisateurs, le profil de PKI Internet est structuré pour prendre en charge les individus qui font généralement fonctionner les autorités de certification (CA, *Certification Authorities*). Fournir aux administrateurs un choix sans limite augmente les chances qu'une faute subtile d'un administrateur de CA résulte en une grosse compromission ou en limitation inutile de l'interopérabilité. Ce profil définit les identifiants d'objets et les formats de données qui doivent être pris en charge pour interpréter les clés publiques de KEA.

# 3. Prise en charge de l'algorithme de KEA

Cette section décrit les identifiants d'objets et les formats de données qui peuvent être utilisés avec la [RFC2459] pour décrire les certificats X.509 qui contiennent une clé publique de KEA. Les CA conformes sont obligées d'utiliser les identifiants d'objets et les formats de données lorsque elles produisent des certificats de KEA. Les applications conformes devront reconnaître les identifiants d'objets et traiter les formats de données lors du traitement de tels certificats.

## 3.1 Informations de clé publique sujette

Le certificat identifie l'algorithme de KEA, porte les paramètres facultatifs, et spécifie la clé publique de KEA dans le champ `subjectPublicKeyInfo`. Le champ `subjectPublicKeyInfo` est une SEQUENCE d'un identifiant d'algorithme et du champ `subjectPublicKey`.

Le certificat indique l'algorithme au moyen d'un identifiant d'algorithme. Cet identifiant d'algorithme consiste en un identifiant d'objet (OID, *object identifier*) et des paramètres facultatifs associés. Le paragraphe 3.1.1 identifie l'OID et les paramètres préférés pour l'algorithme de KEA. Les CA conformes devront utiliser l'OID identifié lorsque ils produisent des certificats qui contiennent des clés publiques pour l'algorithme de KEA. Les applications conformes qui prennent en charge l'algorithme de KEA devront au minimum reconnaître l'OID identifié au paragraphe 3.1.1.

Le certificat porte la clé publique de KEA à travers le champ `subjectPublicKey`. Ce champ `subjectPublicKey` est une CHAINE BINAIRE. Le paragraphe 3.1.2 spécifie la méthode de codage d'une clé publique de KEA comme une CHAINE BINAIRE. Les CA conformes devront coder la clé publique de KEA comme décrit au paragraphe 3.1.2 lorsque elles produisent des certificats contenant des clés publiques pour l'algorithme de KEA. Les applications conformes qui prennent en charge l'algorithme de KEA devront décoder le champ `subjectPublicKey` comme décrit au paragraphe 3.1.2 lorsque l'identifiant d'algorithme est celui présenté en 3.1.1.

### 3.1.1 Identifiant et paramètres d'algorithme

L'algorithme d'échange de clés (KEA, *Key Exchange Algorithm*) est un algorithme pour échanger des clés. Une "paire de clés couplées" de KEA peut être générée entre deux utilisateurs si leurs clés publiques de KEA ont été générées avec les mêmes paramètres de KEA. Les paramètres de KEA ne sont pas inclus dans un certificat ; un "identifiant de domaine" est plutôt fourni dans le champ Paramètres.

Lorsque le champ `subjectPublicKeyInfo` contient une clé de KEA, l'identifiant et les paramètres d'algorithme devront être comme défini dans [sdn.701r]:

```
IDENTIFIANT D'OBJET id-keyExchangeAlgorithm ::= { 2 16 840 1 101 2 1 1 22 }
KEA-Parms-Id ::= CHAINE D'OCTETS
```

Les CA devront remplir le champ Paramètres de `AlgorithmIdentifier` au sein du champ `subjectPublicKeyInfo` de chaque certificat contenant une clé publique de KEA avec un identifiant de paramètre de 80 bits (CHAINE D'OCTETS) aussi appelé l'identifiant de domaine. L'identifiant de domaine sera calculé en trois étapes : (1) les paramètres de KEA sont codés en DER en utilisant la structure `Dss-Parms` ; (2) un hachage SHA-1 de 160 bits est généré à partir des paramètres ; et (3) le hachage de 160 bits est réduit à 80 bits en effectuant un "OU exclusif" des 80 bits de poids fort avec les 80 bits de moindre poids. La valeur résultante est codée de telle sorte que l'octet de poids fort de la valeur de 80 bits soit le premier octet dans la chaîne d'octets.

Le `Dss-Parms` est donné dans la [RFC2459] et est reproduit ici par souci de complétude.

```
Dss-Parms ::= SEQUENCE {
    p          ENTIER,
    q          ENTIER,
    g          ENTIER }
```

### 3.1.2 Codage des clés publiques de KEA

Une clé publique de KEA,  $y$ , est portée dans la CHAINE BINAIRE `subjectPublicKey` de telle façon que le bit de poids fort (MSB, *most significant bit*) de  $y$  devienne le MSB du champ de valeur de la CHAINE BINAIRE et que le bit de moindre poids (LSB, *least significant bit*) de  $y$  devienne le LSB du champ de valeur de la CHAINE BINAIRE. Il en résulte le codage suivant : étiquette de CHAINE BINAIRE, longueur de CHAINE BINAIRE, 0 (indiquant qu'il y a zéro bit non utilisé dans l'octet final de  $y$ ), champ valeur de CHAINE BINAIRE incluant  $y$ .

## 3.2 Extension d'usage de clé dans les certificats de KEA

L'extension d'usage de clé peut facultativement apparaître dans un certificat de KEA. Si un certificat de KEA comporte l'extension `keyUsage`, seules les valeurs suivantes peuvent être affirmées :

```
keyAgreement ;
encipherOnly ;
decipherOnly.
```

Les valeurs `encipherOnly` et `decipherOnly` ne peuvent être affirmées que si la valeur `keyAgreement` est aussi affirmée. Au plus un des deux `encipherOnly` et `decipherOnly` devront être affirmés dans l'extension `keyUsage`. Généralement, la valeur `keyAgreement` est affirmée sans que les valeurs ni de `encipherOnly` ni de `decipherOnly` soient affirmées.

## 4. Modules ASN.1

### 4.1 Syntaxe de 1988

```
PKIXkea88 {iso(1) identified-organization(3) dod(6)
  internet(1) security(5) mechanisms(5) pkix(7)
  id-mod(0) id-mod-kea-profile-88(7) }
```

DEBUT ::=

-- EXPORTE TOUT --

-- IMPORTE RIENE --

IDENTIFIANT D'OBJET id-keyExchangeAlgorithm ::= { 2 16 840 1 101 2 1 1 22 }

KEA-Parms-Id ::= CHAINE D'OCTETS

FIN

### 4.2 Syntaxe de 1993

```
PKIXkea93 {iso(1) identified-organization(3) dod(6)
  internet(1) security(5) mechanisms(5) pkix(7)
  id-mod(0) id-mod-kea-profile-93(8) }
```

DEBUT ::=

-- EXPORTE TOUT --

IMPORTE ALGORITHM-ID

FROM PKIX1Explicit93 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7)  
id-mod(0) id-pkix1-explicit-93(3) }

ALGORITHM-ID KeaPublicKey ::= { OID id-keyExchangeAlgorithm PARMS KEA-Parms-Id }

IDENTIFIANT D'OBJET id-keyExchangeAlgorithm ::= { 2 16 840 1 101 2 1 1 22 }

KEA-Parms-Id ::= CHAINE D'OCTETS

FiN

## 5. Références

[KEA] "Skipjack and KEA Algorithm Specification, Version 2.0", 29 mai 1998, disponible à <http://csrc.nist.gov/encryption/skipjack-kea.htm>

[SDN.701R] SDN.701, "Message Security Protocol", Revision 4.0 1996-06-07 avec "Corrections to Message Security Protocol, SDN.701, Rev 4.0, 96-06-07." 30 août 1996.

[RFC2459] R. Housley, W. Ford, W. Polk et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de CRL pour l'Internet", janvier 1999. (*Obsolète, voir la RFC5280*) (P.S.)

## 6. Considérations pour la sécurité

La présente spécification est dédiée au format et au codage des clés de KEA dans les certificats X.509. Comme les certificats sont à signature numérique, aucun service supplémentaire de vérification d'intégrité n'est nécessaire. Il n'est pas besoin que les certificats soient tenus secrets, et l'accès anonyme et sans restriction aux certificats et aux CRL n'a pas d'implication sur la sécurité.

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

Les procédures suivies par les CA et les autorités d'enregistrement pour valider le lien avec l'identité du sujet de leur clé publique affecte au plus haut point la sûreté qui peut être prêtée au certificat. Les parties qui s'appuient sur lui peuvent souhaiter revoir la déclaration des pratiques en matière de certificat de la CA.

La protection accordée aux clés privées est un facteur critique du maintien de la sécurité. Si la protection accordée par l'utilisateur à ses clés privées de KEA est défaillante cela permettra à un attaquant de se faire passer pour elles, ou de décrypter leurs informations personnelles.

La disponibilité et la fraîcheur des informations de révocation vont affecter le degré de sûreté qui devrait être prêtée à un certificat.

Bien que les certificats arrivent naturellement à expiration, des événements peuvent survenir durant leur durée de vie naturelle qui rompent le lien entre le sujet et la clé publique. Si les informations de révocation ne sont pas mises à jour à temps ou ne sont pas disponibles, la sûreté associée au lien est évidemment réduite. De même, les mises en œuvre des mécanismes de validation de chemin décrits à la section 6 qui omettent les vérifications de révocation fournissent moins d'assurance que celles qui les prennent en charge.

L'algorithme de validation de chemin spécifié dans la [RFC2459] dépend d'une certaine connaissance des clés publiques (et d'autres informations) sur une ou plusieurs CA de confiance. La décision de faire confiance à une CA est une décision importante car elle détermine en fin de compte la confiance que mérite un certificat. La distribution authentifiée de clés publiques de CA de confiance (en général sous la forme d'un certificat "auto signé") est un processus de sécurité hors bande critique qui sort du domaine d'application de la présente spécification.

De plus, lorsque survient la compromission d'une clé ou la défaillance d'une CA pour une CA de confiance, l'utilisateur va devoir modifier les informations fournies au sous-programme de validation de chemin. La sélection de trop de CA de confiance va rendre difficile la maintenance des informations sur les CA de confiance. D'un autre côté, le choix d'une seule CA de confiance peut limiter les usagers à une communauté fermée d'utilisateurs jusqu'à ce qu'émerge un PKI mondial.

La qualité des mises en œuvre qui traitent les certificats peut aussi affecter le degré de sûreté fourni. L'algorithme de validation de chemin décrit à la section 6 s'appuie sur l'intégrité des informations de la CA de confiance, et en particulier sur l'intégrité des clés publiques associées aux CA de confiance. En substituant les clés publiques pour lesquelles il a la clé privée, un attaquant pourrait conduire l'utilisateur à accepter de faux certificats.

Le lien entre une clé et un sujet de certificat ne peut pas être plus fort que la mise en œuvre et les algorithmes du module cryptographique utilisés pour générer la signature.

## 7. Adresse des auteurs

Russell Housley  
SPYRUS  
381 Elden Street  
Suite 1120  
Herndon, VA 20170 USA  
mél : [housley@spyrus.com](mailto:housley@spyrus.com)

Tim Polk  
NIST  
Building 820, Room 426  
Gaithersburg, MD 20899  
USA  
mél : [wpolk@nist.gov](mailto:wpolk@nist.gov)

## 8. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (1999). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de copyright ci-dessus et ce paragraphe soit inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les droits de reproduction définies dans les processus des

normes pour l'Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet, ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation à un objet particulier.

**Remerciement**

Le financement de la fonction d'éditeur des RFC est actuellement assuré par la Internet Society.