Groupe de travail Réseau
Request for Comments : 4523
RFC rendues obsolètes : 2252, 2256, 2587
Catégorie : Standards Track

K. Zeilenga, OpenLDAP Foundation

juin 2006
Traduction Claude Brière de L’Isle
mai 2007

Protocole léger d’accès à un répertoire (LDAP) : Définitions de schémas pour les certificats X.509

Statut du présent mémo

Le présent document spécifie un protocole de normalisation Internet pour la communauté de l'Internet, qui appelle à la discussion et à des suggestions pour son amélioration. Prière de se reporter à l'édition en cours des "Normes de protocole officielles de l'Internet" (STD 1) sur l'état de la normalisation et le statut de ce protocole. La distribution du présent mémo n'est soumise à aucune restriction.

Résumé

Le présent document décrit le schéma de représentation des certificats X.509, des informations de sécurité X.521, et des éléments qui s’y rapportent dans les répertoires accessibles en utilisant le protocole léger d’accès à un répertoire (LDAP). Les définitions LDAP de ces éléments de schéma X.509 et X.521 remplacent ceux fournis dans les RFC 2252 et 2256.

1 Introduction

Le présent document fournit les définitions de schéma LDAP [RFC4510] [RFC4512] pour un sous ensemble d’éléments spécifiés dans X.509 et X.521, incluant les types d’attribut pour les certificats, les paires de certificats croisés, et les listes de révocation de certificats ; les règles de correspondance à utiliser avec ces types d’attributs, et les classes d’objet qui s’y rapportent. Les définitions de syntaxe LDAP sont aussi fournies pour les valeurs d’assertion et d’attribut associées.
Comme la sémantique de ces éléments est semblable à celle définie dans X.509 et X.521, la connaissance de X.509 et de X.521 est nécessaire pour utiliser les définitions de schéma LDAP fournies ici.
Le présent document, conjointement avec la [RFC4510], rend obsolète les RFC 2252 et 2256 dans leur totalité. Les changements (dans le présent document) faits depuis la RFC 2252 et la RFC 2256 incluent :
- l’ajout des classes pkiUser, pkiCA, et deltaCRL ;
- la mise à jour des types d’attribut pour inclure les règles de concordance d’égalité conformément à leurs spécifications X.500 ;
- l’ajout des règles de correspondance de certificat, de paire de certificats, de liste de certificats, et d’identifiant d’algorithme ;
- l’ajout de la syntaxe LDAP pour les syntaxes d’assertion de ces règles de correspondance.Le présent document rend obsolète la RFC 2587. Les descriptions de schéma X.509 pour LDAPv2 [RFC1777] sont dépassées, comme l’est LDAPv2 [RFC3494].

Les mots clé "DOIT", "NE DOIT PAS", "EXIGE", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans le BCP 14 [RFC2119].

Les définitions de schéma sont fournies en utilisant les formats de description de LDAP [RFC4512]. Les définitions fournies ici sont formatées (coupure de ligne) pour faciliter la lecture.

2 Syntaxes

La présente section décrit diverses syntaxes utilisées dans LDAP pour transférer les certificats et les types de données qui s'y rapportent.

2.1 Certificate

(1.3.6.1.4.1.1466.115.121.1.8 DESC 'X.509 Certificate')

Une valeur de cette syntaxe est un certificat X.509 [X.509, Section 7].

Du fait des changements apportés à la définition d'un certificat à travers le temps, aucun codage spécifique de LDAP n'est défini pour cette syntaxe. Les valeurs de cette syntaxe DEVRAIENT être codées en utilisant les règles de codage distinctif (DER) [X.690] et ne DOIVENT être transférées qu'en utilisant l'option de transfert binaire [RFC4522] ; c'est-à-dire, en demandant et en retournant des valeurs qui utilisent des descriptions d'attribut telles que "userCertificate;binary".

Comme les valeurs de cette syntaxe contiennent des données signées numériquement, les valeurs de cette syntaxe et la forme de chaque valeur DOIVENT être préservées dans leur présentation d'origine.

2.2 CertificateList

(1.3.6.1.4.1.1466.115.121.1.9 DESC 'X.509 Certificate List')

Une valeur de cette syntaxe est une CertificateList X.509 [X.509, paragraphe 7.3].Du fait des changements apportés dans le temps à la définition d'une CertificateList, aucun codage spécifique de LDAP n'est défini pour cette syntaxe. Les valeurs de cette syntaxe DEVRAIENT être codées en utilisant DER [X.690] et NE DOIVENT être transférées qu'en utilisant l'option de transfert binaire [RFC4522] ; c'est-à-dire, en demandant et en retournant les valeurs en utilisant des descriptions d'attribut telles que "certificateRevocationList;binary".Comme les valeurs de cette syntaxe contiennent des données à signature numérique, les valeurs de cette syntaxe et la forme de chaque valeur DOIVENT être préservées telles qu'elles ont été présentées.

2.3 CertificatePair

(1.3.6.1.4.1.1466.115.121.1.10 DESC 'X.509 Certificate Pair')

Une valeur de cette syntaxe est une CertificatePair X.509 [X.509, paragraphe 11.2.3].Du fait des changements apportés à travers le temps à la définition d'une CertificatePair X.509, aucun codage spécifique de LDAP n'est défini pour cette syntaxe. Les valeurs de cette syntaxe DEVRAIENT être codées en utilisant DER [X.690] et NE DOIVENT être transférées qu'en utilisant l'option de transfert binaire [RFC4522]; c'est-à-dire, en demandant et retournant les valeurs en utilisant des descriptions d'attribut telles que "crossCertificatePair;binary".Comme les valeurs de cette syntaxe contiennent des données à signature numérique, les valeurs de cette syntaxe et la forme de chaque valeur DOIVENT être préservées telles qu'elles ont été présentées.

2.4 SupportedAlgorithm

(1.3.6.1.4.1.1466.115.121.1.49 DESC 'X.509 Supported Algorithm')

Une valeur de cette syntaxe est un SupportedAlgorithm X.509 [X.509, paragraphe 11.2.7].

Du fait des changements apportés à travers le temps à la définition d'un SupportedAlgorithm X.509, aucun codage spécifique de LDAP n'est défini pour cette syntaxe. Les valeurs de cette syntaxe DEVRAIENT être codées en utilisant DER [X.690] et NE DOIVENT être transférées qu'en utilisant l'option de transfert binaire [RFC4522]; c'est-à-dire, en demandant et retournant les valeurs en utilisant des descriptions d'attribut telles que "supportedAlgorithms;binary".Comme les valeurs de cette syntaxe contiennent des données à signature numérique, les valeurs de cette syntaxe et la forme de la valeur DOIVENT être préservées telles qu'elles ont été présentées.

2.5 CertificateExactAssertion

(1.3.6.1.1.15.1 DESC 'X.509 Certificate Exact Assertion')

Une valeur de cette syntaxe est une CertificateExactAssertion X.509 [X.509, paragraphe 11.3.1]. Les valeurs de cette syntaxe DOIVENT être codées en utilisant les règles de codage de chaîne générique (GSER, Generic String Encoding Rules) [RFC3641]. L'appendice A.1 fournit un équivalent de la grammaire du formalisme Backus-Naur augmenté (ABNF) [RFC4234] pour cette syntaxe.

2.6 CertificateAssertion

(1.3.6.1.1.15.2 DESC 'X.509 Certificate Assertion')

Une valeur de cette syntaxe est une CertificateAssertion X.509 [X.509, paragraphe 11.3.2]. Les valeurs de cette syntaxe DOIVENT être codées en utilisant GSER [RFC3641]. L'appendice A.2 fournit une grammaire équivalente à l'ABNF [RFC4234] pour cette syntaxe.

2.7 CertificatePairExactAssertion

(1.3.6.1.1.15.3 DESC 'X.509 Certificate Pair Exact Assertion')
Une valeur de cette syntaxe est une CertificatePairExactAssertion X.509 [X.509, paragraphe 11.3.3]. Les valeurs de cette syntaxe DOIVENT être codées en utilisant GSER [RFC3641]. L'appendice A.3 fournit une grammaire équivalente à l'ABNF [RFC4234] pour cette syntaxe.

2.8 CertificatePairAssertion

(1.3.6.1.1.15.4 DESC 'X.509 Certificate Pair Assertion')
Une valeur de cette syntaxe est une CertificatePairAssertion X.509 [X.509, paragraphe 11.3.4]. Les valeurs de cette syntaxe DOIVENT être codées en utilisant GSER [RFC3641]. L'appendice A.4 fournit une grammaire équivalente à l'ABNF [RFC4234] pour cette syntaxe.

2.9 CertificateListExactAssertion

(1.3.6.1.1.15.5 DESC 'X.509 Certificate List Exact Assertion')
Une valeur de cette syntaxe est une CertificateListExactAssertion X.509 [X.509, paragraphe 11.3.5]. Les valeurs de cette syntaxe DOIVENT être codées en utilisant GSER [RFC3641]. L'appendice A.5 fournit une grammaire équivalente à l'ABNF pour cette syntaxe.

2.10 CertificateListAssertion

(1.3.6.1.1.15.6 DESC 'X.509 Certificate List Assertion')Une valeur de cette syntaxe est une CertificateListAssertion X.509 [X.509, paragraphe 11.3.6]. Les valeurs de cette syntaxe DOIVENT être codées en utilisant GSER [RFC3641]. L'appendice A.6 fournit une grammaire équivalente à l'ABNF [RFC4234] pour cette syntaxe.

2.11 AlgorithmIdentifier

(1.3.6.1.1.15.7 DESC 'X.509 Algorithm Identifier')Une valeur de cette syntaxe est un AlgorithmIdentifier X.509 [X.509, Section 7]. Les valeurs de cette syntaxe DOIVENT être codées en utilisant la [RFC3641].L'appendice A.7 fournit une grammaire équivalente à l'ABNF [RFC4234] pour cette syntaxe.

3 Règles de correspondance

La présente section introduit un ensemble de certificats et de règles de correspondances qui s'y rapportent à utiliser dans LDAP. Ces règles sont destinées à agir conformément à leurs contreparties dans X.500.

3.1 certificateExactMatch

La règle de correspondance certificateExactMatch compare la valeur d'assertion exacte du certificat présenté avec la valeur d'un attribut de la syntaxe de certificat comme décrit au paragraphe 11.3.1 de [X.509].(2.5.13.34 NAME 'certificateExactMatch' DESC 'X.509 Certificate Exact Match' SYNTAX 1.3.6.1.1.15.1)

3.2 certificateMatch

La règle de correspondance certificateMatch compare la valeur d'assertion du certificat présenté avec la valeur d'un attribut de la syntaxe de certificat comme décrit au paragraphe 11.3.2 of [X.509].(2.5.13.35 NAME 'certificateMatch' DESC 'X.509 Certificate Match' SYNTAX 1.3.6.1.1.15.2)

3.3 certificatePairExactMatch

La règle de correspondance certificatePairExactMatch compare la valeur d'assertion exacte de la paire de certificats présentée avec la valeur d'un attribut de la syntaxe de paire de certificats comme décrit au paragraphe 11.3.3 de [X.509].(2.5.13.36 NAME 'certificatePairExactMatch' DESC 'X.509 Certificate Pair Exact Match' SYNTAX 1.3.6.1.1.15.3)

3.4 certificatePairMatch

La règle de correspondance certificatePairMatch compare la valeur d'assertion de la paire de certificats présentée avec la valeur d'un attribut de la syntaxe de paire de certificats comme décrit au paragraphe 11.3.4 of [X.509].(2.5.13.37 NAME 'certificatePairMatch' DESC 'X.509 Certificate Pair Match' SYNTAX 1.3.6.1.1.15.4)

3.5 certificateListExactMatch

La règle de correspondance certificateListExactMatch compare la valeur d'assertion exacte de la liste de certificats présentée avec la valeur d'un attribut de la syntaxe de paire de certificats comme décrit au paragraphe 11.3.5 de [X.509].(2.5.13.38 NAME 'certificateListExactMatch' DESC 'X.509 Certificate List Exact Match' SYNTAX 1.3.6.1.1.15.5)

3.6 certificateListMatch

La règle de correspondance certificateListMatch compare la valeur d'assertion de la liste de certificats présentée avec la valeur d'un attribut de la syntaxe de paire de certificats comme décrit au paragraphe 11.3.6 de [X.509].(2.5.13.39 NAME 'certificateListMatch' DESC 'X.509 Certificate List Match' SYNTAX 1.3.6.1.1.15.6)

3.7 algorithmIdentifierMatch

La règle de correspondance algorithmIdentifierMatch compare un identifiant d'algorithme présenté avec la valeur d'un attribut de l'algorithme pris en charge comme décrit au paragraphe 11.3.7 de [X.509].

(2.5.13.40 NAME 'algorithmIdentifier' DESC 'X.509 Algorithm Identifier Match' SYNTAX 1.3.6.1.1.15.7)

4 Types d'attribut

La présente section détaille un ensemble de certificats et de types d'attributs qui s'y rapportent à utiliser dans LDAP.

4.1 userCertificate

L'attribut userCertificate détient les certificats X.509 produits à l'utilisateur par une ou plusieurs autorités de certificat, comme exposé au paragraphe 11.2.1 de [X.509].

```
( 2.5.4.36 NAME 'userCertificate'
    DESC 'X.509 user certificate'
    EQUALITY certificateExactMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )
```

Comme exigé par la syntaxe de ce type d'attribut, les valeurs de cet attribut sont demandées et transférées en utilisant la description d'attribut "userCertificate;binary".

4.2 cACertificate

L'attribut cACertificate détient les certificats X.509 produits à l'autorité de certificat (CA), comme exposé au paragraphe 11.2.2 de [X.509].

```
( 2.5.4.37 NAME 'cACertificate'
    DESC 'X.509 CA certificate'
    EQUALITY certificateExactMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )
```

Comme exigé par la syntaxe de ce type d'attribut, les valeurs de cet attribut sont demandées et transférées en utilisant la description d'attribut "cACertificate;binary".

4.3 crossCertificatePair

L'attribut crossCertificatePair détient une paire de certificats X.509, comme exposé au paragraphe 11.2.3 de [X.509].

```
( 2.5.4.40 NAME 'crossCertificatePair'
    DESC 'X.509 cross certificate pair'
    EQUALITY certificatePairExactMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.10 )
```

Comme exigé par la syntaxe de ce type d'attribut, les valeurs de cet attribut sont demandées et transférées en utilisant la description d'attribut "crossCertificatePair;binary".

4.4 certificateRevocationList

L'attribut certificateRevocationList détient les listes de certificats, comme exposé au paragraphe 11.2.4 de [X.509].

(2.5.4.39 NAME 'certificateRevocationList'
DESC 'X.509 certificate revocation list'
EQUALITY certificateListExactMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.9)

Comme exigé par la syntaxe de ce type d'attribut, les valeurs de cet attribut sont demandées et transférées en utilisant la description d'attribut "certificateRevocationList;binary".

4.5 authorityRevocationList

L'attribut authorityRevocationList détient les listes de certificats, comme exposé au paragraphe 11.2.5 de [X.509].

(2.5.4.38 NAME 'authorityRevocationList'
DESC 'X.509 authority revocation list'
EQUALITY certificateListExactMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.9)

Comme exigé par la syntaxe de ce type d'attribut, les valeurs de cet attribut sont demandées et transférées en utilisant la description d'attribut "authorityRevocationList;binary".

4.6 deltaRevocationList

L'attribut deltaRevocationList détient les listes de certificats, comme exposé au paragraphe 11.2.6 de [X.509].

(2.5.4.53 NAME 'deltaRevocationList'
DESC 'X.509 delta revocation list'
EQUALITY certificateListExactMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.9)

Comme exigé par la syntaxe de ce type d'attribut, les valeurs de cet attribut DOIVENT être demandées et transférées en utilisant la description d'attribut "deltaRevocationList;binary".

4.7 supportedAlgorithms

L'attribut supportedAlgorithms détient les algorithmes pris en charge, comme exposé au paragraphe 11.2.7 de [X.509].

(2.5.4.52 NAME 'supportedAlgorithms' DESC 'X.509 supported algorithms' EQUALITY algorithmIdentifierMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.49)

Comme exigé par la syntaxe de ce type d'attribut, les valeurs de cet attribut DOIVENT être demandées et transférées en utilisant la description d'attribut "supportedAlgorithms;binary".

5. Classes d'objet

La présente section détaille un ensemble de classes d'objets se rapportant aux certificats à utiliser dans LDAP.

5.1 pkiUser

Cette classe d'objets est utilisée à augmenter les entrées pour les objets qui peuvent être soumis à des certificats, comme défini au paragraphe 11.1.1 de [X.509].
(2.5.6.21 NAME 'pkiUser' DESC 'X.509 PKI User' SUP top AUXILIARY MAY userCertificate)

5.2 pkiCA

Cette classe d'objets est utilisée pour augmenter les entrées pour les objets qui agissent comme autorités de certificat, comme défini au paragraphe 11.1.2 de [X.509]
(2.5.6.22 NAME 'pkiCA' DESC 'X.509 PKI Certificate Authority' SUP top AUXILIARY MAY (cACertificate $ certificateRevocationList $ authorityRevocationList $ crossCertificatePair))

5.3 cRLDistributionPoint

Cette classe est utilisée pour représenter des objets qui agissent comme points de distribution CRL, comme exposé au paragraphe 11.1.3 de [X.509].
(2.5.6.19 NAME 'cRLDistributionPoint' DESC 'X.509 CRL distribution point' SUP top STRUCTURAL MUST cn MAY (certificateRevocationList $ authorityRevocationList $ deltaRevocationList))

5.4 deltaCRL

La classe d'objet deltaCRL est utilisée pour augmenter les entrées qui détiennent des listes de révocation hold delta revocation lists, comme exposé au paragraphe 11.1.4 of [X.509].

(2.5.6.23 NAME 'deltaCRL' DESC 'X.509 delta CRL' SUP top AUXILIARY MAY deltaRevocationList)

5.5 strongAuthenticationUser

Cette classe d'objets est utilisée pour augmenter les entrées pour les objets qui participent à l'authentification fondée sur le certificat, comme défini au paragraphe 6.15 de [X.521]. Cette classe d'objet est déconseillée au profit de pkiUser.
(2.5.6.15 NAME 'strongAuthenticationUser' DESC 'X.521 strong authentication user' SUP top AUXILIARY MUST userCertificate)

5.6 userSecurityInformation

Cette classe d'objets est utilisée pour augmenter les entrées qui ont besoin d'informations de sécurité associée supplémentaire, comme défini au paragraphe 6.16 de [X.521].
(2.5.6.18 NAME 'userSecurityInformation' DESC 'X.521 user security information' SUP top AUXILIARY MAY (supportedAlgorithms))

5.7 certificationAuthority

Cette classe d'objets est utilisée pour augmenter les entrées pour les objets qui agissent comme autorité de certificat, comme défini au paragraphe 6.17 de [X.521]. Cette classe d'objet est déconseillée au profit de pkiCA.
(2.5.6.16 NAME 'certificationAuthority'
DESC 'X.509 certificate authority'
SUP top AUXILIARY
MUST (authorityRevocationList $ certificateRevocationList $ cACertificate)
MAY crossCertificatePair)

5.8 certificationAuthority-V2

Cette classe d'objets est utilisée pour augmenter les entrées pour les objets qui agissent comme autorités de certificat, comme défini au paragraphe 6.18 of [X.521]. Cette classe d'objet est déconseillée au profit de pkiCA.
(2.5.6.16.2 NAME 'certificationAuthority-V2' DESC 'X.509 certificate authority, version 2' SUP certificationAuthority AUXILIARY MAY deltaRevocationList)

6 Considérations sur la sécurité

Les considérations générales sur les certificats [RFC3280] s'appliquent aux applications de certificat relatives à LDAP. Les considérations générales sur la sécurité pour LDAP [RFC4510] s'appliquent également.
Bien que les éléments des informations de certificat soient habituellement signés, ces signatures ne protègent que l'intégrité des informations signées. En l'absence de protections d'intégrité des données dans LDAP (ou de couche inférieure, par exemple, IPsec), un serveur n'est pas assuré qu'une demande de certificat cliente (ou une autre demande) n'a pas été altérée dans le transit. De même, un client ne peut être assuré que le résultat de l'interrogation n'a pas été altéré dans le transit. Et donc, il est généralement recommandé que les mises en œuvre utilisent les services d'authentification et d'intégrité des données de LDAP [RFC4513][RFC4511].

7 Considérations relatives à l'IANA

7.1 Enregistrement d'identifiant d'objet

L'IANA a enregistré un identifiant d'objet LDAP [RFC4520] à utiliser dans la présente spécification technique.
Sujet : Demande d'enregistrement d'un OID LDAP
Personne et adresse de messagerie à contacter pour des informations complémentaires : Kurt Zeilenga
kurt@OpenLDAP.org
Spécification : RFC 4523
Auteur/Contrôleur des modifications : IESG
Commentaires : Identifie les éléments de schéma de certificat X.509 de LDAP introduits dans ce document.

7.2 Enregistrement de descripteur

L'IANA a mis à jour le registre de descripteur LDAP [RFC44520] comme indiqué ci-dessous.
Sujet : Demande d'enregistrement de descripteur LDAP
Descripteur (nom abrégé) : voir le tableau
Identifiant d'objet : voir le tableau
Personne et adresse de messagerie à contacter pour des informations complémentaires : Kurt Zeilenga
kurt@OpenLDAP.org
Usage : voir le tableau
Spécification : RFC 4523
Auteur/Contrôleur des modifications : IESG

algorithmIdentifierMatch	M	2.5.13.40
authorityRevocationList	A	2.5.4.38 *
cACertificate	A	2.5.4.37 *
cRLDistributionPoint	O	2.5.6.19 *
certificateExactMatch	M	2.5.13.34
certificateListExactMatch	M	2.5.13.38
certificateListMatch	M	2.5.13.39
certificateMatch	M	2.5.13.35
certificatePairExactMatch	M	2.5.13.36
certificatePairMatch	M	2.5.13.37
certificateRevocationList	A	2.5.4.39 *
certificationAuthority	O	2.5.6.16 *
certificationAuthority-V2	O	2.5.6.16.2 *
crossCertificatePair	A	2.5.4.40 *
deltaCRL	O	2.5.6.23 *
deltaRevocationList	A	2.5.4.53 *
pkiCA	O	2.5.6.22 *
pkiUser	O	2.5.6.21 *
strongAuthenticationUser	O	2.5.6.15 *
supportedAlgorithms	A	2.5.4.52 *
userCertificate	A	2.5.4.36 *
userSecurityInformation	O	2.5.6.18 *

* Met à jour l'enregistrement précédent

8 Remerciements

Le présent document est fondé sur X.509, produit par l'UIT-T. Un certain nombre de définitions de schéma LDAP sont fondées sur celles qui se trouvent dans les RFC 2252 et 2256, toutes deux produites par le groupe de travail ASID de l'IETF. Les productions d'ABNF de l'appendice A ont été fournies par Steven Legg. Des éléments supplémentaires ont été empruntés à des travaux antérieurs de David Chadwick et Steven Legg pour affiner le schéma X.509 de LDAP.

9 Références

9.1 Références normatives

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

[RFC3641] Legg, S., "Règles génériques de codage de chaîne (GSER) pour les types ASN.1", octobre 2003.

[RFC4510] Zeilenga, K., Ed., "Protocole léger d'accès à un répertoire (LDAP) : Descriptif des spécifications techniques", juin 2006.

[RFC4512] Zeilenga, K., "Protocole léger d'accès à un répertoire (LDAP) : Modèles d'information de répertoire", juin 2006.

[RFC4522] Legg, S., "Protocole léger d'accès à un répertoire (LDAP) : L'option de codage binaire", juin 2006.

[X.509] Union Internationale des Télécommunications – Secteur de la normalisation des télécommunications, "Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire : cadre général des certificats de clé publique et d'attribut", (mars 2000).

[X.521] Union Internationale des Télécommunications – Secteur de la normalisation des télécommunications, "Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire : classes d'objets sélectionnées", (février 2001).

[X.690] Union Internationale des Télécommunications – Secteur de la normalisation des télécommunications "Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives", (juillet 2002) (aussi ISO/CEI 8825-1:2002).

9.2 Références informatives

[RFC1777] Yeong, W., Howes, T., et S. Kille, "Protocole léger d'accès à un répertoire", mars 1995.

[RFC2156] Kille, S., "MIXER (Relais X.400 Internet amélioré pour Mime) : Transposition de X.400 au MIME de la RFC 822", janvier 1998.

[RFC3280] Housley, R., Polk, W., Ford, W., et D. Solo, "Profil Internet de certificat d'infrastructure de clé publique X.509 et liste de révocation de certificats (CRL)", avril 2002.

[RFC3494] Zeilenga, K., "Vers un dépassement de la version 2 du Protocole léger d'accès à un répertoire (LDAPv2)", mars 2003.

[RFC3642] Legg, S., "Éléments communs des codages des règles de codage de chaîne générique (GSER)", octobre 2003.

[RFC4234] Crocker, D. and P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", octobre 2005.

[RFC4511] Sermersheim, J., Ed., "Protocole léger d'accès à un répertoire (LDAP) : Le Protocole", juin 2006.

[RFC4513] Harrison, R. Ed., "Protocole léger d'accès à un répertoire (LDAP) : Méthodes d'authentification et mécanismes de sécurité", juin 2006.

[RFC4520] Zeilenga, K., "Considérations de l'Autorité d'allocation des numéros de l'Internet (IANA) sur le Protocole léger d'accès à un répertoire (LDAP)", BCP 64, juin 2006.

Appendice A.

Le présent appendice est pour information seulement.

Le présent appendice donne les grammaires ABNF [RFC4234] pour les codages spécifiques de LDAP fondés sur GSER [RFC3641] spécifiés dans ce document. Ces grammaires ont été produites en utilisant, et en s'appuyant sur les éléments communs pour les codages GSER [RFC3642].

A.1 CertificateExactAssertion

```
CertificateExactAssertion = "{" sp cea-serialNumber "," sp cea-issuer sp "}"
  cea-serialNumber = id-serialNumber msp CertificateSerialNumber
  cea-issuer = id-issuer msp Name
  id-serialNumber = %x73.65.72.69.61.6C.4E.75.6D.62.65.72 ; 'serialNumber'
  id-issuer = %x69.73.73.75.65.72 ; 'issuer'
  Name = id-rdnSequence ":" RDNSequence
  id-rdnSequence = %x72.64.6E.53.65.71.75.65.6E.63.65 ; 'rdnSequence'
  CertificateSerialNumber = INTEGER
```

A.2 CertificateAssertion

```
CertificateAssertion = "{" [ sp ca-serialNumber ]
    [ sep sp ca-issuer ]
    [ sep sp ca-subjectKeyIdentifier ]
    [ sep sp ca-authorityKeyIdentifier ]
    [ sep sp ca-certificateValid ]
    [ sep sp ca-privateKeyValid ]
    [ sep sp ca-subjectPublicKeyAlgID ]
    [ sep sp ca-keyUsage ]
    [ sep sp ca-subjectAltName ]
    [ sep sp ca-policy ]
    [ sep sp ca-pathToName ]
    [ sep sp ca-subject ]
    [ sep sp ca-nameConstraints ] sp "}"

ca-serialNumber = id-serialNumber msp CertificateSerialNumber
ca-issuer = id-issuer msp Name
ca-subjectKeyIdentifier = id-subjectKeyIdentifier msp SubjectKeyIdentifier
ca-authorityKeyIdentifier = id-authorityKeyIdentifier msp AuthorityKeyIdentifier
ca-certificateValid = id-certificateValid msp Time
ca-privateKeyValid = id-privateKeyValid msp GeneralizedTime
ca-subjectPublicKeyAlgID = id-subjectPublicKeyAlgID msp
    OBJECT-IDENTIFIER
ca-keyUsage = id-keyUsage msp KeyUsage
ca-subjectAltName = id-subjectAltName msp AltNameType
ca-policy = id-policy msp CertPolicySet
ca-pathToName = id-pathToName msp Name
ca-subject = id-subject msp Name
ca-nameConstraints = id-nameConstraints msp NameConstraintsSyntax

id-subjectKeyIdentifier = %x73.75.62.6A.65.63.74.4B.65.79.49.64.65.6E.74.69.66.69.65.72
    ; 'subjectKeyIdentifier'
id-authorityKeyIdentifier = %x61.75.74.68.6F.72.69.74.79.4B.65.79.49.64.65.6E.74.69.66.69.65.72
    ; 'authorityKeyIdentifier'
id-certificateValid = %x63.65.72.74.69.66.69.63.61.74.65.56.61.6C.69.64
    ; 'certificateValid'
id-privateKeyValid = %x70.72.69.76.61.74.65.4B.65.79.56.61.6C.69.64
    ; 'privateKeyValid'
```

```
id-subjectPublicKeyAlgID  = %x73.75.62.6A.65.63.74.50.75.62.6C.69.63.4B.65.79.41.6C.67.49.44
    ; 'subjectPublicKeyAlgID'
id-keyUsage = %x6B.65.79.55.73.61.67.65 ; 'keyUsage'
id-subjectAltName = %x73.75.62.6A.65.63.74.41.6C.74.4E.61.6D.65
    ; 'subjectAltName'
id-policy = %x70.6F.6C.69.63.79 ; 'policy'
id-pathToName = %x70.61.74.68.54.6F.4E.61.6D.65 ; 'pathToName'
id-subject = %x73.75.62.6A.65.63.74 ; 'subject'
id-nameConstraints = %x6E.61.6D.65.43.6F.6E.73.74.72.61.69.6E.74.73
    ; 'nameConstraints'

SubjectKeyIdentifier = KeyIdentifier

KeyIdentifier = OCTET-STRING

AuthorityKeyIdentifier = "{" [ sp aki-keyIdentifier ]
    [ sep sp aki-authorityCertIssuer ]
    [ sep sp aki-authorityCertSerialNumber ] sp "}"

aki-keyIdentifier = id-keyIdentifier msp KeyIdentifier
aki-authorityCertIssuer = id-authorityCertIssuer msp GeneralNames

GeneralNames = "{" sp GeneralName *( "," sp GeneralName ) sp "}"
GeneralName  = gn-otherName
    / gn-rfc822Name
    / gn-dNSName
    / gn-x400Address
    / gn-directoryName
    / gn-ediPartyName
    / gn-uniformResourceIdentifier
    / gn-iPAddress
    / gn-registeredID

gn-otherName = id-otherName ":" OtherName
gn-rfc822Name = id-rfc822Name ":" IA5String
gn-dNSName = id-dNSName ":" IA5String
gn-x400Address = id-x400Address ":" ORAddress
gn-directoryName = id-directoryName ":" Name
gn-ediPartyName = id-ediPartyName ":" EDIPartyName
gn-iPAddress = id-iPAddress ":" OCTET-STRING
gn-registeredID = gn-id-registeredID ":" OBJECT-IDENTIFIER

gn-uniformResourceIdentifier = id-uniformResourceIdentifier
    ":" IA5String

id-otherName = %x6F.74.68.65.72.4E.61.6D.65 ; 'otherName'
gn-id-registeredID = %x72.65.67.69.73.74.65.72.65.64.49.44
    ; 'registeredID'

OtherName = "{" sp on-type-id "," sp on-value sp "}"
on-type-id = id-type-id msp OBJECT-IDENTIFIER
on-value = id-value msp Value
    ;; <Value> comme défini à la Section 3 de [RFC3641]

id-type-id = %x74.79.70.65.2D.69.64 ; 'type-id'
id-value = %x76.61.6C.75.65 ; 'value'

ORAddress = dquote *SafeIA5Character dquote
SafeIA5Character = %x01-21 / %x23-7F / ; ASCII minus dquote
    dquote dquote ; esquivé par des doubles guillemets
```

```
dquote = %x22 ; "" (double guillemets)

;; Note : La règle <ORAddress> code le composant x400Address d'un GeneralName comme une chaîne de caractères
entre des double guillemets. La chaîne de caractères est d'abord déduite conformément au paragraphe 4.1 de la
[RFC2156], puis tous les doubles guillemets incorporés sont esquivés par répétition. Cette chaîne résultante est sortie
entre des doubles guillemets.

EDIPartyName = "{" [ sp nameAssigner "," ] sp partyName sp "}"
nameAssigner = id-nameAssigner msp DirectoryString
partyName = id-partyName msp DirectoryString
id-nameAssigner = %x6E.61.6D.65.41.73.73.69.67.6E.65.72
    ; 'nameAssigner'

id-partyName    = %x70.61.72.74.79.4E.61.6D.65 ; 'partyName'

aki-authorityCertSerialNumber = id-authorityCertSerialNumber
    msp CertificateSerialNumber

id-keyIdentifier = %x6B.65.79.49.64.65.6E.74.69.66.69.65.72
    ; 'keyIdentifier'
id-authorityCertIssuer =
    %x61.75.74.68.6F.72.69.74.79.43.65.72.74.49.73.73.75.65.72
    ; 'authorityCertIssuer'

id-authorityCertSerialNumber = %x61.75.74.68.6F.72.69.74.79.43
    %x65.72.74.53.65.72.69.61.6C.4E.75.6D.62.65.72
    ; 'authorityCertSerialNumber'

Time = time-utcTime / time-generalizedTime
time-utcTime = id-utcTime ":" UTCTime
time-generalizedTime = id-generalizedTime ":" GeneralizedTime
id-utcTime = %x75.74.63.54.69.6D.65 ; 'utcTime'
id-generalizedTime = %x67.65.6E.65.72.61.6C.69.7A.65.64.54.69.6D.65
    ; 'generalizedTime'

KeyUsage = BIT-STRING / key-usage-bit-list
key-usage-bit-list = "{" [ sp key-usage *( "," sp key-usage ) ] sp "}"

;; Note : La règle <key-usage-bit-list> code les bits un dans une valeur KeyUsage comme une liste d'identifiants
séparés par des virgules.

key-usage = id-digitalSignature
    / id-nonRepudiation
    / id-keyEncipherment
    / id-dataEncipherment
    / id-keyAgreement
    / id-keyCertSign
    / id-cRLSign
    / id-encipherOnly
    / id-decipherOnly

id-digitalSignature = %x64.69.67.69.74.61.6C.53.69.67.6E.61.74
    %x75.72.65 ; 'digitalSignature'
id-nonRepudiation   = %x6E.6F.6E.52.65.70.75.64.69.61.74.69.6F.6E
    ; 'nonRepudiation'
id-keyEncipherment  = %x6B.65.79.45.6E.63.69.70.68.65.72.6D.65.6E.74
    ; 'keyEncipherment'
id-dataEncipherment = %x64.61.74.61.45.6E.63.69.70.68.65.72.6D.65.6E
    %x74 ; "dataEncipherment'
id-keyAgreement     = %x6B.65.79.41.67.72.65.65.6D.65.6E.74
```

```
    ; 'keyAgreement'
id-keyCertSign      = %x6B.65.79.43.65.72.74.53.69.67.6E
    ; 'keyCertSign'
id-cRLSign          = %x63.52.4C.53.69.67.6E ; "cRLSign"
id-encipherOnly     = %x65.6E.63.69.70.68.65.72.4F.6E.6C.79
    ; 'encipherOnly'
id-decipherOnly     = %x64.65.63.69.70.68.65.72.4F.6E.6C.79
    ; 'decipherOnly'

AltNameType = ant-builtinNameForm / ant-otherNameForm

ant-builtinNameForm = id-builtinNameForm ":" BuiltinNameForm
ant-otherNameForm = id-otherNameForm ":" OBJECT-IDENTIFIER

id-builtinNameForm = %x62.75.69.6C.74.69.6E.4E.61.6D.65.46.6F.72.6D
    ; 'builtinNameForm'
id-otherNameForm   = %x6F.74.68.65.72.4E.61.6D.65.46.6F.72.6D
    ; 'otherNameForm'

BuiltinNameForm  = id-rfc822Name
    / id-dNSName
    / id-x400Address
    / id-directoryName
    / id-ediPartyName
    / id-uniformResourceIdentifier
    / id-iPAddress
    / id-registeredId

id-rfc822Name = %x72.66.63.38.32.32.4E.61.6D.65 ; 'rfc822Name'
id-dNSName = %x64.4E.53.4E.61.6D.65 ; 'dNSName'
id-x400Address  = %x78.34.30.30.41.64.64.72.65.73.73 ; 'x400Address'
id-directoryName = %x64.69.72.65.63.74.6F.72.79.4E.61.6D.65
    ; 'directoryName'
id-ediPartyName  = %x65.64.69.50.61.72.74.79.4E.61.6D.65
    ; 'ediPartyName'
id-iPAddress = %x69.50.41.64.64.72.65.73.73 ; 'iPAddress'
id-registeredId = %x72.65.67.69.73.74.65.72.65.64.49.64
    ; 'registeredId'

id-uniformResourceIdentifier = %x75.6E.69.66.6F.72.6D.52.65.73.6F.75
    %x72.63.65.49.64.65.6E.74.69.66.69.65.72
    ; 'uniformResourceIdentifier'

CertPolicySet = "{" sp CertPolicyId *( "," sp CertPolicyId ) sp "}"
CertPolicyId = OBJECT-IDENTIFIER

NameConstraintsSyntax = "{" [ sp ncs-permittedSubtrees ]
    [ sep sp ncs-excludedSubtrees ] sp "}"

ncs-permittedSubtrees = id-permittedSubtrees msp GeneralSubtrees
ncs-excludedSubtrees = id-excludedSubtrees  msp GeneralSubtrees

id-permittedSubtrees =
    %x70.65.72.6D.69.74.74.65.64.53.75.62.74.72.65.65.73
    ; 'permittedSubtrees'
id-excludedSubtrees =
    %x65.78.63.6C.75.64.65.64.53.75.62.74.72.65.65.73
    ; 'excludedSubtrees'

GeneralSubtrees = "{" sp GeneralSubtree
```

```
    *( "," sp GeneralSubtree ) sp "}"
GeneralSubtree  = "{" sp gs-base
    [ "," sp gs-minimum ]
    [ "," sp gs-maximum ] sp "}"

gs-base = id-base msp GeneralName
gs-minimum = id-minimum msp BaseDistance
gs-maximum = id-maximum msp BaseDistance

id-base = %x62.61.73.65 ; 'base'
id-minimum = %x6D.69.6E.69.6D.75.6D ; 'minimum'
id-maximum = %x6D.61.78.69.6D.75.6D ; 'maximum'

BaseDistance = INTEGER-0-MAX
```

A.3 CertificatePairExactAssertion

```
CertificatePairExactAssertion = "{" [ sp cpea-issuedTo ]
    [sep sp cpea-issuedBy ] sp "}"
;; Au moins un de <cpea-issuedTo> ou de <cpea-issuedBy> DOIT être présent.

cpea-issuedTo = id-issuedToThisCAAssertion msp
    CertificateExactAssertion
cpea-issuedBy = id-issuedByThisCAAssertion msp
    CertificateExactAssertion

id-issuedToThisCAAssertion = %x69.73.73.75.65.64.54.6F.54.68.69.73
    %x43.41.41.73.73.65.72.74.69.6F.6E ; 'issuedToThisCAAssertion'
id-issuedByThisCAAssertion = %x69.73.73.75.65.64.42.79.54.68.69.73
    %x43.41.41.73.73.65.72.74.69.6F.6E ; 'issuedByThisCAAssertion'
```

A.4 CertificatePairAssertion

```
CertificatePairAssertion = "{" [ sp cpa-issuedTo ]
    [sep sp cpa-issuedBy ] sp "}"
;; Au moins un de <cpa-issuedTo> et de <cpa-issuedBy> DOIT être présent.

cpa-issuedTo = id-issuedToThisCAAssertion msp CertificateAssertion
cpa-issuedBy = id-issuedByThisCAAssertion msp CertificateAssertion
```

A.5 CertificateListExactAssertion

```
CertificateListExactAssertion = "{" sp clea-issuer ","
    sp clea-thisUpdate
    [ "," sp clea-distributionPoint ] sp "}"

clea-issuer = id-issuer msp Name
clea-thisUpdate = id-thisUpdate msp Time
clea-distributionPoint = id-distributionPoint msp
    DistributionPointName

id-thisUpdate = %x74.68.69.73.55.70.64.61.74.65 ; 'thisUpdate'
id-distributionPoint =
    %x64.69.73.74.72.69.62.75.74.69.6F.6E.50.6F.69.6E.74
    ; 'distributionPoint'

DistributionPointName = dpn-fullName / dpn-nameRelativeToCRLIssuer
```

```
dpn-fullName = id-fullName ":" GeneralNames
dpn-nameRelativeToCRLIssuer = id-nameRelativeToCRLIssuer ":"
    RelativeDistinguishedName

id-fullName = %x66.75.6C.6C.4E.61.6D.65 ; 'fullName'
id-nameRelativeToCRLIssuer = %x6E.61.6D.65.52.65.6C.61.74.69.76.65
    %x54.6F.43.52.4C.49.73.73.75.65.72 ; 'nameRelativeToCRLIssuer'
```

A.6 CertificateListAssertion

```
CertificateListAssertion = "{" [ sp cla-issuer ]
    [ sep sp cla-minCRLNumber ]
    [ sep sp cla-maxCRLNumber ]
    [ sep sp cla-reasonFlags ]
    [ sep sp cla-dateAndTime ]
    [ sep sp cla-distributionPoint ]
    [ sep sp cla-authorityKeyIdentifier ] sp "}"

cla-issuer = id-issuer msp Name
cla-minCRLNumber = id-minCRLNumber msp CRLNumber
cla-maxCRLNumber = id-maxCRLNumber msp CRLNumber
cla-reasonFlags = id-reasonFlags msp ReasonFlags
cla-dateAndTime = id-dateAndTime msp Time

cla-distributionPoint = id-distributionPoint msp DistributionPointName

cla-authorityKeyIdentifier = id-authorityKeyIdentifier msp AuthorityKeyIdentifier

id-minCRLNumber = %x6D.69.6E.43.52.4C.4E.75.6D.62.65.72
    ; 'minCRLNumber'
id-maxCRLNumber = %x6D.61.78.43.52.4C.4E.75.6D.62.65.72
    ; 'maxCRLNumber'
id-reasonFlags = %x72.65.61.73.6F.6E.46.6C.61.67.73 ; 'reasonFlags'
id-dateAndTime = %x64.61.74.65.41.6E.64.54.69.6D.65 ; 'dateAndTime'

CRLNumber = INTEGER-0-MAX

ReasonFlags = BIT-STRING
    / "{" [ sp reason-flag *( "," sp reason-flag ) ] sp "}"

reason-flag = id-unused
    / id-keyCompromise
    / id-cACompromise
    / id-affiliationChanged
    / id-superseded
    / id-cessationOfOperation
    / id-certificateHold
    / id-privilegeWithdrawn
    / id-aACompromise

id-unused = %x75.6E.75.73.65.64 ; 'unused'
id-keyCompromise = %x6B.65.79.43.6F.6D.70.72.6F.6D.69.73.65
    ; 'keyCompromise'
id-cACompromise = %x63.41.43.6F.6D.70.72.6F.6D.69.73.65
    ; 'cACompromise'
id-affiliationChanged =
    %x61.66.66.69.6C.69.61.74.69.6F.6E.43.68.61.6E.67.65.64
    ; 'affiliationChanged'
```

```
id-superseded = %x73.75.70.65.72.73.65.64.65.64 ; 'superseded'
id-cessationOfOperation =
    %x63.65.73.73.61.74.69.6F.6E.4F.66.4F.70.65.72.61.74.69.6F.6E
    ; 'cessationOfOperation'
id-certificateHold = %x63.65.72.74.69.66.69.63.61.74.65.48.6F.6C.64
    ; 'certificateHold'
id-privilegeWithdrawn =
    %x70.72.69.76.69.6C.65.67.65.57.69.74.68.64.72.61.77.6E
    ; 'privilegeWithdrawn'
id-aACompromise = %x61.41.43.6F.6D.70.72.6F.6D.69.73.65
    ; 'aACompromise'
```

A.7 AlgorithmIdentifier

```
AlgorithmIdentifier = "{" sp ai-algorithm  [ "," sp ai-parameters ] sp "}"
  ai-algorithm = id-algorithm msp OBJECT-IDENTIFIER
  ai-parameters = id-parameters msp Value
  id-algorithm = %x61.6C.67.6F.72.69.74.68.6D ; 'algorithm'
  id-parameters = %x70.61.72.61.6D.65.74.65.72.73 ; 'parameters'
```

Adresse de l'auteur

Kurt D. Zeilenga
OpenLDAP Foundation
EMail: Kurt@OpenLDAP.org

RemerciementLe financement de la fonction d'édition des RFC est fourni par la Administrative Support Activity (IASA) de l'IETF.