Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre	Ministère du budget, des comptes publics et de la réforme de l'État
Agence nationale de la sécurité des systèmes d'information	Direction générale de la modernisation de l'État

Référentiel Général de Sécurité

version 1.0

Annexe A14

Profils de Certificats / LCR / OCSP et Algorithmes Cryptographiques

Version 2.3 du 11 février 2010

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
06/11/2006	2.1	*Document constitutif de la Politique de Référencement Intersectorielle de Sécurité – PRISv2.1.*	DCSSI / SDAE
12/12/2008	2.2	*Document constitutif du Référentiel Général de Sécurité – RGSv0.98, annexe A14.* Modifications : • Ajout extension pour certificat de signature qualifiée ; • Modification extension pour certificat authentification serveur ; • Modification du champ *reasonCode* des LCR ; • Précisions sur le codage des DN et des ICD ; • Réécriture du chapitre 5.	DCSSI / DGME
11/02/2010	2.3	*Document constitutif du Référentiel Général de Sécurité – RGSv1.0, annexe A14.* Modifications : • Précisions sur les champs *keyUsage* et *ExtendedKeyUsage* ; • Précisions sur le champ *nextUpdate* ; • Réécriture du chapitre 5.	ANSSI / DGME

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

rgs@ssi.gouv.fr

Direction générale de la modernisation de l'État

Service Projets

64-70 allée de Bercy
75012 Paris

rgs.dgme@finances.gouv.fr

SOMMAIRE

I. INTRODUCTION 4

II. CERTIFICATS 5

II.1. Certificats d'AC 5

II.1.1. Champs de base 5

II.1.2. Extensions 5

II.2. Certificats porteurs 6

II.2.1. Champs de base 6

II.2.2. Extensions 7

II.3. Certificats de machines 9

II.3.1. Champs de base 9

II.3.2. Extensions 9

III. LISTE DE CERTIFICATS RÉVOQUÉS 12

III.1. Champs de base 12

III.2. Extensions de LCR 12

III.3. Extensions d'entrée de LCR 13

IV. PROTOCOLES D'ETAT EN LIGNE DES CERTIFICATS 14

V. ALGORITHMES ET LONGUEURS DE CLÉS 15

VI. ANNEXE 1 - DOCUMENTS DE RÉFÉRENCE 16

VI.1. Réglementation 16

VI.2. Documents techniques 16

VII. ANNEXE 2 - EXIGENCES SUR LES IDENTIFIANTS D'AC, DE PORTEURS ET DE MACHINES 17

VII.1. Identification d'une Autorité de Certification 17

VII.2. Identification de porteur 17

VII.2.1. Certificats [ENTREPRISE] et [ADMINISTRATION] 18

VII.2.2. Certificats [ENTREPRISE], [ADMINISTRATION], [PARTICULIER] 18

VII.3. Identification d'une machine 19

I. Introduction

Les politiques de certification types (PC Types), annexes du [RGS], contiennent des règles sur les formats des certificats, des LCR et des requêtes / réponses OCSP (état en ligne des certificats) ainsi que sur les mécanismes cryptographiques.

Ces règles, communes à toutes les fonctions de sécurité à base de certificats traitées dans les PC Types, ont été factorisées dans le présent document. Celui-ci précise, lorsqu'il y en a, les différences entre les fonctions de sécurité et/ou les niveaux de sécurité.

II. Certificats

II.1. Certificats d'AC

Ce chapitre porte sur les certificats de clés d'AC utilisées pour la signature de certificats de porteurs ou de machines, et à la signature de LCR.

II.1.1. Champs de base

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat d'AC conforme au [RGS] doit respecter, de base, les exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Intitulé de l'exigence
Version	La valeur de ce champ doit être "2", indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Issuer	Ce champ doit être un DN répondant aux exigences du chapitre VII ci-dessous.
Validity	Pas d'exigence supplémentaire par rapport au [RFC5280]
Subject	Ce champ doit respecter les mêmes exigences que le champ "Issuer".
Subject Public Key Info	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Unique Identifiers (issuer et subject)	Les PC Types du [RGS] imposant l'unicité des DN des champs Issuer et Subject au sein du domaine de l'AC, les champs Unique Identifiers ne doivent pas être utilisés.
Extensions	Cf. chapitre suivant.

II.1.2. Extensions

Une extension d'un certificat est caractérisée par :

- Sa présence obligatoire ou non dans le certificat. Ceci indique si l'AC émettrice du certificat a l'obligation ou non d'intégrer l'extension dans tous les certificats qu'elle émet.
- Sa criticité. Ceci indique comment les utilisateurs de certificats doivent traiter l'extension et le certificat correspondant, ceci conformément aux principes de gestion de la criticité définis dans [X.509].

Le tableau ci-dessous présente les exigences requises par le [RGS] en complément des exigences définies dans [RFC5280], en précisant le caractère obligatoire de chaque extension (colonne "O", O(ui)/N(on)) et sa criticité (colonne "C", O(ui)/N(on)).

Les extensions qui apparaissent dans ce tableau doivent respecter l'ensemble des exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis ici.

Les autres extensions traitées dans le [RFC5280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC5280]. Notamment, les extensions obligatoires pour les certificats d'AC (Basic Constraints, Authority / Subject Key Identifiers,...) doivent être intégrées. La prise en compte des extensions non obligatoires est laissée au choix de l'AC.

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC5280]. Lorsque le [RFC5280] n'impose pas d'exigence de criticité, l'extension doit être systématiquement marquée "non critique". De même, l'AC peut intégrer des extensions non traitées ni dans le [RFC5280] ni dans le présent document, y compris des extensions propriétaires, mais ces extensions doivent obligatoirement être marquées "non critiques".

Champ	O	C	Intitulé de l'exigence
Authority Key Identifier	O	N	Cette extension doit être présente, être marquée "non critique" et contenir l'identifiant de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice).
Key Usage	O	O	Cette extension doit être marquée "critique".
Certificate Policies	O	N	Cette extension doit être conforme aux exigences du chapitre 3.2.3 du [RFC3739].
Subject Alternative Name *Issuer Alternative Name*	N	N	L'identification des AC via les DN des champs Subject et Issuer étant obligatoire dans les PC Types du [RGS], les champs Subject Alternative Name et Issuer Alternative Name peuvent être présents, mais ils doivent obligatoirement être marqués "non critique" et être conformes aux exigences du chapitre 3.2.1 du [RFC3739].
CRL Distribution Points	O	N	Pour les certificats d'AC autres que les certificats auto-signés (AC Racine), cette extension doit être présente et être conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT].
Basic Constraints	O	O [1]	Pas d'exigences supplémentaires par rapport à la [RFC5280]
Authority Information Access	O [2]	N	Si l'AC fournit un service OCSP (ce qui est recommandé par les PC Types du [RGS]), cette extension doit être présente, marquée "non critique" et être conforme aux exigences du chapitre 3.1 du [RFC2560].

II.2. Certificats porteurs

II.2.1. Champs de base

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat porteur conforme au [RGS] doit respecter, de base, les exigences correspondantes du [RFC5280], du [RFC3739] et de [ETSI_QC] pour les certificats qualifiés, moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

[1] Cette extension peut être éventuellement non critique dans certains cas précisés dans la [RFC5280].

[2] Si l'AC fournit un service OCSP, ce champ doit être présent. Inversement, si ce champ est présent, l'AC doit fournir le service correspondant.

Champ	Intitulé de l'exigence
Version	La valeur de ce champ doit être "2", indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Issuer	Ce champ est un DN répondant aux exigences du chapitre VII ci-dessous.
Validity	Pas d'exigence supplémentaire par rapport au [RFC5280]
Subject	Ce champ doit être un DN répondant aux exigences du chapitre VII ci-dessous.
Subject Public Key Info	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Unique Identifiers (issuer et subject)	Les PC Types du [RGS] imposant l'unicité des DN des champs Issuer et Subject au sein du domaine de l'AC, les champs Unique Identifiers ne doivent pas être utilisés.
Extensions	Cf. chapitre suivant.

II.2.2. Extensions

Une extension d'un certificat est caractérisée par :

- Sa présence obligatoire ou non dans le certificat. Ceci indique si l'AC émettrice du certificat a l'obligation ou non d'intégrer l'extension dans tous les certificats qu'elle émet.
- Sa criticité. Ceci indique comment les utilisateurs de certificats doivent traiter l'extension et le certificat correspondant, ceci conformément aux principes de gestion de la criticité définis dans [X.509].

Le tableau ci-dessous présente les exigences requises par le [RGS] en complément des exigences définies dans [RFC5280], en précisant le caractère obligatoire de chaque extension (colonne "O", O(ui)/N(on)) et sa criticité (colonne "C", O(ui)/N(on)).

Les extensions qui apparaissent dans ce tableau doivent respecter l'ensemble des exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis ici.

Les autres extensions traitées dans le [RFC5280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC5280]. La prise en compte des extensions non obligatoires est laissée au choix de l'AC.

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC5280]. Lorsque le [RFC5280] n'impose pas d'exigence de criticité, l'extension doit être systématiquement marquée "non critique". De même, l'AC peut intégrer des extensions non traitées ni dans le [RFC5280] ni dans le présent document, y compris des extensions propriétaires, mais ces extensions doivent obligatoirement être marquées "non critiques".

Champ	Intitulé de l'exigence					
	O	**C**	**PC Type Signature**	**PC Type Authentification**	**PC Type Authentification et Signature**	**PC Type Confidentialité**
Authority Key Identifier	O	N	Pour tous les certificats porteurs, cette extension doit être présente, être marquée "non critique" et contenir l'identifiant de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice).			
Key Usage	O	O	Le bit "nonRepudiation[3]" doit être à "1", les autres bits à "0".	Le bit "digitalSignature" doit être à "1", les autres bits à "0".	Les bits " nonRepudiation " et "digitalSignature" doivent être à "1", les autres bits à "0".	Le bit "keyEncipherment" pour une clé RSA ou (exclusif) le bit "keyAgreement" ou (exclusif) le bit "dataEncipherment " doit être à "1", les autres bits à "0"
Certificate Policies	O	N	Cette extension doit être conforme aux exigences du chapitre 3.2.3 du [RFC3739].			
Subject Alternative Name	N	N	L'identification du porteur via le DN du champ Subject étant obligatoire dans les PC Types du [RGS], le champ Subject Alternative Name peut être présent, mais il doit obligatoirement être marqué "non critique" et être conforme aux exigences du chapitre 3.2.1 du [RFC3739].			
Issuer Alternative Name	N	N	L'identification de l'AC émettrice via le DN du champ Issuer étant obligatoire dans les PC Types du [RGS], le champ Issuer Alternative Name peut être présent, mais il doit obligatoirement être marqué "non critique".			
Subject Directory Attributes	N	N	Si cette extension est utilisée, elle doit être conforme aux exigences du chapitre 3.2.2 du [RFC3739].			
CRL Distribution Points	O	N	Cette extension doit être présente et être conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT].			
Freshest CRL	O[4]	N	Si l'AC utilise des deltaLCR (ce qui est recommandé par les PC Types du [RGS]), cette extension doit être présente. La syntaxe de cette extension étant identique à celle de "CRL Distribution Points", elle doit être également conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT].			
Authority Information Access	O[5]	N	Si l'AC fournit un service OCSP (ce qui est recommandé par les PC Types du [RGS]), cette extension doit être présente, marquée "non critique" et être conforme aux exigences du chapitre 3.1 du [RFC2560].			
QCStatements	Applicable uniquement pour les certificats de signature électronique (***). Les exigences sont décrites ci-après.					

[3] Le bit nonRepudiation est désormais nommé contentCommitment

[4] Si l'AC émet des deltaLCR, ce champ doit être présent. Inversement, si ce champ est présent, l'AC doit fournir le service correspondant.

[5] Si l'AC fournit un service OCSP, ce champ doit être présent. Inversement, si ce champ est présent, l'AC doit fournir le service correspondant.

Extension QCStatements :

Pour les certificats de signature électronique (***), cette extension doit contenir a minima les deux OID évoqués aux chapitres 5.2.1 et 5.2.4 du document [ETSI_QC] :

- esi4-qcStatement-QcCompliance : indique que le certificat émis est qualifié conformément à la législation en vigueur dans le pays dans lequel est établie l'AC :
- esi4-qcStatement-QcSSCD : indique que la clé privée correspondante est stockée dans un dispositif sécurisé de création de signature électronique (SSCD).

En France, le PSCE peut faire qualifier son offre de certificat de signature électronique :

- selon la PC Type Signature (***) conformément à la procédure de qualification des PSCO décrite dans le [DécretRGS] ;
- selon l'arrêté du 26 juillet 2004 décrivant le schéma de qualification des PSCE délivrant des certificats qualifiés conformément au décret [SIG].

II.3. Certificats de machines

II.3.1. Champs de base

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat de machine (serveur par exemple), conforme aux exigences de la PC Type « authentification serveur » ou de la PC Type « cachet », doit respecter, de base, les exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Intitulé de l'exigence
Version	La valeur de ce champ doit être "2", indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Issuer	Ce champ est un DN répondant aux exigences du chapitre VII ci-dessous.
Validity	Pas d'exigence supplémentaire par rapport au [RFC5280]
Subject	Ce champ doit être un DN répondant aux exigences du chapitre VII ci-dessous.
Subject Public Key Info	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Unique Identifiers (issuer et subject)	Les PC Types du [RGS] imposant l'unicité des DN des champs Issuer et Subject au sein du domaine de l'AC, les champs Unique Identifiers ne doivent pas être utilisés.
Extensions	Cf. chapitre suivant.

II.3.2. Extensions

Une extension d'un certificat est caractérisée par :

- Sa présence obligatoire ou non dans le certificat. Ceci indique si l'AC émettrice du certificat a l'obligation ou non d'intégrer l'extension dans tous les certificats qu'elle émet.
- Sa criticité. Ceci indique comment les utilisateurs de certificats doivent traiter l'extension et le certificat correspondant, ceci conformément aux principes de gestion de la criticité définis dans [X.509].

Le tableau ci-dessous présente les exigences requises par le [RGS] en complément des exigences définies dans [RFC5280], en précisant le caractère obligatoire de chaque extension (colonne "O", O(ui)/N(on)) et sa criticité (colonne "C", O(ui)/N(on)).

Les extensions qui apparaissent dans ce tableau doivent respecter l'ensemble des exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis ici.

Les autres extensions traitées dans le [RFC5280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC5280]. La prise en compte des extensions non obligatoires est laissée au choix de l'AC.

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC5280]. Lorsque le [RFC5280] n'impose pas d'exigence de criticité, l'extension doit être systématiquement marquée "non critique". De même, l'AC peut intégrer des extensions non traitées ni dans le [RFC5280] ni dans le présent document, y compris des extensions propriétaires, mais ces extensions doivent obligatoirement être marquées "non critiques".

Champ	O	C	Intitulé de l'exigence
Authority Key Identifier	O	N	Pour tous les certificats de machines, cette extension doit être présente, être marquée "non critique" et contenir l'identifiant de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice).
Key Usage	O	O	*Pour les certificats d'authentification de type serveur SSL/TLS* - Le serveur doit disposer d'un certificat pour lequel un seul bit parmi les bits « keyEncipherement » (pour une clé RSA), « keyAgreement » (pour une clé Diffie-Hellman) et « digitalSignature » est à 1 et tous les autres à 0. Si plusieurs modes d'authentification et d'échange de clé sont acceptés par le serveur, les certificats correspondants doivent être distincts. *Pour les certificats d'authentification serveur de type client*- Les bits "digitalSignature" ou (exclusif) "keyAgreement" doivent être à "1", tous les autres bits à "0". *Pour les certificats cachet* - Le bit "digitalSignature" (et éventuellement le bit « nonRepudiation ») doit être à "1", tous les autres bits à "0".
Certificate Policies	O	N	Cette extension doit être conforme aux exigences du chapitre 3.2.3 du [RFC3739].
Subject Alternative Name	N	N	L'identification du serveur via le DN du champ Subject étant obligatoire dans les présentes PC Type, le champ Subject Alternative Name peut être présent, mais il doit obligatoirement être marqué "non critique".
Issuer Alternative Name	N	N	L'identification de l'AC émettrice via le DN du champ Issuer étant obligatoire dans les présentes PC Type, le champ Issuer Alternative Name peut être présent, mais il doit obligatoirement être marqué "non critique".

Champ	O	C	Intitulé de l'exigence
Subject Directory Attributes	N	N	Si cette extension est utilisée, elle doit obligatoirement être marquée "non critique".
CRL Distribution Points	O	N	Cette extension doit être présente et être conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT].
Freshest CRL	O [6]	N	Si l'AC utilise des deltaLCR (ce qui est recommandé par les présentes PC Types), cette extension doit être présente. La syntaxe de cette extension étant identique à celle de "CRL Distribution Points", elle doit être également conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT].
Authority Information Access	O [7]	N	Si l'AC fournit un service OCSP (ce qui est recommandé par les présentes PC Types), cette extension doit être présente, marquée "non critique" et être conforme aux exigences du chapitre 3.1 du [RFC2560].
Extended Key Usage	O	N [8]	Pour les certificats cachet dont la clé privée est utilisée pour signer des contremarques de temps, cette extension doit contenir l'identifiant « id-kp-timeStamping » à l'exclusion de tout autre. Pour les certificats d'authentification serveur (authentification et sécurisation de session), cette extension doit contenir les valeurs suivantes : - « id-kp-serverAuth » pour les serveurs de type serveur SSL/TLS - « id-kp-clientAuth » pour les serveurs « clients » telles que définit dans [RFC5280].

[6] Si l'AC émet des deltaLCR, ce champ doit être présent. Inversement, si ce champ est présent, l'AC doit fournir le service correspondant.

[7] Si l'AC fournit un service OCSP, ce champ doit être présent. Inversement, si ce champ est présent, l'AC doit fournir le service correspondant.

[8] Pour les certificats cachet serveur dont la clé privée est utilisée pour signer des contremarques de temps, cette extension doit être marquée critique

III. Liste de Certificats Révoqués

III.1. Champs de base

Le tableau ci-dessous reprend l'ensemble des champs de base d'une LCR X.509v2. Une LCR conforme au [RGS] doit respecter, de base, les exigences correspondantes du [RFC5280], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Intitulé de l'exigence
Version	La valeur de ce champ doit être "1", indiquant qu'il s'agit d'une LCR version 2.
Signature	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
Issuer	Ce champ doit être identique au champ "Subject" du certificat d'AC dont la clé privée est utilisée pour signer la LCR (cf. chapitre II.1.1).
This Update	Pas d'exigence supplémentaire par rapport au [RFC5280]
Next Update	Pas d'exigence supplémentaire par rapport au [RFC5280]. Il est recommandé que ce champ soit fonction de la fréquence de publication définie dans le document [RGS_A_13][9]
Revoked Certificates	- userCertificate : pas d'exigence supplémentaire par rapport au [RFC5280] - revocationDate : pas d'exigence supplémentaire par rapport au [RFC5280] - crlEntryExtensions : cf. chapitre III.3
Extensions de LCR	Cf. chapitre suivant.

III.2. Extensions de LCR

Une extension de LCR est caractérisée par :

- Sa présence obligatoire ou non dans la LCR. Ceci indique si l'AC émettrice de la LCR a obligation ou non d'intégrer l'extension dans toutes les LCR qu'elle émet.
- Sa criticité. Ceci indique comment les utilisateurs de la LCR doivent traiter l'extension correspondante, ceci conformément aux principes de gestion de la criticité définis dans [X.509].

Le tableau ci-dessous présente les exigences requises par le [RGS] pour certaines extensions en complément de celles du [RFC5280]. Ce tableau précise le caractère obligatoire de chaque extension (colonne "O", O(ui)/N(on)) et sa criticité (colonne "C", O(ui)/N(on)).

[9] Exemples :
- (*) : next update = this update + 72h*2
- (**) : next update = this update + 24h*2
- (***) : next update = this update + 36h

Les autres extensions traitées dans le [RFC5280] et qui n'apparaissent pas dans ce tableau doivent respecter strictement les exigences du [RFC5280]. La prise en compte des extensions non obligatoires est laissée au choix de l'AC.

L'intégration de ces autres extensions (obligatoires et non obligatoires) doit respecter les exigences de criticité imposées par le [RFC5280]. Lorsque le [RFC5280] n'impose pas d'exigence de criticité, l'extension doit être systématiquement marquée "non critique". De même, l'AC peut intégrer des extensions non traitées ni dans le [RFC5280] ni dans le présent document, y compris des extensions propriétaires, mais ces extensions doivent obligatoirement être marquées "non critiques".

Champ	O	C	Intitulé de l'exigence
Authority Key Identifier	O	N	Cette extension doit être présente, être marquée "non critique" et contenir l'identifiant de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice).
Issuer Alternative Name	N	N	L'identification de l'AC émettrice via le DN du champ Issuer étant obligatoire dans les présentes PC Type, le champ Issuer Alternative Name peut être présent, mais il doit obligatoirement être marqué "non critique".
CRL Number	O	N	Cette extension doit obligatoirement être présente, être marquée "non critique" et être conforme aux exigences du [RFC5280]. Ce numéro doit être incrémenté de 1 à chaque nouvelle CRL[10].
Delta CRL Indicator	O [11]	O [11]	S'il s'agit d'une deltaLCR, cette extension doit obligatoirement être présente, être marquée "critique" et être conforme aux exigences du [RFC5280].
Freshest CRL	O [12]	N	Si l'AC utilise des deltaLCR (ce qui est recommandé par les présentes PC Types), cette extension doit être présente dans les LCR complètes (et absente dans les deltaLCR) et son contenu doit être identique au contenu de l'extension "Freshest CRL" des certificats des porteurs couverts par cette LCR (cf. chapitre II.2.2).

III.3. Extensions d'entrée de LCR

Les extensions d'entrées de LCR doivent être conformes aux exigences du [RFC5280].

[10] Ceci permet à un téléservice qui se base sur ce champ d'avoir la garantie qu'il a effectivement récupéré la CRL attendue.

[11] Uniquement s'il s'agit d'une deltaLCR

[12] Obligatoire uniquement dans les LCR complètes et si l'AC émet des deltaLCR. Inversement, si ce champ est présent, l'AC doit fournir le service correspondant.

IV. Protocoles d'Etat en ligne des Certificats

Il n'y a pas d'exigence spécifique. Le service doit être conforme au [RFC2560].

V. Algorithmes et longueurs de clés

Ce chapitre liste les exigences relatives aux algorithmes cryptographiques et aux longueurs de clés conformes au [RGS] mis en œuvre dans les AC des PSCE.

Les règles à respecter concernant le choix et le dimensionnement des algorithmes cryptographiques et des longueurs de clés sont fixées dans le document [RGS_B_1][13].

Conformément à l'article 14 de l'[ORDONNANCE], les systèmes d'information existants à la date de publication du [RGS] disposent d'un délai pour se mettre en conformité avec celui-ci. En conséquence, les offres des PSCE pourront rester compatibles avec ces systèmes d'information. Elles pourront même obtenir, **dans le même délai,** une qualification au titre de l'[ORDONNANCE] sous réserve de recourir à des produits de sécurité qualifiés. Ces produits devront proposer, outre les éventuelles fonctions compatibles avec les systèmes existants[14], des fonctions conformes à l'annexe [RGS_B_1]. Cette exigence vise à faciliter la migration des systèmes existants vers des fonctions de sécurité conformes au [RGS].

Les remarques suivantes méritent d'être précisées :

- conformément au [RFC3279], l'identifiant utilisé dans le champ "subjectPublicKeyInfo" des certificats permet de spécifier l'algorithme cryptographique correspondant à la clé certifiée[15], mais ne permet pas de spécifier l'éventuel algorithme de hachage à utiliser en liaison avec cet algorithme cryptographique. L'information concernant les fonctions de hachage est donc fournie dans ce document à destination des applications et non pas à destination des AC ;
- si ce n'est pas l'AC qui génère le bi-clé du porteur / serveur, elle doit s'assurer que celle-ci est conforme aux exigences de ce chapitre ;
- pour les algorithmes pouvant être utilisés pour divers usages cryptographiques (authentification, signature, confidentialité), l'usage de la clé doit être restreint au travers du champ "keyUsage" du certificat.

[13] Notamment, les fonctions, algorithmes et longueurs de clé RSA 2048 bits, DSA 2048 bits / q=256, ECDSA (type GF(p)) avec q=256, SHA-256, DH 2048 bits / q=256, ECDH avec q=256.

[14] Seules les fonctions SHA-1 (160 bits), RSA 1024 bits, DSA 1024 bits avec q=160, ECDSA avec q=160, DH 1024 bits avec q=160, ECDH avec q=160 sont acceptées dans ce cadre.

[15] rsaEncryption, id-dsa, id-ecPublicKey, dhpublicnumber, id-ecPublicKey.

VI. Annexe 1 - Documents de référence

VI.1. Réglementation

Renvoi	Document
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
[SIG]	Décret n° 2001-272 du 20 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516.
[RGS]	Référentiel Général de Sécurité – Version 1

VI.2. Documents techniques

Renvoi	Document
[ETSI_CERT]	ETSI - TS 102 280 - X.509 V3 Certificate Profile for Certificates Issued to Natural Persons, V1.1.1 mars 2004
[ETSI_QC]	ETSI - TS 101 862 - Qualified certificate Profile, V1.3.3 janvier 2006
[PKCS#1]	RSA Laboratories - PKCS #1 v2.1 - RSA Cryptography Standard, 14 juin 2002
[RFC2560]	IETF - Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol, RFC 2560 - juin 1999
[RFC3279]	IETF - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profil - avril 2002
[RFC3739]	IETF - Internet X.509 Public Key Infrastructure, Qualified Certificates Profile, RFC 3726 - mars 2004
[RFC5280]	IETF - Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 5280- mai 2008
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 1.20
[X.509]	ITU - Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version 03/2000 (complétée par les correctifs techniques n° 1 de 10/2001, n° 2 de 04/2002 et n° 3 de 04/2004)

VII. Annexe 2 - Exigences sur les identifiants d'AC, de porteurs et de machines

VII.1. Identification d'une Autorité de Certification

Le DN qui se trouve dans le champ "Subject" d'un certificat d'AC, dans le champ "Issuer" d'un certificat d'AC ou d'utilisateur final, ainsi que dans le champ "Issuer" d'une LCR, doivent être conforme aux exigences des chapitres 4.1.2.4 de la RFC [5280], 3.1.1 de [RFC3739] et 5.2.4 de [ETSI_CERT], ainsi qu'aux exigences supplémentaires du présent chapitre.

Ce DN doit être encodé en printableString ou en UTF8String.

L'attribut countryName doit être présent et doit indiquer le pays de l'autorité compétente auprès de laquelle l'entité émettant le certificat est officiellement enregistrée (tribunal de commerce, ministère, …). Il doit être renseigné en lettres majuscules.

L'attribut organizationName doit être présent et doit contenir le nom officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes (cf. [ETSI_CERT]).

Une instance de l'attribut organizationalUnitName doit être présente et doit contenir l'identification de l'entité. L'instance de cet attribut doit être structurée conformément à la norme ISO 6523 et le format retenu est « <ICD> <Identification de l'organisation> » :

- l'ICD est sur 4 caractères ;
- l'identification de l'organisation sur 35 caractères :
- le séparateur entre les deux chaînes est un espace.

Pour les entités de droit français :

- ICD = 0002 ;
- l'identification est le n° SIREN ou le n° SIRET (9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Cette identification ne doit pas comporter d'espace. Ceci est cohérent avec la formalisation XML proposée par l'INSEE.

Pour les entités de droit non français, plusieurs possibilités existent :

- soit il n'y a pas d'instance de l'attribut organizationalUnitName conforme à la norme ISO 6523 et auquel cas elle ne doit pas commencer par 4 chiffres
- soit l'attribut organizationalUnitName est présent mais avec un numéro ICD différent de 0002
- soit l'attribut organizationalUnitName est présent et avec un numéro ICD égal à 0002, auquel cas il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France.

D'autres instances de l'attribut organizationalUnitName peuvent être présentes mais ne doivent pas commencer par 4 chiffres.

Exemple de DN : C=FR, O= Société ABC, OU= 0002 243516879, OU= Centre de Paris

VII.2. Identification de porteur

Le DN qui se trouve dans le champ "Subject" d'un certificat remis à une personne (par opposition à une machine) doit être conforme aux exigences des chapitres 4.1.2.6 du [RFC5280], 3.1.2 du [RFC3739] et 5.2.6 de [ETSI_CERT], ainsi qu'aux exigences supplémentaires du présent chapitre.

Les attributs du DN doivent être encodés en printableString ou en UTF8String[16].

VII.2.1. Certificats [ENTREPRISE] et [ADMINISTRATION]

Si le certificat n'est pas un certificat pseudonyme, une identification de l'entité à laquelle le porteur est rattaché est obligatoire.

L'attribut countryName doit être présent et doit indiquer le pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère, …). Il doit être renseigné en lettres majuscules.

L'attribut organizationName doit être présent et doit contenir le nom officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes.

Une instance de l'attribut organizationalUnitName doit être présente et doit contenir l'identification de cette entité telle que définie au chapitre VII.1.

Si d'autres instances de l'attribut organizationalUnitName sont présentes, elles ne doivent pas commencer par 4 chiffres.

Le CN doit être conforme au § VII.2.2.

VII.2.2. Certificats [ENTREPRISE], [ADMINISTRATION], [PARTICULIER]

L'attribut countryName doit être présent.

Si le certificat est un certificat pseudonyme, l'attribut pseudonym doit être utilisé mais pas les attributs givenName (GN), surname (SN) et commonName (CN) conformément à la [RFC3739].

Si le certificat n'est pas un certificat pseudonyme, deux possibilités :

- utilisation des attributs givenName et surname : l'attribut givenName doit comporter le premier prénom de l'état civil du porteur (si la pièce d'identité présentée pour l'enregistrement comporte d'autres prénoms, il n'y a pas d'obligation à mentionner ces autres prénoms dans le certificat, mais s'ils le sont, ils doivent l'être dans le même ordre que sur la pièce d'identité et séparés par une virgule sans espace ni avant ni après la virgule) et l'attribut surname doit comporter le nom de l'état civil du porteur. Pour les prénoms et noms composés, le tiret est utilisé comme élément séparateur. L'attribut commonName peut également être utilisé, dans ce cas l'AC précise dans sa PC son format et la sémantique correspondante. La distinction des cas d'homonymie au sein du domaine de l'AC peut se faire au travers de l'attribut commonName ;
- seul l'attribut commonName est utilisé : il doit comporter le premier prénom de l'état civil du porteur (si la pièce d'identité présentée pour l'enregistrement comporte d'autres prénoms, il n'y a pas d'obligation à mentionner ces autres prénoms dans le certificat, mais s'ils le sont, ils doivent l'être dans le même ordre que sur la pièce d'identité et séparés par une virgule sans espace ni avant ni après la virgule), suivi d'un espace, suivi du nom de l'état civil du porteur. Pour les prénoms et noms composés, le tiret est utilisé comme élément séparateur. A la suite du nom d'état civil, et en fonction des besoins de l'AC, d'autres informations peuvent être mentionnées dans cet attribut (séparées par des espaces), notamment des informations permettant de traiter les cas d'homonymie au sein du domaine de l'AC. L'AC doit préciser dans sa PC le format exact et la sémantique correspondante de l'attribut commonName.

[16] A l'exception des attributs `emailAddress` et `dc(domaincomponent)` qui, lorsque présents dans le DN du champ « Subject » doivent être en `IA5String` (afin de permettre la saisie du caractère « @ »).

Exemples de DN :

- C=FR, O= Société DEF, OU= 0002 243516879, OU= Site de Toulouse, CN= Michel Martin
- C=FR, O= Société DEF, OU= 0002 243516879, OU= Site de Toulouse, GN= Michel + SN = Martin

VII.3. Identification d'un service applicatif

Est entendu par « service applicatif » :

- un service de création de cachet tel que décrit dans la PC Type « Cachet » ;
- un service d'authentification de serveur tel que décrit dans la PC Type « Authentification serveur ».

Le DN qui se trouve dans le champ "Subject" d'un certificat remis à un service applicatif (par opposition à une personne physique) doit être conforme aux exigences des chapitres 4.1.2.6 du [RFC5280], 3.1.2 du [RFC3739] et 5.2.6 de [ETSI_CERT], ainsi qu'aux exigences supplémentaires du présent chapitre.

Ce DN doit être encodé en printableString ou en UTF8String.

L'attribut countryName doit être présent et doit indiquer le pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère, …). Il doit être renseigné en lettres majuscules.

L'attribut organizationName doit être présent et doit contenir le nom officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes et à laquelle le serveur est rattaché.

Une instance de l'attribut organizationalUnitName doit être présente et doit contenir l'identification de cette entité telle que définie au chapitre VII.1.

L'attribut commonName doit être utilisé et doit contenir un nom significatif du service applicatif. Lorsqu'il s'agit d'un certificat serveur de type SSL/TLS, ce nom significatif est le FQDN (Fully Qualified Domain Name) du serveur.

Les attributs givenName et surname ne doivent pas être utilisés.

Si un nom DNS (Domain Name System) est présent dans le commonName la [RFC1123] section 2.1 doit être appliquée en plus du [RFC1034]. Ceci permet de contrôler la validité du nom.

Si d'autres instances de l'attribut organizationalUnitName sont présentes, elles ne doivent pas commencer par 4 chiffres.

Exemple de DN : C=FR, O= Société ABC, OU= 0002 243516879, OU= Site de Toulouse, CN= www.abc.fr