



Premier ministre

**Agence nationale de la
sécurité
des systèmes d'information
(ANSSI)**

**Secrétariat général pour la
modernisation de l'action publique
(SGMAP)**

Référentiel Général de Sécurité

version 2.0

Annexe A4

**Profils de Certificats / LCR / OCSP et
Algorithmes Cryptographiques**

Version 3.0 du 27 février 2014

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
06/11/2006	2.1	<i>Document constitutif de la Politique de Référencement Intersectorielle de Sécurité – PRISv2.1.</i>	DCSSI / SDAE
12/12/2008	2.2	<i>Document constitutif du Référentiel Général de Sécurité – RGSv0.98, annexe A14.</i> Modifications : <ul style="list-style-type: none"> • Ajout extension pour certificat de signature qualifiée ; • Modification extension pour certificat authentification serveur ; • Modification du champ <i>reasonCode</i> des LCR ; • Précisions sur le codage des DN et des ICD ; • Réécriture du chapitre 5. 	DCSSI / DGME
11/02/2010	2.3	<i>Document constitutif du Référentiel Général de Sécurité – RGSv1.0, annexe A14.</i> Modifications : <ul style="list-style-type: none"> • Précisions sur les champs <i>keyUsage</i> et <i>ExtendedKeyUsage</i> ; • Précisions sur le champ <i>nextUpdate</i> ; • Réécriture du chapitre 5. 	ANSSI / DGME
27/02/2014	3.0	<i>Document constitutif du Référentiel Général de Sécurité – RGSv2.0, annexe A4.</i> Modifications : <ul style="list-style-type: none"> • Précisions sur le champ <i>basicConstraints</i> ; • Précisions sur le champ <i>authorityInformationAccess</i> ; • Précisions sur le champ <i>crlDistributionPoint</i> ; • Introduction d'une recommandation sur la génération des numéros de série. 	ANSSI

Les commentaires sur le présent document sont à adresser à :

5

<p>Agence nationale de la sécurité des systèmes d'information</p> <p>SGDSN/ANSSI</p> <p>51 boulevard de La Tour-Maubourg 75700 Paris 07 SP</p> <p>rgs@ssi.gouv.fr</p>

10

15

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	2/22

SOMMAIRE

	I. INTRODUCTION	4
	II. CERTIFICATS	5
5	II.1. Certificats d'AC.....	5
	II.1.1. Champs de base	5
	II.1.2. Extensions	5
	II.2. Certificats porteurs	7
10	II.2.1. Champs de base	7
	II.2.2. Extensions	7
	II.3. Certificats de machines	10
	II.3.1. Champs de base	10
	II.3.2. Extensions	10
	III. LISTE DE CERTIFICATS REVOQUES.....	14
15	III.1. Champs de base.....	14
	III.2. Extensions de LCR.....	14
	III.3. Extensions d'entrée de LCR	15
	IV. PROTOCOLES D'ETAT EN LIGNE DES CERTIFICATS.....	16
	V. ALGORITHMES ET LONGUEURS DE CLES	17
20	VI. ANNEXE 1 - DOCUMENTS DE REFERENCE	18
	VI.1. Réglementation	18
	VI.2. Documents techniques	18
	VII. ANNEXE 2 - EXIGENCES SUR LES IDENTIFIANTS D'AC, DE PORTEURS ET DE MACHINES.....	19
25	VII.1. Identification d'une Autorité de Certification.....	19
	VII.2. Identification de porteur	20
	VII.2.1. Certificats [ENTREPRISE] et [ADMINISTRATION].....	20
	VII.2.2. Certificats [ENTREPRISE], [ADMINISTRATION], [PARTICULIER].....	20
30	VII.3. Identification d'une machine.....	21

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques

Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	3/22

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.

- 5 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.

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	4/22

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 services applicatifs, et à la signature de LCR.

5 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
<i>Version</i>	La valeur de ce champ doit être "2", indiquant qu'il s'agit d'un certificat version 3.
<i>Serial number</i>	Il doit être généré pour être unique. Il est recommandé que le Serial Number soit non prédictible. Les AC en service lors de la parution de la V2.0 du RGS qui ne respecteraient pas cette exigence doivent le faire lors du renouvellement de leur certificat.
<i>Signature</i>	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
<i>Issuer</i>	Ce champ doit être un DN répondant aux exigences du chapitre VII ci-dessous.
<i>Validity</i>	Pas d'exigence supplémentaire par rapport au [RFC5280]
<i>Subject</i>	Ce champ doit respecter les mêmes exigences que le champ "Issuer".
<i>Subject Public Key Info</i>	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
<i>Unique Identifiers (issuer et subject)</i>	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.
<i>Extensions</i>	Cf. chapitre suivant.

10 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].

15

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)).

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	5/22

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.

5 **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.

10 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
<i>Identifiant de la clé de l'autorité / Authority Key Identifier</i>	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).
<i>Usages de la clé / Key Usage</i>	O	O	Cette extension doit être marquée "critique". Les bits keyCertSign et cRLSign doivent être à 1. Si l'AC signe des réponses OCSP, le bit digitalSignature doit être à 1.
<i>Politique de certification / Certificate Policies</i>	O	N	Cette extension doit être conforme aux exigences du chapitre 4.2.1.4 du [RFC5280].
<i>Autre nom de l'objet / de l'émetteur Subject Alternative Name Issuer Alternative Name</i>	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 4.1.2.4 du [RFC5280].
<i>Point de publication des listes de certificats révoqués / CRL Distribution Points</i>	N	N	S'il est proposé un service de LCR pour vérifier le statut de révocation du certificat d'AC concerné (à l'exception des certificats racines auto-signés), alors cette extension doit être présente, marquée "non critique". La règle générale est qu'il doit y avoir au moins une manière de vérifier le statut de révocation du certificat d'AC ; si cette extension n'est pas présente, alors l'extension suivante doit l'être.
<i>Accès aux informations publiées par l'AC / Authority Information Access</i>	N	N	S'il est proposé un service de validation de certificat en ligne (type serveur OCSP pour « Online Certificate Service Protocol »), alors cette extension doit être renseignée du type de service proposé et de la méthode à suivre pour l'atteindre, conformément au chapitre 4.2.2.1 de [RFC5280]. Si cette extension n'est pas présente, alors l'extension précédente doit l'être.

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	6/22

Champ	O	C	Intitulé de l'exigence
<i>Basic Constraints</i>	O	O	<p>Pour les certificats d'AC utilisés pour la signature de certificats de personnes physiques ou de services applicatifs, le champ <i>pathLenConstraint</i> doit être positionné à « 0 ».</p> <p>Pour les certificats d'AC utilisés pour la signature de certificats d'AC, il est recommandé de positionner dans le champ <i>pathLenConstraint</i> la valeur adéquate.</p>

II.2. Certificats porteurs

II.2.1. Champs de base

5 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.

Champ	Intitulé de l'exigence
<i>Version</i>	La valeur de ce champ doit être "2", indiquant qu'il s'agit d'un certificat version 3.
<i>Serial number</i>	Il doit avoir été généré pour être unique. Il est recommandé que le Serial Number soit non prédictible. Les AC en service lors de la parution de la V2.0 du RGS qui ne respecteraient pas cette exigence doivent le faire sous trois ans.
<i>Signature</i>	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
<i>Issuer</i>	Ce champ est un DN répondant aux exigences du chapitre VII ci-dessous.
<i>Validity</i>	Pas d'exigence supplémentaire par rapport au [RFC5280]
<i>Subject</i>	Ce champ doit être un DN répondant aux exigences du chapitre VII ci-dessous.
<i>Subject Public Key Info</i>	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
<i>Unique Identifiers (issuer et subject)</i>	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.
<i>Extensions</i>	Cf. chapitre suivant.

II.2.2. Extensions

10 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.

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	7/22

- 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.

- 10 **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.

15 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
<i>Authority Key Identifier</i>	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).			
<i>Key Usage</i>	O	O	Le bit "nonRepudiation" 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"
<i>Certificate Policies</i>	O	N	Cette extension doit être conforme aux exigences du chapitre 3.2.3 du [RFC3739].			
<i>Subject Alternative Name</i>	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 4.1.2.4 du [RFC5280].			
<i>Issuer Alternative Name</i>	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".			

¹ Le bit nonRepudiation est désormais nommé contentCommitment

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OSCP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	8/22

Champ	Intitulé de l'exigence					
	O	C	PC Type Signature	PC Type Authentification	PC Type Authentification et Signature	PC Type Confidentialité
<i>Subject Directory Attributes</i>	N	N	Si cette extension est utilisée, elle doit être conforme aux exigences du chapitre 3.2.2 du [RFC3739].			
<i>CRL Distribution Points</i>	N	N	S'il est proposé un service de CRL pour vérifier le statut de révocation du certificat concerné, alors cette extension doit être présente, marquée "non critique" et être conforme aux exigences du chapitre 5.4.14 de [ETSI_CERT]. La règle générale est qu'il doit y avoir au moins une manière de vérifier le statut de révocation du certificat (par CRL ou par OCSP).			
<i>Freshest CRL</i>	N ²	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].			
<i>Authority Information Access</i>	N	N	S'il est proposé un service OCSP pour vérifier le statut de révocation du certificat concerné, alors cette extension doit être présente, marquée "non critique" et être conforme aux exigences du chapitre 3.1 du [RFC2560]. La règle générale est qu'il doit y avoir au moins une manière de vérifier le statut de révocation du certificat (par CRL ou par OCSP).			
<i>QCStatements</i>	Applicable uniquement pour les certificats de signature électronique (***). Les exigences sont décrites ci-après.					

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] :

- 5
- 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 :

- 10
- 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 [Décret2001-272].

² Si l'AC émet des deltaLCR, ce champ doit être présent. Inversement, si ce champ est présent, l'AC doit fournir le service correspondant.

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	9/22

II.3. Certificats de services applicatifs

II.3.1. Champs de base

5 Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3. Un certificat de services applicatifs (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
<i>Version</i>	La valeur de ce champ doit être "2", indiquant qu'il s'agit d'un certificat version 3.
<i>Serial number</i>	Il doit avoir été généré pour être unique. Il est recommandé que le Serial Number soit non prédictible.
<i>Signature</i>	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
<i>Issuer</i>	Ce champ est un DN répondant aux exigences du chapitre VII ci-dessous.
<i>Validity</i>	Pas d'exigence supplémentaire par rapport au [RFC5280]
<i>Subject</i>	Ce champ doit être un DN répondant aux exigences du chapitre VII ci-dessous
<i>Subject Public Key Info</i>	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
<i>Unique Identifiers (issuer et subject)</i>	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.
<i>Extensions</i>	Cf. chapitre suivant.

II.3.2. Extensions

10 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].

15

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)).

20

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.

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	10/22

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.

5 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
<i>Authority Key Identifier</i>	O	N	Pour tous les certificats de services applicatifs, 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).
<i>Key Usage</i>	O	O	<p><i>Pour les certificats d'authentification de type serveur SSL/TLS ou de type serveur IPsec :</i></p> <ul style="list-style-type: none"> - si le mécanisme d'échange de clé est le chiffrement RSA, le bit « keyEncipherment » doit être à 1 ; - si le mécanisme d'échange de clé est Diffie-Hellman éphémère signé, le bit « digitalSignature » doit être à 1 ; - si le mécanisme d'échange de clé est Diffie-Hellman avec une clé publique fixe, le bit « keyAgreement » doit être à 1. <p>En particulier, cela signifie qu'une clé RSA (qui peut correspondre aux deux premiers cas), peut nécessiter d'avoir les deux bits « keyEncipherment » et « digital signature » à 1.</p> <p><i>Pour les certificats d'authentification serveur de type client-</i> Les bits "digitalSignature" ou (exclusif) "keyAgreement" doivent être à "1", tous les autres bits à "0".</p> <p><i>Pour les certificats cachet -</i> Le bit "digitalSignature" (et éventuellement le bit « nonRepudiation ») doit être à "1", tous les autres bits à "0".</p> <p><i>Pour les certificats de signature de code –</i> Le bit "digitalSignature" doit être à "1", tous les autres bits à "0".</p>
<i>Certificate Policies</i>	O	N	Cette extension doit être conforme aux exigences du chapitre 4.2.1.4 du [RFC5280].
<i>Subject Alternative Name</i>	O	N	Pour les certificats serveurs de type SSL/TLS, le champ Subject Alternative Name doit être présent. Il doit contenir au moins une entrée de type DNS Name correspondant à l'un des FQDN du service applicatif hébergé par la machine »
<i>Issuer Alternative Name</i>	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".
<i>Subject Directory Attributes</i>	N	N	Si cette extension est utilisée, elle doit obligatoirement être marquée "non critique".

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	11/22

Champ	O	C	Intitulé de l'exigence
<i>CRL Distribution Points</i>	N	N	<p>S'il est proposé un service de CRL pour vérifier le statut de révocation du certificat concerné, alors cette extension doit être présente, marquée "non critique".</p> <p>La règle générale est qu'il doit y avoir au moins une manière de vérifier le statut de révocation du certificat (par CRL ou par OCSP).</p>
<i>Freshest CRL</i>	N ³	N	<p>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].</p>
<i>Authority Information Access</i>	N	N	<p>S'il est proposé un service OCSP pour vérifier le statut de révocation du certificat concerné, alors cette extension doit être présente, marquée "non critique" et être conforme aux exigences du chapitre 3.1 du [RFC2560].</p> <p>La règle générale est qu'il doit y avoir au moins une manière de vérifier le statut de révocation du certificat (par CRL ou par OCSP).</p>
<i>Extended Key Usage</i>	O	N ⁴	<p>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.</p> <p>Pour les certificats dont la clé privée est utilisée pour signer des certificats de répondeurs OCSP, , conformément au chapitre 4.2.2.2 de la [RFC2560], cette extension doit contenir l'identifiant « id-kp-OCSPSigning » à l'exclusion de tout autre.</p> <p>Pour les certificats de signature de code, cette extension doit contenir l'identifiant « id-kp-codeSigning » à l'exclusion de tout autre.</p> <p>Pour les certificats d'authentification serveur (authentification et sécurisation de session), tel que défini dans la [RFC5280] cette extension doit contenir les valeurs suivantes :</p> <ul style="list-style-type: none"> - « id-kp-serverAuth » pour les serveurs de type serveur SSL/TLS ou de type serveur IPsec ; - « id-kp-clientAuth » pour les serveurs « clients » .

³ Si l'AC émet des deltaLCR, ce champ doit être présent. Inversement, si ce champ est présent, l'AC doit fournir le service correspondant.

⁴ Pour les certificats cachet serveur dont la clé privée est utilisée pour signer des contremarques de temps, cette extension doit être marquée critique

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	12/22

II.4. Certificats de recette

Les profils de certificat de recette sont identiques à ceux prévus par le présent document, avec les exceptions suivantes :

- 5 - Pour les certificats de personnes, les attributs commonName (CN), givenName (GN), surname (SN) ou pseudonym, s'ils sont présents dans le certificat, doivent débiter par la chaîne de caractères « TEST », suivie d'une espace, suivie de la valeur du champ prévue par la PC de l'AC ;
- 10 - Pour les certificats de services applicatifs, l'attribut commonName (CN) doit être présent sauf dans le cas d'un certificat de serveur SSL/TLS ou d'un certificat de signature de code (cf. VIII.3). Si l'attribut CN est présent, il doit débiter par la chaîne de caractères « TEST », suivie d'une espace, suivie de la valeur du champ prévue par la PC de l'AC »
Si l'attribut CN n'est pas présent, l'extension SubjectAlternativeName ou le champ OU doit débiter par la chaîne de caractère « TEST ».

Les certificats de recette seront révoqués à la fin de la période de recette.

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	13/22

III. Liste de Certificats Révoqués

III.1. Champs de base

5 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.

Une LAR est un LCR qui ne contient que des certificats d'AC.

Champ	Intitulé de l'exigence
<i>Version</i>	La valeur de ce champ doit être "1", indiquant qu'il s'agit d'une LCR version 2.
<i>Signature</i>	Cf. chapitre V ci-dessous sur les exigences en matière d'algorithmes et de longueurs de clés.
<i>Issuer</i>	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).
<i>This Update</i>	Pas d'exigence supplémentaire par rapport au [RFC5280]
<i>Next Update</i>	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] ⁵
<i>Revoked Certificates</i>	- userCertificate : pas d'exigence supplémentaire par rapport au [RFC5280] - revocationDate : pas d'exigence supplémentaire par rapport au [RFC5280] - crlEntryExtensions : cf. chapitre III.3
<i>Extensions de LCR</i>	Cf. chapitre suivant.

III.2. Extensions de LCR

10 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].

15

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)).

⁵ Exemples :

- (*) : next update = this update + 72h*2
- (**): next update = this update + 24h*2
- (***) : next update = this update + 36h

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	14/22

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.

- 5 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
<i>Authority Key Identifier</i>	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).
<i>Issuer Alternative Name</i>	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".
<i>CRL Number</i>	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 ⁶ .
<i>Delta CRL Indicator</i>	O ⁷	O ⁷	S'il s'agit d'une deltaLCR, cette extension doit obligatoirement être présente, être marquée "critique" et être conforme aux exigences du [RFC5280].
<i>Freshest CRL</i>	O ⁸	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).

10

III.3. Extensions d'entrée de LCR

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

- 15 Pour les LCR qui comportent des numéros de série correspondant à des certificats d'unité d'horodatage, il est obligatoire de supporter l'extension d'entrée LCR : reasonCode.

⁶ Ceci permet à un téléservice qui se base sur ce champ d'avoir la garantie qu'il a effectivement récupéré la CRL attendue.

⁷ Uniquement s'il s'agit d'une deltaLCR

⁸ 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.

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	15/22

IV. Protocoles d'Etat en ligne des Certificats

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

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	16/22

V. Algorithmes et longueurs de clés

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]⁹.

5 Conformément au [RFC3279], l'identifiant utilisé dans le champ "subjectPublicKeyInfo" des certificats permet de spécifier l'algorithme cryptographique correspondant à la clé certifiée¹⁰, 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.

10

¹⁰ rsaEncryption, id-dsa, id-ecPublicKey, dhpublicnumber, id-ecPublicKey.

¹⁰ rsaEncryption, id-dsa, id-ecPublicKey, dhpublicnumber, id-ecPublicKey.

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	17/22

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
[Décret2001-272]	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

5

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 3739 - 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 08/2005 (complétée par les correctifs techniques Corrigendum 1 de 01/2007, Corrigendum 2 de 11/2008)

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	18/22

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

VII.1. Identification d'une Autorité de Certification

5 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.

10 Le nom commun (attribut commonName) mentionné dans le champ « émetteur » des AC, doit identifier précisément l'AC émettrice ; il est recommandé de porter dans ce champ un libellé représentatif de l'activité de l'AC émettrice du certificat.

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.

15 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]). Un nom différent du nom officiel complet de l'entité peut être toléré si le nom utilisé est similaire au nom officiel et identifie l'entité de manière non-ambiguë.

20 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.

25 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.

30 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.

35 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

40

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	19/22

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.

- 5 Les attributs du DN doivent être encodés en printableString ou en UTF8String¹¹.

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.

- 10 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.

- 15 L'attribut organizationName doit être présent et doit contenir le nom officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes. Un nom différent du nom officiel complet de l'entité peut être toléré si le nom utilisé est similaire au nom officiel et identifie l'entité de manière non-ambiguë.

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.

- 20 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].

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

- 30 ▪ utilisation des attributs givenName et surname : l'attribut givenName doit comporter le un des prénoms 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 ou le nom d'usage 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 ;
- 35 ▪ seul l'attribut commonName est utilisé : il doit comporter un des prénoms 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 ou le nom
- 40

¹¹ 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 « @ »).

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	20/22

5 d'usage du porteur. Pour les prénoms et noms composés, le tiret est utilisé comme élément séparateur. A la suite du nom d'état civil ou du nom d'usage, 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.

Exemples de DN :

- C=FR, O= Société DEF, OU= 0002 243516879, OU= Site de Toulouse, CN= Michel Martin
- 10 ▪ 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 « Certificats électroniques de services applicatifs » ;
- 15 • un service d'authentification de serveur tel que décrit dans la PC Type « Certificats électroniques de services applicatifs ».

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] et 5.2.6 de [ETSI_CERT], ainsi qu'aux exigences supplémentaires du présent chapitre.

20 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.

25 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. Un nom différent du nom officiel complet de l'entité peut être toléré si le nom utilisé est similaire au nom officiel et identifie l'entité de manière non-ambiguë.

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

30 L'attribut commonName doit être utilisé et doit contenir un nom significatif du service applicatif, à l'exception des deux cas particuliers suivants :

- lorsqu'il s'agit d'un certificat serveur de type SSL/TLS, l'attribut commonName est facultatif. S'il est présent, il doit contenir un FQDN (Fully Qualified Domain Name) du serveur également présent dans l'extension SubjectAlternativeName. S'il est absent,
- 35 l'extension SubjectAlternativeName doit être critique ;
- lorsqu'il s'agit d'un certificat de signature de code, l'attribut commonName est facultatif. S'il est présent, il ne doit pas contenir un FQDN.

Les attributs givenName et surname ne doivent pas être utilisés.

40 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

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	21/22

Lorsqu'il s'agit d'un service de création de cachet, pour préserver l'unicité des noms, il est proposé la règle de nommage suivante pour le champ CN :

[Nom de l'organisme].[Nom du bureau responsable du serveur].[Nom du service applicatif]

Annexe A4 au RGSv2.0 : Profils de certificats / LCR / OCSP et algorithmes cryptographiques			
Version	Date	Critère de diffusion	Page
3.0	27/02/2014	PUBLIC	22/22