	NATURE DU DOCUMENT	
Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE	Document Sécurité	MINISTÈRE DE L'ACTION ET DES COMPTES PUBLICS

DOUANES & DROITS INDIRECTS

REFERENCE	DATE	VERSION
DT-FL-1703/002	1er Mars 2019	1.1

POLITIQUE DE CERTIFICATION

Profils de certificats / LCR / OCSP

et Algorithmes Cryptographiques

EMETTEUR	DESTINATAIRES	COPIES
DGDDI	PUBLIC	

Direction Générale des Douanes et Droits Indirects
Sous-Direction C - Système d'information et de télécommunication
Bureau C2 - Architecture et Réseau
11, rue des deux-communes
93558 Montreuil Cedex

Historique des versions

DATE	VERSION	EVOLUTION	AUTEUR
10/03/2017	1.0	Version initiale	Franck Leroy
01/03/2019	1.1	Suppression de l'Extended Key Usage pour les certificats de chiffrement	François Chassery

TABLE DES MATIERES

AVERTISSEMENT

La présente Politique de Certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de Certinomis. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisées préalablement par écrit par Certinomis ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'article L.122-5, d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

La Déclaration des Pratiques de Certification, propriété de la société Certinomis peut être concédée par des accords de licence à toutes entités privées ou publiques qui souhaiteraient l'utiliser dans le cadre de leurs propres services de certification.

1 INTRODUCTION

Les politiques de certification de l'AC, 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, 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.

2 PROFILS DES CERTIFICATS, OCSP ET DES LCR

Ce chapitre contient les règles et directives relatives à l'utilisation de certains types de certificats X.509, des champs, des extensions des LCR conformes aux normes PKIX.

Le contenu des certificats et des LCR, sont conformes aux exigences de la RFC 5280 : « Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile ».

2.1 PROFIL DES CERTIFICATS D'AC

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

2.1.1 Champs de base

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3.

Champ	**DGDDI**
Version	"2", indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	sha256WithRSAEncryption
Issuer	CN= Certinomis - Root CA OU=0002 433998903 O=Certinomis C=FR
Validity	10 ans
Subject	CN= DGDDI - AC AGENTS OU=0002 120023015 O=DGDDI C=FR
Subject Public Key Info	RSA 4096 bits
Unique Identifiers (issuer et subject)	Non utilisé.

2.1.2 Extensions du certificat

La criticité est défini par la colonne "C", O(ui)/N(on).

Champ	*C*	**Général**
Authority Key Identifier	N	Pour tous les certificats d'AC, autres que les certificats auto-signés, cette extension doit être présente, être marquée "non critique" et contenir l'identifiant de clé de la clé publique de l'AC émettrice (même valeur que le champ

		"Subject Key Identifier" du certificat de cette AC émettrice). Méthode 1 définie dans la RFC 5280 chapitre 4.2.1.2.
Key Usage	O	keyCertSign, CRLSign
Certificate Policies	N	anyPolicy identifier (2.5.29.32.0)
Subject Alternative Name Issuer Alternative Name	N	Non utilisée
CRL Distribution Points	N	Points de distribution vers la CRL de l'AC Racine
Authority Information Access	N	Non utilisée

2.2 PROFIL DES CERTIFICATS PORTEURS

2.2.1 Champs de base

Le tableau ci-dessous reprend l'ensemble des champs de base d'un certificat X.509v3.

Champ	**DGDDI**
Version	"2", indiquant qu'il s'agit d'un certificat version 3.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	sha256WithRSAEncryption
Issuer	CN= DGDDI - AC AGENTS OU=0002 120023015 O=DGDDI C=FR
Validity	3 ans.
Subject	Voir chapitre 7.2
Subject Public Key Info	Cf. chapitre 5 sur les exigences en matière d'algorithmes et de longueurs de clés.
Unique Identifiers (issuer et subject)	Non utilisé.

2.2.2 Extensions du certificat

La criticité est défini par la colonne "C", O(ui)/N(on).

Champ	*C*	**Signature**	**Authentification**	**Confidentialité**
Authority Key Identifier	N	Pour tous les certificats porteurs, cette extension doit être présente, être marquée "non critique" et contenir l'identifiant de clé de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice). Méthode 1 définie dans la RFC 5280 chapitre 4.2.1.2.		

Key Usage	O	nonRepudiation	digitalSignature	keyEncipherment
Certificate Policies	N	OID de la PC de l'AC émettrice		
Subject Alternative Name	N	Adresse RFC822.		
Issuer Alternative Name	N	Non utilisée		
Subject Directory Attributes	N	Non utilisée		
CRL Distribution Points	N	Points de distribution vers la CRL de l'AC émettrice.		
Authority Information Access	N	Point de distribution vers l'OCSP de l'AC émettrice		
Freshest CRL	N	Non utilisée		
Extended Key Usage Cf [RFC5280]	N	id-kp-emailProtection	id-kp-clientAuth	
Qc Compliance	N	id-etsi-qcs 1	Non utilisée	Non utilisée
QcSSCD	N	id-etsi-qcs 4	Non utilisée	Non utilisée
QcType	N	id-etsi-qct-esign	Non utilisée	Non utilisée
QcPDS	N	URL vers les CGU-EN	Non utilisée	Non utilisée

Nota : Le bit nonRepudiation est désormais nommé contentCommitment.

Lorsque le certificat électronique délivré est un certificat double usage signature électronique + authentification, les usages sont l'ensemble de ceux identifiés ci-dessus pour les usages séparés d'authentification et de signature.

2.3 PROFIL DES CERTIFICATS SERVEURS

Sans objet.

3 PROFIL DES LCR

3.1 CHAMPS DE BASE

Le tableau ci-dessous reprend l'ensemble des champs de base d'une LCR X.509v2.

Champ	**DGDDI**
Version	"1", indiquant qu'il s'agit d'un certificat version 2.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	sha256WithRSAEncryption
Issuer	CN= DGDDI - AC AGENTS OU=0002 120023015 O=DGDDI C=FR
This Update	date d'émission de cette LCR.
Next Update	date limite d'émission de la prochaine LCR.
Revoked Certificates	- userCertificate : numéro de série unique du certificat révoqué - revocationDate : date de la révocation - crlEntryExtensions : non utilisé

3.2 EXTENSIONS DE LCR

La criticité est défini par la colonne "C", O(ui)/N(on).

Champ	*C*	**Général**
Authority Key Identifier	N	Cette extension doit être présente, être marquée "non critique" et contenir l'identifiant de clé de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice). Méthode 1 définie dans la RFC 5280 chapitre 4.2.1.2.
Issuer Alternative Name	N	Non utilisée
CRL Number	N	Numéro incrémental de la CRL.
Delta CRL Indicator	O	Non utilisée
Freshest CRL	N	Non utilisée

3.3 EXTENSIONS D'ENTREE DE LCR

La criticité est défini par la colonne "C", O(ui)/N(on).

Champ	*C*	**Général**
Reason Code	N	Non utilisée

Invalidity Date	N	Date de prise en compte de la révocation par l'AC.
Certificate Issuer	N	Non utilisée

4 PROTOCOLES D'ETAT EN LIGNE DES CERTIFICATS

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

4.1.1 Numéro de version

Sans objet.

4.1.2 Extensions OCSP

Sans objet.

5 ALGORITHMES ET LONGUEURS DE CLES

5.1 OID DES ALGORITHMES

Les identifiants d'algorithmes correspondant à utiliser dans le champ "signature" des certificats (cf. chapitres II.1.1 et II.2.1) sont définis dans [RFC3279] et [PKCS#1] :

- sha256WithRSAEncryption : Utilisation de l'algorithme RSA avec la fonction de hachage SHA-2 256 bits.

5.2 LONGUEURS DE CLES

5.2.1 Clés d'AC

Les bi-clés d'une AC dont la durée de validité est supérieure ou égale à 10 ans sont d'une complexité au moins équivalente à 4096 bits pour l'algorithme RSA.

Les bi-clés AC d'une complexité inférieure à 4096 bits pour l'algorithme RSA, ne sont pas supportées par cette PC.

5.2.2 Clés des bénéficiaires

Général
Taille des clés
Les bi-clés des certificats émis sont d'une complexité au moins équivalente à 2048 bits pour l'algorithme RSA et P-256 pour l'algorithme ECDSA-GF(P).

5.3 VALIDITE DE CLES

La validité de la clé privée veut dire la période pendant laquelle elle peut être utilisée pour une opération cryptographique.

Une fois l'opération cryptographique réalisée, cette opération est vérifiable pendant la validité de la clé publique.

Par exemple, pour une clé privée valable 3 ans et une clé publique valable 10 ans, si un document est signé pendant la période des 3 ans et vérifié pendant la période des 10 ans, le document est valable (la vérification de la révocation doit elle aussi être effectuée).

5.3.1 Clés privées

La durée de vie de la clé privée est celle portée par le certificat.

5.3.2 Clés publiques

La durée de vie de la clé publique est liée à la taille de la clé.

5.3.2.1 Clés RSA :

Les clés RSA de moins de 2048 bits ne sont pas supportées, ni garanties par cette PC.

La période de validité des clés RSA 2048 bits est d'au plus dix (10) ans.

La période de validité des clés RSA 4096 bits est d'au plus vingt (20) ans.

5.3.2.2 Clés ECDSA-GF(p) ;

L'emploi des courbes autre que P-256, P-384 et P-521, n'est pas supporté, ni garantie par cette PC.

La période de validité des clés issues des courbes P-256, P-384 et P-521 est d'au plus vingt (20) ans.

6 ANNEXE 1 - DOCUMENTS DE REFERENCE

6.1 REGLEMENTATION

Renvoi	Document
[ORDONNANCE]	*Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électronique entre les usagers et les autorités administratives et entre les autorités administratives*
[DécretRGS]	*Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005.*
[SIG]	*Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.*

6.2 DOCUMENTS TECHNIQUES

Renvoi	Document
[RGS2]	Référentiel Général de Sécurité – version 3.0
[EN_CERT_N]	EN 319 412-2 v2.1.1, février 2016, Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[EN_CERT_L]	EN 319 412-3 v1.1.1, février 2016, Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[EN_CERT_W]	EN 319 412-4 v1.1.1, février 2016, Certificate Profiles; Part 4: Certificate profile for web site certificates
[EN_CERT_QC]	EN 319 412-5 v2.1.1, février 2016 Certificate Profiles; Part 5: QCStatements
[PKCS#1]	RSA Laboratories - PKCS #1 v2.1 - RSA Cryptography Standard, 14 juin 2002 1
[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: Publickey 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)

7 ANNEXE 2 - EXIGENCES SUR LES IDENTIFIANTS D'AC, DE PORTEURS ET DE SERVEURS

7.1 IDENTIFICATION DE L'AUTORITE DE CERTIFICATION

7.1.1 Forme des noms

EASY
DN de l'AC
C=FR, O= DGDDI, OU=0002 120023015, CN= DGDDI - AC AGENTS

Ce DN est encodé en printableString.

7.1.2 Contraintes sur les noms

Sans objet.

7.1.3 Utilisation de l'extension "contraintes de politique"

Sans objet.

7.1.4 Sémantique et syntaxe des qualifiants de politique

Sans objet.

7.1.5 Sémantiques de traitement des extensions critiques de la PC

Sans objet.

7.2 IDENTIFICATION DE PORTEUR

7.2.1 Forme des noms

Certificat d'organisation
DN des certificats émis
SNU = « n° unique » SN = « Nom de famille » GN = « Prénom » CN= « Identité » T = « Texte libre » OU= « Identifiant d'Organisation SIREN » OrgID= « Identifiant d'Organisation NTRFR» O= « Raison sociale » C= « Pays »

Ce DN est encodé en printableString ou en UTF8String.

7.2.2 Contraintes sur les noms

Certificat d'organisation
Contraintes sur les noms
• Le SNU est calculé par l'Autorité de façon à assurer l'unicité du bénéficiaire • Le CN doit contenir le « Prénom Nom » du bénéficiaire • Le SN peut contenir le « Nom » du bénéficiaire • Le GN peut contenir le « Prénom » du bénéficiaire • Le T peut contenir la fonction du bénéficiaire • Le OrgID est destiné à recevoir l'identifiant de l'organisation du bénéficiaire. • Le OU est destiné à recevoir l'identifiant de l'organisation du bénéficiaire. • Le O contient la raison sociale de l'organisation du bénéficiaire • Le C contient le pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère, …). L'attribut organizationName contient le nom officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes. L'attribut organizationIdentifier contient l'identification de cette entité de la forme : • NTRFR, • L'identification de l'organisation sur 9 caractères, • Le séparateur entre les deux chaînes est un tiret. L'attribut organizationalUnitName est structuré conformément à la norme ISO 6523. Le format 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, l'identification doit être le n° SIREN ou le n° SIRET (l'ICD du numéro SIREN / SIRET est 0002, suivi d'un espace et de 9 caractères pour le n° SIREN et de 14 caractères pour le n° SIRET). Le commonName comporte le premier prénom de l'état civil du bénéficiaire (si la pièce d'identité présentée pour l'enregistrement comporte d'autres prénoms, ils peuvent être mentionnés dans le certificat dans le même ordre que sur la pièce d'identité), suivi d'un espace, suivi du nom de l'état civil du bénéficiaire. Pour les prénoms et noms composés, le tiret est utilisé comme élément séparateur. L'attribut serialNumber est présent dans les certificats, pour traiter les cas d'homonymie (cf. [RFC3739] et §suivant).

7.2.3 Utilisation de l'extension "contraintes de politique"

Sans objet.

7.2.4 Sémantique et syntaxe des qualifiants de politique

Sans objet.

7.2.5 Sémantiques de traitement des extensions critiques de la PC

Sans objet.

7.3 IDENTIFICATION D'UN SERVICE APPLICATIF

Sans objet.