

POLITIQUE DE CERTIFICATION					
Profils des Certificats, Listes de Certificats Révoqués, OCSP Algorithmes Cryptographiques					
EMETTEUR		DESTINATAIRES		COPIES	
CERTINOMIS		PUBLIC			
Certinomis					
<p>Docaposte Certinomis SAS au capital de 40 156 euros.</p> <p>Siège social : 45-47 Boulevard Paul Vaillant-Couturier</p> <p>94200 Ivry sur Seine – France. RCS Créteil B 433 998 903</p>					
Historique des versions					
DATE	VERSION	EVOLUTION	AUTEUR		
03/09/2021	1.0	Validation version publique	F. CHASSERY		
26/10/2022	1.1	Modification Key Usage §2.8.1 & §2.8.7	P. SALENDRES		
25/11/2022	1.2	Ajout AC Signature Contralia	P. SALENDRES		
20/03/2023	1.3	Modification de la raison sociale	P. SALENDRES		
20/06/2024	1.4	<p>Ajout de la description des certificats émis par l'AC FLASH sous l'OID 1.2.250.1.86.2.6.10.2.2 au §2.6.2</p> <p>Complément pour l'AC Signature Contralia aux paragraphes 2.1.1.2 et 2.1.1.3</p> <p>Mise à jour du paragraphe 4.2 pour indiquer la durée de vie des certificats "éphémères"</p> <p>Ajout de l'email dans le champ SAN pour l'OID 1.2.250.1.86.2.6.1.10.1 au paragraphe 2.4.4</p> <p>Ajout des gabarits de certificat de l'AC Flash G2</p> <p>Suppression de l'OID spécifique 0.4.0.194112.1.2</p>	Y. THOMASSIER		
23/09/2024	1.5	<p>Corrections apportées suite à l'audit interne</p> <p>Modification des paragraphes 4.1.2 et 4.2 concernant la durée de validité des bi-clés RSA 2048 bits.</p> <p>Ajout des OID 1.2.250.1.86.2.6.7.23.1 et 1.2.250.1.86.2.6.8.23.1</p>	Y. THOMASSIER		

Table des matières

1	INTRODUCTION.....	6
2	PROFILS DES CERTIFICATS.....	7
	2.1 Profil des certificats d'AC.....	7
2.1.1	Champs de base.....	7
	Extensions du certificat.....	8
	2.2 Caractéristiques communes des certificats émis.....	9
2.2.1	Champs de base.....	9
	2.3 AC AA-AGENTS.....	9
2.3.1	OID 1.2.250.1.86.2.3.7.1.1.....	9
2.3.2	OID 1.2.250.1.86.2.3.7.2.1.....	10
2.3.3	OID 1.2.250.1.86.2.3.7.3.1.....	10
2.3.4	OID 1.2.250.1.86.2.3.7.10.1.....	10
2.3.5	OID 1.2.250.1.86.2.3.7.20.1.....	11
2.3.6	OID 1.2.250.1.86.2.3.7.22.1.....	11
2.3.7	OID 1.2.250.1.86.2.3.7.23.1.....	12
2.3.8	OID 1.2.250.1.86.2.3.8.1.1.....	12
2.3.9	OID 1.2.250.1.86.2.3.8.2.1.....	13
2.3.10	OID 1.2.250.1.86.2.3.8.3.1.....	13
2.3.11	OID 1.2.250.1.86.2.3.8.10.1.....	14
2.3.12	OID 1.2.250.1.86.2.3.8.20.1.....	14
2.3.13	OID 1.2.250.1.86.2.3.8.22.1.....	15
2.3.14	OID 1.2.250.1.86.2.3.8.23.1.....	15
	2.4 AC EASY G2.....	16
2.4.1	OID 1.2.250.1.86.2.6.1.1.1.....	16
2.4.2	OID 1.2.250.1.86.2.6.1.2.1.....	16
2.4.3	OID 1.2.250.1.86.2.6.1.3.1.....	17
2.4.4	OID 1.2.250.1.86.2.6.1.10.1.....	17
2.4.5	OID 1.2.250.1.86.2.6.1.22.1.....	18
2.4.6	OID 1.2.250.1.86.2.6.1.26.1.....	19
	2.5 AC EASY.....	19
2.5.1	OID 1.2.250.1.86.2.3.1.1.1.....	19
2.5.2	OID 1.2.250.1.86.2.3.1.2.1.....	20
2.5.3	OID 1.2.250.1.86.2.3.1.3.1.....	20
2.5.4	OID 1.2.250.1.86.2.3.1.10.1.....	21
2.5.5	OID 1.2.250.1.86.2.3.1.20.1.....	21
2.5.6	OID 1.2.250.1.86.2.3.1.22.1.....	22
2.5.7	OID 1.2.250.1.86.2.3.1.23.1.....	22
2.5.8	OID 1.2.250.1.86.2.3.4.1.1.....	23
2.5.9	OID 1.2.250.1.86.2.3.4.2.1.....	23
2.5.10	OID 1.2.250.1.86.2.3.4.3.1.....	23
2.5.11	OID 1.2.250.1.86.2.3.4.10.1.....	24
	2.6 AC FLASH.....	24
2.6.1	OID 1.2.250.1.86.2.6.10.2.1.....	24
2.6.2	OID 1.2.250.1.86.2.6.10.2.2.....	26
	2.7 AC FLASH G2.....	26
2.7.1	OID 1.2.250.1.86.2.6.14.2.1 (AE Id Claim Signature Particulier).....	26
2.7.2	OID 1.2.250.1.86.2.6.14.2.2 (AE BPCE Signature Particulier).....	27
2.7.3	OID 1.2.250.1.86.2.6.15.2.2 (AE BPCE Signature Pro).....	27
	2.8 AC ONCE.....	28
2.8.1	OID 1.2.250.1.86.2.6.11.2.1.....	28
2.8.2	OID 1.2.250.1.86.2.6.11.2.2.....	28
2.8.3	OID 1.2.250.1.86.2.6.12.2.1.....	29

2.8.4	OID 1.2.250.1.86.2.6.12.2.2	29
2.9	AC PRIME G2	30
2.9.1	OID 1.2.250.1.86.2.6.3.25.1	30
2.9.2	OID 1.2.250.1.86.2.6.6.30.1	30
2.9.3	OID 1.2.250.1.86.2.6.3.1.1	31
2.9.4	OID 1.2.250.1.86.2.6.3.2.1	31
2.9.5	OID 1.2.250.1.86.2.6.3.3.1	32
2.9.6	OID 1.2.250.1.86.2.6.3.10.1	32
2.9.7	OID 1.2.250.1.86.2.6.3.22.1	33
2.9.8	OID 1.2.250.1.86.2.6.3.30.1	34
2.9.9	OID 1.2.250.1.86.2.6.3.40.1	34
2.9.10	OID 1.2.250.1.86.2.6.6.1.1	35
2.9.11	OID 1.2.250.1.86.2.6.6.2.1	35
2.9.12	OID 1.2.250.1.86.2.6.6.10.1	36
2.9.13	OID 1.2.250.1.86.2.6.6.40.1	36
2.10	AC PRIME	37
2.10.1	OID 1.2.250.1.86.2.3.3.1.1	37
2.10.2	OID 1.2.250.1.86.2.3.3.2.1	37
2.10.3	OID 1.2.250.1.86.2.3.3.10.1	38
2.10.4	OID 1.2.250.1.86.2.3.3.20.1	39
2.10.5	OID 1.2.250.1.86.2.3.3.22.1	39
2.10.6	OID 1.2.250.1.86.2.3.3.23.1	40
2.10.7	OID 1.2.250.1.86.2.3.3.24.1	40
2.10.8	OID 1.2.250.1.86.2.3.3.30.1	41
2.10.9	OID 1.2.250.1.86.2.3.6.1.1	41
2.10.10	OID 1.2.250.1.86.2.3.6.2.1	42
2.10.11	OID 1.2.250.1.86.2.3.6.10.1	42
2.10.12	OID 1.2.250.1.86.2.3.6.30.1	43
2.11	AC SAFE	43
2.11.1	OID 1.2.250.1.86.2.6.6.20.1	43
2.11.2	OID 1.2.250.1.86.2.6.6.23.1	44
2.12	AC STANDARD G2	44
2.12.1	OID 1.2.250.1.86.2.6.2.1.1	44
2.12.2	OID 1.2.250.1.86.2.6.2.2.1	45
2.12.3	OID 1.2.250.1.86.2.6.2.10.1	45
2.12.4	OID 1.2.250.1.86.2.6.2.22.1	46
2.12.5	OID 1.2.250.1.86.2.6.2.30.1	46
2.13	AC STANDARD	47
2.13.1	OID 1.2.250.1.86.2.3.2.22.1	47
2.13.2	OID 1.2.250.1.86.2.3.2.30.1	47
2.13.3	OID 1.2.250.1.86.2.3.5.30.1	48
2.14	AC TIMESTAMP	48
2.14.1	OID 1.2.250.1.86.2.6.5.24.1	48
2.15	AC WEB	49
2.15.1	OID 1.2.250.1.86.2.6.4.20.1	49
2.15.2	OID 1.2.250.1.86.2.6.4.23.1	49
2.15.3	OID 1.2.250.1.86.2.6.4.60.1	50
2.15.4	OID 1.2.250.1.86.2.6.4.61.1	50
2.16	AC Signature Contralia	51
2.16.1	OID 1.2.250.1.86.2.6.9.34.1	51
3	Profil des LCR	52
3.1	Champ de base	52
3.2	Extensions de LCR	52
3.3	Extensions d'entrée de LCR	52
4	Algorithmes et longueurs de clés	53

4.1 Longueurs de clés	53
4.1.1 Clés d'AC	53
4.1.2 Clés des bénéficiaires	53
4.2 Validité des clés	53
4.2.1 Clés privées	53
4.2.2 Clés publiques	53
5 Annexe – Exigences sur les identifiants de porteurs et de serveurs	55
5.1 Forme des noms des porteurs	55
5.1.1 Certificat d'organisation	55
5.1.2 Certificat de particulier	55
5.2 Forme des noms des services applicatifs	56
5.2.1 Certificat de serveur	56

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 Certinomis, 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

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 demachines, 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.

2.1.1.1 Champs communs à toutes les AC

Champ	Contenu
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	Voir 2.1.1.2
Subject	CN={ CN de l'AC (voir 2.1.1.2) } OU=0002 433998903 (voir ci-dessous) O=Certinomis C=FR
Subject Public Key Info	RSA 4096 bits
Unique Identifiers (issuer et subject)	Non utilisé.

Le DN du sujet (*subject*) contient un attribut OU dans le cas des AC : EASY, PRIME, STANDARD, AA-AGENTS.

Le DN du sujet (*subject*) contient un attribut OI dans le cas des AC : EASY G2, PRIME G2, STANDARD G2, FLASH, ONCE, SAFE, TIMESTAMP, WEB.

2.1.1.2 CN et durée de vie des AC

Le préfixe commun des CN est constitué du nom « Certinomis », suivi d'un espace (U+0020), d'un trait d'union (U+002d) et d'un espace (U+0020).

AC	Common Name	Durée de vie
AA-AGENTS	Certinomis - AA et AGENTS	10 ans
AC SIGNATURE CONTRALIA	AC Signature Contralia	10 ans
EASY	Certinomis - Easy CA	10 ans
EASY G2	Certinomis - Easy CA G2	16 ans
FLASH	Certinomis - Flash CA	15 ans
ONCE	Certinomis - Once CA	15 ans

AC	Common Name	Durée de vie
PRIME	Certinomis - Prime CA	10 ans
PRIME G2	Certinomis - Prime CA G2	16 ans
SAFE	Certinomis - Safe CA	16 ans
STANDARD	Certinomis - Standard CA	10 ans
STANDARD G2	Certinomis - Standard CA G2	16 ans
TIMESTAMP	Certinomis - Timestamp CA	16 ans
WEB	Certinomis - Web CA	16 ans

Extensions du certificat

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

Champ	C	Général
<i>Authority Key Identifier</i>	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.
<i>Subject Key Identifier</i>	N	Identifiant de la clé du sujet (AC)
<i>Key Usage</i>	O	keyCertSign, CRLSign
<i>Basic Constraints</i>	O	CA:TRUE
<i>Certificate Policies</i>	N	anyPolicy identifier (2.5.29.32.0)
<i>Subject Alternative Name</i> <i>Issuer Alternative Name</i>	N	Non utilisée
<i>CRL Distribution Points</i>	N	Points de distribution vers la CRL de l'AC Racine
<i>Authority Information Access</i>	N	Non utilisée pour les AC : EASY, PRIME, STANDARD, AA-AGENTS. Pour les autres AC, contient : CA Issuers - URI: https://www.certinomis.fr/publi/cer/AC_Racine_G3.cer

2.1.1.3 Extended Key Usage des AC

AC	Extended Key Usage
AA-AGENTS	Non utilisée
AC SIGNATURE CONTRALIA	<i>E-mail Protection, OCSP Signing</i>
EASY	Non utilisée
EASY G2	<i>TLS Web Client Authentication, E-mail Protection, OCSP Signing</i>
FLASH	<i>E-mail Protection, OCSP Signing</i>
ONCE	<i>E-mail Protection, OCSP Signing</i>
PRIME	Non utilisée
PRIME G2	<i>TLS Web Client Authentication, E-mail Protection, OCSP Signing</i>
SAFE	<i>TLS Web Client Authentication, TLS Web Server Authentication, OCSP Signing</i>

AC	Extended Key Usage
STANDARD	Non utilisée
STANDARD G2	TLS Web Client Authentication, E-mail Protection, OCSP Signing
TIMESTAMP	Timestamping, OCSP Signing
WEB	TLS Web Client Authentication, TLS Web Server Authentication, OCSP Signing

2.2 CARACTERISTIQUES COMMUNES DES CERTIFICATS ÉMIS

2.2.1 Champs de base

Champ	Contenu
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	DN de l'AC émettrice
Validity	3 ans à 5 ans en fonction du profil.
Subject	Voir chapitre 5.
Subject Public Key Info	Voir chapitre 4.
Unique Identifiers (issuer et subject)	Non utilisé.

2.3 AC AA-AGENTS

2.3.1 OID 1.2.250.1.86.2.3.7.1.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.3.2 OID 1.2.250.1.86.2.3.7.2.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.3.3 OID 1.2.250.1.86.2.3.7.3.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	keyEncipherment
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.3.4 OID 1.2.250.1.86.2.3.7.10.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)

Champ	C	Contenu/Présent/Absent
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth, emailProtection
Qc Compliance	N	Non utilisée

2.3.5 OID 1.2.250.1.86.2.3.7.20.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, keyEncipherment
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	(présent)
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsServerAuth
Qc Compliance	N	Non utilisée
ct_precert_scts (1.3.6.1.4.1.11129.2.4.2)	N	Défini dans la RFC 6962, section 3.2.

2.3.6 OID 1.2.250.1.86.2.3.7.22.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false

Champ	C	Contenu/Présent/Absent
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.3.7 OID 1.2.250.1.86.2.3.7.23.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.3.8 OID 1.2.250.1.86.2.3.8.1.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)

Champ	C	Contenu/Présent/Absent
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	tlsClientAuth
<i>Qc Compliance</i>	N	Non utilisée

2.3.9 OID 1.2.250.1.86.2.3.8.2.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	emailProtection
<i>Qc Compliance</i>	N	(présent)
<i>QcSSCD</i>	N	(présent)
<i>QcType</i>	N	id-etsi-qct-esign(1)
<i>QcPDS</i>	N	URL vers les CGU-EN

2.3.10 OID 1.2.250.1.86.2.3.8.3.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	keyEncipherment
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)

Champ	C	Contenu/Présent/Absent
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	emailProtection
<i>Qc Compliance</i>	N	Non utilisée

2.3.11 OID 1.2.250.1.86.2.3.8.10.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	DigitalSignature, nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	tlsClientAuth, emailProtection
<i>Qc Compliance</i>	N	(présent)
<i>QcSSCD</i>	N	(présent)
<i>QcType</i>	N	id-etsi-qct-esign(1)
<i>QcPDS</i>	N	URL vers les CGU-EN

2.3.12 OID 1.2.250.1.86.2.3.8.20.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	DigitalSignature, keyEncipherment
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)

Champ	C	Contenu/Présent/Absent
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	(présent)
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	tlsServerAuth
<i>Qc Compliance</i>	N	(présent)
<i>QcSSCD</i>	N	Non utilisée
<i>QcType</i>	N	id-etsi-qct-web(3)
<i>QcPDS</i>	N	URL vers les CGU-EN

2.3.13 OID 1.2.250.1.86.2.3.8.22.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	DigitalSignature
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	emailProtection
<i>Qc Compliance</i>	N	Non utilisée

2.3.14 OID 1.2.250.1.86.2.3.8.23.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	DigitalSignature, nonRepudiation

Champ	C	Contenu/Présent/Absent
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	tlsClientAuth, emailProtection
<i>Qc Compliance</i>	N	(présent)
<i>QcSSCD</i>	N	(présent)
<i>QcType</i>	N	id-etsi-qct-esign(1)
<i>QcPDS</i>	N	URL vers les CGU-EN

2.4 AC EASY G2

2.4.1 OID 1.2.250.1.86.2.6.1.1.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	DigitalSignature
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.2042.1.3
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	tlsClientAuth
<i>Qc Compliance</i>	N	Non utilisée

2.4.2 OID 1.2.250.1.86.2.6.1.2.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)

Champ	C	Contenu/Présent/Absent
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.2042.1.3
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.4.3 OID 1.2.250.1.86.2.6.1.3.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	keyEncipherment, dataEncipherment
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.2042.1.3
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.4.4 OID 1.2.250.1.86.2.6.1.10.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation

Champ	C	Contenu/Présent/Absent
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.2042.1.3
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Adresse mail du bénéficiaire si fourni
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth, emailProtection
Qc Compliance	N	Non utilisée

2.4.5 OID 1.2.250.1.86.2.6.1.22.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.2042.1.3
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.4.6 OID 1.2.250.1.86.2.6.1.23.1

Champ	C	Contenu/Présent/Absent
Authority Key Identifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
Certificate Policies (OID de la PC de l'AC émettrice)	N	(présent)
Certificate Policies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée

Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer Alternative Name	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL Distribution Points	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended Key Usage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.4.7 OID 1.2.250.1.86.2.6.1.26.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, keyEncipherment
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.2042.1.3
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.5 AC EASY

2.5.1 OID 1.2.250.1.86.2.3.1.1.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée

Champ	C	Contenu/Présent/Absent
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	tlsClientAuth
<i>Qc Compliance</i>	N	Non utilisée

2.5.2 OID 1.2.250.1.86.2.3.1.2.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	emailProtection
<i>Qc Compliance</i>	N	Non utilisée

2.5.3 OID 1.2.250.1.86.2.3.1.3.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	keyEncipherment
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)

Champ	C	Contenu/Présent/Absent
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.5.4 OID 1.2.250.1.86.2.3.1.10.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth, emailProtection
Qc Compliance	N	Non utilisée

2.5.5 OID 1.2.250.1.86.2.3.1.20.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, keyEncipherment
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	(présent)
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée

Champ	C	Contenu/Présent/Absent
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	tlsServerAuth
<i>Qc Compliance</i>	N	Non utilisée

2.5.6 OID 1.2.250.1.86.2.3.1.22.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	DigitalSignature
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access</i> (CA Issuer)	N	(présent)
<i>Authority Information Access</i> (OCSP)	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	emailProtection
<i>Qc Compliance</i>	N	Non utilisée

2.5.7 OID 1.2.250.1.86.2.3.1.23.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	DigitalSignature
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access</i> (CA Issuer)	N	(présent)
<i>Authority Information Access</i> (OCSP)	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	tlsClientAuth
<i>Qc Compliance</i>	N	Non utilisée

2.5.8 OID 1.2.250.1.86.2.3.4.1.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.5.9 OID 1.2.250.1.86.2.3.4.2.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.5.10 OID 1.2.250.1.86.2.3.4.3.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)

Champ	C	Contenu/Présent/Absent
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	keyEncipherment
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.5.11 OID 1.2.250.1.86.2.3.4.10.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth, emailProtection
Qc Compliance	N	Non utilisée

2.6 AC FLASH

2.6.1 OID 1.2.250.1.86.2.6.10.2.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)

Champ	C	Contenu/Présent/Absent
<i>Basic Constraints</i>	O	False
<i>Key Usage</i>	O	nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access</i> (CA Issuer)	N	(présent)
<i>Authority Information Access</i> (OCSP)	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	Non utilisée
<i>Qc Compliance</i>	N	Non utilisée

2.6.2 OID 1.2.250.1.86.2.6.10.2.2

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	False
<i>Key Usage</i>	O	nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access</i> (CA Issuer)	N	(présent)
<i>Authority Information Access</i> (OCSP)	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	Non utilisée
<i>Qc Compliance</i>	N	Non utilisée

2.7 AC FLASH G2

2.7.1 OID 1.2.250.1.86.2.6.14.2.1 (AE Id Claim Signature Particulier)

Champ	C	Contenu/Présent/Absent
<i>Authority Key Identifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	False
<i>Key Usage</i>	O	nonRepudiation
<i>Certificate Policies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>Certificate Policies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer Alternative Name</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL Distribution Points</i>	N	(présent)
<i>Authority Information Access</i> (CA Issuer)	N	(présent)
<i>Authority Information Access</i> (OCSP)	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended Key Usage</i> Cf [RFC5280]	N	Non utilisée
<i>Qc Compliance</i>	N	Non utilisée

2.7.2 OID 1.2.250.1.86.2.6.14.2.2 (AE BPCE Signature Particulier)

Champ	C	Contenu/Présent/Absent
Authority Key Identifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	False
Key Usage	O	nonRepudiation
Certificate Policies (OID de la PC de l'AC émettrice)	N	(présent)
Certificate Policies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer Alternative Name	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL Distribution Points	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended Key Usage Cf [RFC5280]	N	Non utilisée
Qc Compliance	N	Non utilisée

2.7.3 OID 1.2.250.1.86.2.6.15.2.2 (AE BPCE Signature Pro)

Champ	C	Contenu/Présent/Absent
Authority Key Identifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	False
Key Usage	O	nonRepudiation
Certificate Policies (OID de la PC de l'AC émettrice)	N	(présent)
Certificate Policies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer Alternative Name	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL Distribution Points	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended Key Usage Cf [RFC5280]	N	Non utilisée
Qc Compliance	N	Non utilisée

2.8 AC ONCE

2.8.1 OID 1.2.250.1.86.2.6.11.2.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	False
<i>Key Usage</i>	O	nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access</i> (CA Issuer)	N	(présent)
<i>Authority Information Access</i> (OCSP)	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	Non utilisée
<i>Qc Compliance</i>	N	Non utilisée

2.8.2 OID 1.2.250.1.86.2.6.11.2.2

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access</i> (CA Issuer)	N	(présent)
<i>Authority Information Access</i> (OCSP)	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	Non utilisée
<i>Qc Compliance</i>	N	Non utilisée

2.8.3 OID 1.2.250.1.86.2.6.12.2.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access</i> (CA Issuer)	N	(présent)
<i>Authority Information Access</i> (OCSP)	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	Non utilisée
<i>Qc Compliance</i>	N	Non utilisée

2.8.4 OID 1.2.250.1.86.2.6.12.2.2

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access</i> (CA Issuer)	N	(présent)
<i>Authority Information Access</i> (OCSP)	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	Non utilisée
<i>Qc Compliance</i>	N	Non utilisée

2.9 AC PRIME G2

2.9.1 OID 1.2.250.1.86.2.6.3.25.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-eseal(2)
QcPDS	N	URL vers les CGU-EN

2.9.2 OID 1.2.250.1.86.2.6.6.30.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	(présent)

Champ	C	Contenu/Présent/Absent
QcSSCD	N	Non utilisée
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.9.3 OID 1.2.250.1.86.2.6.3.1.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.9.4 OID 1.2.250.1.86.2.6.3.2.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	(présent)

Champ	C	Contenu/Présent/Absent
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.9.5 OID 1.2.250.1.86.2.6.3.3.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	keyEncipherment
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.2042.1.2
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.9.6 OID 1.2.250.1.86.2.6.3.10.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.194112.1.2
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth, emailProtection

Champ	C	Contenu/Présent/Absent
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.9.7 OID 1.2.250.1.86.2.6.3.22.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.194112.1.1
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-eseal(2)
QcPDS	N	URL vers les CGU-EN

2.9.8 1.2.250.1.86.2.6.3.23.1

Champ	C	Contenu/Présent/Absent
Authority Key Identifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
Certificate Policies (OID de la PC de l'AC émettrice)	N	(présent)
Certificate Policies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisé
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer Alternative Name	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL Distribution Points	N	(présent)

Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended Key Usage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.9.9 OID 1.2.250.1.86.2.6.3.30.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.194112.1.0
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	Non utilisée
Qc Compliance	N	(présent)
QcSSCD	N	Non utilisée
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.9.10 OID 1.2.250.1.86.2.6.3.40.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.194112.1.2
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)

Champ	C	Contenu/Présent/Absent
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.9.11 OID 1.2.250.1.86.2.6.6.1.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.2042.1.2
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.9.12 OID 1.2.250.1.86.2.6.6.2.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.194112.1.2
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)

Champ	C	Contenu/Présent/Absent
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.9.13 OID 1.2.250.1.86.2.6.6.10.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.194112.1.2
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth, emailProtection
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.9.14 OID 1.2.250.1.86.2.6.6.40.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.194112.1.2
CertificatePolicies (Point de distribution (CPS))	N	(présent)

Champ	C	Contenu/Présent/Absent
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.10AC PRIME

2.10.1 OID 1.2.250.1.86.2.3.3.1.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.10.2 OID 1.2.250.1.86.2.3.3.2.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation

Champ	C	Contenu/Présent/Absent
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	emailProtection
<i>Qc Compliance</i>	N	(présent)
<i>QcSSCD</i>	N	(présent)
<i>QcType</i>	N	id-etsi-qct-esign(1)
<i>QcPDS</i>	N	URL vers les CGU-EN

2.10.3 OID 1.2.250.1.86.2.3.3.10.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	DigitalSignature, nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> Cf [RFC5280]	N	tlsClientAuth, emailProtection
<i>Qc Compliance</i>	N	(présent)
<i>QcSSCD</i>	N	(présent)
<i>QcType</i>	N	id-etsi-qct-esign(1)
<i>QcPDS</i>	N	URL vers les CGU-EN

2.10.4 OID 1.2.250.1.86.2.3.3.20.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, keyEncipherment
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	(présent)
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsServerAuth
Qc Compliance	N	(présent)
QcSSCD	N	Non utilisée
QcType	N	id-etsi-qct-web(3)
QcPDS	N	URL vers les CGU-EN

2.10.5 OID 1.2.250.1.86.2.3.3.22.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	(présent)
QcSSCD	N	Non utilisée
QcType	N	id-etsi-qct-seal(2)

Champ	C	Contenu/Présent/Absent
QcPDS	N	URL vers les CGU-EN

2.10.6 OID 1.2.250.1.86.2.3.3.23.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.10.7 OID 1.2.250.1.86.2.3.3.24.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	O	timeStamping
Qc Compliance	N	(présent)
QcSSCD	N	Non utilisée
QcType	N	id-etsi-qct-seal(2)

Champ	C	Contenu/Présent/Absent
QcPDS	N	URL vers les CGU-EN

2.10.8 OID 1.2.250.1.86.2.3.3.30.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.10.9 OID 1.2.250.1.86.2.3.6.1.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth

Champ	C	Contenu/Présent/Absent
Qc Compliance	N	Non utilisée

2.10.10 OID 1.2.250.1.86.2.3.6.2.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.10.11 OID 1.2.250.1.86.2.3.6.10.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth, emailProtection

Champ	C	Contenu/Présent/Absent
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.10.12 OID 1.2.250.1.86.2.3.6.30.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.11AC SAFE

2.11.1 OID 1.2.250.1.86.2.6.6.20.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, keyEncipherment
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	(présent)
Issuer AlternativeName	N	Non utilisée

Champ	C	Contenu/Présent/Absent
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsServerAuth
Qc Compliance	N	(présent)
QcSSCD	N	Non utilisée
QcType	N	id-etsi-qct-web(3)
QcPDS	N	URL vers les CGU-EN

2.11.2 OID 1.2.250.1.86.2.6.6.23.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.12AC STANDARD G2

2.12.1 OID 1.2.250.1.86.2.6.2.1.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)

Champ	C	Contenu/Présent/Absent
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.12.2 OID 1.2.250.1.86.2.6.2.2.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.12.3 OID 1.2.250.1.86.2.6.2.10.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée

Champ	C	Contenu/Présent/Absent
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	tlsClientAuth, emailProtection
<i>Qc Compliance</i>	N	Non utilisée

2.12.4 OID 1.2.250.1.86.2.6.2.22.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	DigitalSignature
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	emailProtection
<i>Qc Compliance</i>	N	Non utilisée

2.12.5 OID 1.2.250.1.86.2.6.2.30.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access (CA Issuer)</i>	N	(présent)
<i>Authority Information Access (OCSP)</i>	N	(présent)

Champ	C	Contenu/Présent/Absent
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	Non utilisée
Qc Compliance	N	Non utilisée

2.13AC STANDARD

2.13.1 OID 1.2.250.1.86.2.3.2.22.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.13.2 OID 1.2.250.1.86.2.3.2.30.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée

Champ	C	Contenu/Présent/Absent
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.13.3 OID 1.2.250.1.86.2.3.5.30.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	nonRepudiation
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : email)	N	(présent)
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	emailProtection
Qc Compliance	N	Non utilisée

2.14AC TIMESTAMP

2.14.1 OID 1.2.250.1.86.2.6.5.24.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	Non utilisée
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée

Champ	C	Contenu/Présent/Absent
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	timeStamping
<i>Qc Compliance</i>	N	(présent)
<i>QcSSCD</i>	N	Non utilisée
<i>QcType</i>	N	id-etsi-qct-eseal(2)
<i>QcPDS</i>	N	URL vers les CGU-EN

2.15AC WEB

2.15.1 OID 1.2.250.1.86.2.6.4.20.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	DigitalSignature, keyEncipherment
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	(présent)
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access</i> (CA Issuer)	N	(présent)
<i>Authority Information Access</i> (OCSP)	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	tlsServerAuth
<i>Qc Compliance</i>	N	Non utilisée

2.15.2 OID 1.2.250.1.86.2.6.4.23.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	DigitalSignature
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)

Champ	C	Contenu/Présent/Absent
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth
Qc Compliance	N	Non utilisée

2.15.3 OID 1.2.250.1.86.2.6.4.60.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, keyEncipherment
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	(présent)
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée
Extended KeyUsage Cf [RFC5280]	N	tlsClientAuth, tlsServerAuth
Qc Compliance	N	Non utilisée

2.15.4 OID 1.2.250.1.86.2.6.4.61.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	N	(présent)
Basic Constraints	O	false
Key Usage	O	DigitalSignature, keyEncipherment
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent)
CertificatePolicies (Point de distribution (CPS))	N	(présent)
Subject Alternative Name (Adresse RFC822 : email)	N	Non utilisée
Subject Alternative Name (Adresse RFC822 : DNS)	N	(présent)
Issuer AlternativeName	N	Non utilisée
Subject Directory Attributes	N	Non utilisée
CRL DistributionPoints	N	(présent)
Authority Information Access (CA Issuer)	N	(présent)
Authority Information Access (OCSP)	N	(présent)
Freshest CRL	N	Non utilisée

Champ	C	Contenu/Présent/Absent
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	tlsServerAuth
<i>Qc Compliance</i>	N	Non utilisée

2.16AC SIGNATURE CONTRALIA

2.16.1 OID 1.2.250.1.86.2.6.9.34.1

Champ	C	Contenu/Présent/Absent
<i>Authority KeyIdentifier</i>	N	(présent)
<i>Subject Key Identifier</i>	N	(présent)
<i>Basic Constraints</i>	O	false
<i>Key Usage</i>	O	nonRepudiation
<i>CertificatePolicies</i> (OID de la PC de l'AC émettrice)	N	(présent)
<i>CertificatePolicies</i> (Point de distribution (CPS))	N	(présent)
<i>Subject Alternative Name</i> (Adresse RFC822 : email)	N	Non utilisée
<i>Subject Alternative Name</i> (Adresse RFC822 : DNS)	N	Non utilisée
<i>Issuer AlternativeName</i>	N	Non utilisée
<i>Subject Directory Attributes</i>	N	Non utilisée
<i>CRL DistributionPoints</i>	N	(présent)
<i>Authority Information Access</i> (CA Issuer)	N	(présent)
<i>Authority Information Access</i> (OCSP)	N	(présent)
<i>Freshest CRL</i>	N	Non utilisée
<i>Extended KeyUsage</i> <i>Cf [RFC5280]</i>	N	Non utilisée
<i>Qc Compliance</i>	N	(présent)
<i>QcSSCD</i>	N	(présent)
<i>QcType</i>	N	id-etsi-qct-esign(1)
<i>QcPDS</i>	N	URL vers les CGU-EN

3 PROFIL DES LCR

3.1 CHAMP DE BASE

Champ	Contenu
Version	"1", indiquant qu'il s'agit d'une LCR version 2.
Serial number	Pas d'exigence supplémentaire par rapport au [RFC5280]
Signature	sha256WithRSAEncryption
Issuer	DN de l'AC émettrice
This Update	date d'émission de cette LCR.
Next Update	date limite d'émission de la prochaine LCR.
Revoked Certificates	<ul style="list-style-type: none"> - 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	Contenu
Authority Key Identifier	N	(présente)
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 ALGORITHMES ET LONGUEURS DE CLES

4.1 LONGUEURS DE CLES

4.1.1 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.

4.1.2 Clés des bénéficiaires

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).

Dans la pratique, sauf cas exceptionnel (en respectant la note mentionnée ci-après), les bi-clés RSA ont une longueur de 4096 bits.

Note : Suivant la note de l'ANSSI n°920 datée du 15 mai 2024¹, les bi-clés de 2048 bits peuvent être émises jusqu'au 31/12/2025, avec une durée de validité de 3 ans maximum.

4.2 VALIDITE DES CLÉS

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).

Dans le cas spécifique des certificats éphémères², la durée de vie des certificats est fixée à 30 minutes. La clé privée associée au certificat est supprimée à l'échéance du certificat.

4.2.1 Clés privées

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

4.2.2 Clés publiques

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

4.2.2.1 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 trois (3) ans, en respectant la note n°920 de l'ANSSI citée plus haut dans le document .

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

¹ [Note clarification utilisation RSA 2948 bits PCSo qualifiés \(cyber.gouv.fr\)](#)

² OID : 1.2.250.1.86.2.6.10.2.1, 1.2.250.1.86.2.6.10.2.2, 1.2.250.1.86.2.6.11.2.1, 1.2.250.1.86.2.6.11.2.2, 1.2.250.1.86.2.6.12.2.1, 1.2.250.1.86.2.6.12.2.2 et 1.2.250.1.86.2.6.9.34.1

4.2.2.2 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.

5 ANNEXE – EXIGENCES SUR LES IDENTIFIANTS DE PORTEURS ET DE SERVEURS

5.1 FORME DES NOMS DES PORTEURS

5.1.1 Certificat d'organisation

SNU = « n° unique »	Le SNU est calculé par l'Autorité de façon à assurer l'unicité du bénéficiaire
SN = « Nom de famille »	Le SN peut contenir le « Nom » du bénéficiaire
GN = « Prénom »	Le GN peut contenir le « Prénom » du bénéficiaire
CN= « Identité »	Le CN doit contenir le « Prénom Nom » du bénéficiaire
T = « Texte libre »	Le T peut contenir la fonction du bénéficiaire
OU= « Texte libre »	L'OU peut contenir la direction dans l'organisation du bénéficiaire
OI= « Identifiant d'Organisation »	L'OI est destiné à recevoir l'identifiant de l'organisation du bénéficiaire.
O= « Raison sociale »	Le O contient la raison sociale de l'organisation du bénéficiaire
C= « Pays »	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.

Pour cela, l'attribut organizationIdentifier 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 SIREN ou le SIRET (l'ICD du numéro SIREN / SIRET est 0002, suivi d'un espace et de 9 caractères pour le SIREN et de 14 caractères pour le 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).

5.1.2 Certificat de particulier

SNU = « n° unique »	Le SNU est calculé par l'Autorité de façon à assurer l'unicité du bénéficiaire
SN = « Nom de famille »	Le SN peut contenir le « Nom » du bénéficiaire
GN = « Prénom »	Le GN peut contenir le « Prénom » du bénéficiaire
CN= « Identité »	Le CN doit contenir le « Prénom Nom » du bénéficiaire
C= « Pays »	Le C contient le pays de l'autorité compétente ayant émise la pièce d'identité.

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).

5.2 FORME DES NOMS DES SERVICES APPLICATIFS

5.2.1 Certificat de serveur

SNU = « n° unique »	Le SNU est calculé par l'Autorité de façon à assurer l'unicité du bénéficiaire
CN= « Identité »	Le CN doit contenir l'identité du serveur
L = « Texte libre »	Le L doit contenir la ville du serveur
ST = « Texte libre »	Le ST peut contenir le département du serveur
OU= « Texte libre »	L'OU est destiné à recevoir l'ICD de l'organisation du serveur.
OI= « Identifiant d'Organisation »	L'OI est destiné à recevoir l'identifiant de l'organisation du serveur.
O= « Raison sociale »	Le O contient la raison sociale de l'organisation du serveur
C= « Pays »	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.

Pour cela, l'attribut `organizationIdentifier` 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 SIREN ou le SIRET (l'ICD du numéro SIREN / SIRET est 0002, suivi d'un espace et de 9 caractères pour le SIREN et de 14 caractères pour le SIRET).

L'attribut `serialNumber` est présent dans les certificats, pour traiter les cas d'homonymie (cf. [RFC3739] et suivant).

5.2.1.1 Authentification SSL / TLS

L'attribut `commonName` est utilisé et ne comporte que le *FQDN (Fully Qualified Domain Name)* du serveur.

5.2.1.2 Authentification Client

L'attribut `commonName` est utilisé et comporte soit le FQDN soit l'identité et la fonction du serveur.

L'identité peut être soit la Raison Sociale de l'organisation, soit une marque déposée par l'organisation.

La fonction du serveur est séparée par un tiret ; Exemple : CN=Certinomis – Services SAML

5.2.1.3 Cachet serveur

L'attribut `commonName` est utilisé et comporte soit le FQDN soit l'identité et la fonction du serveur.

L'identité peut être soit la Raison Sociale de l'organisation, soit une marque déposée par l'organisation.

La fonction du serveur est séparée par un tiret ; Exemple : CN=Certinomis - Facture électronique

5.2.1.4 Unité d'Horodatage

L'attribut `commonName` est utilisé et comporte au minimum l'identité et la fonction du serveur séparée par le numéro de série de l'unité d'horodatage.

L'identité peut être soit la Raison Sociale de l'organisation, soit une marque déposée par l'organisation.

La fonction du serveur est Unité Horodatage ou UNITE HORODATAGE ; Exemple : TSA-LAPOSTE - UNITE HORODATAGE-0925327-2