POLITIQUE DE CERTIFICATION

Profils des Certificats, Listes de Certificats Révoqués, OCSP Algorithmes Cryptographiques

EMETTEUR	DESTINATAIRES	COPIES
CERTINOMIS	PUBLIC	

Certinomis

Certinomis SA au capital de 40 156 euros.

Siège social : 45-47 Boulevard Paul Vaillant-Couturier

94200 Ivry sur Seine – France. RCS Créteil B 433 998 903

Historique des versions

DATE	VERSION	EVOLUTION	AUTEUR
03/09/2021	1.0	Validation version publique	F. CHASSERY

Table des matières

AVERTISSEMENT

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)*	OI=NTRFR-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
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
PRIME	Certinomis - Prime CA	10 ans

AC	Common Name	Durée de vie
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

2.1.2 Extensions du certificat

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

Champ	C	Général
Authority Key Identifier	N	Pour tous les certificats d'AC, autres que les certificats auto-signés, cette extension doit être présente, être marquée "non critique" et contenir l'identifiant de clé de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice). Méthode 1 définie dans la RFC 5280 chapitre 4.2.1.2.
Subject Key Identifier	N	Identifiant de la clé du sujet (AC)
Key Usage	O	keyCertSign, CRLSign
Basic Constraints	O	CA:TRUE
Certificate Policies	N	anyPolicy identifier (2.5.29.32.0)
Subject Alternative Name *Issuer Alternative Name*	N	Non utilisée
CRL Distribution Points	N	Points de distribution vers la CRL de l'AC Racine
Authority Information Access	N	Non utilisée 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*

2.1.2.1 Extended Key Usage des AC

AC	Extended Key Usage
AA-AGENTS	Non utilisée
EASY	Non utilisée
EASY G2	*TLS Web Client Authentication, E-mail Protection, OCSP Signing*
FLASH	*E-mail Protection, OCSP Signing*
ONCE	*E-mail Protection, OCSP Signing*
PRIME	Non utilisée
PRIME G2	*TLS Web Client Authentication, E-mail Protection, OCSP Signing*
SAFE	*TLS Web Client Authentication, TLS Web Server Authentication, OCSP Signing*
STANDARD	Non utilisée
STANDARD G2	*TLS Web Client Authentication, E-mail Protection, OCSP Signing*

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

AC	Extended Key Usage
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 1.2.250.1.86.2.3.8.1.1

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)
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

2.3.8 OID 1.2.250.1.86.2.3.8.2.1

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)

Champ	C	Contenu/Présent/Absent
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

2.3.9 OID 1.2.250.1.86.2.3.8.3.1

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

2.3.10 OID 1.2.250.1.86.2.3.8.10.1

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)

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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

2.3.11 OID 1.2.250.1.86.2.3.8.22.1

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

2.3.12 OID 1.2.250.1.86.2.3.8.23.1

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)
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	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	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
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	(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

2.4.2 OID 1.2.250.1.86.2.6.1.2.1

Champ	C	Contenu/Présent/Absent
Authority KeyIdentifier	N	(présent)
Subject Key Identifier	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	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	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 1.2.250.1.86.2.6.1.26.1

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)

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	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
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

2.5.2 OID 1.2.250.1.86.2.3.1.2.1

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)

Champ	C	Contenu/Présent/Absent
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

2.5.3 OID 1.2.250.1.86.2.3.1.3.1

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

2.5.4 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)

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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, 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
Extended KeyUsage *Cf [RFC5280]*	N	tlsServerAuth
Qc Compliance	N	Non utilisée

2.5.6 OID 1.2.250.1.86.2.3.1.22.1

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)
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

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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

2.5.7 OID 1.2.250.1.86.2.3.1.23.1

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

2.5.8 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

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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)
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)

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	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)
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	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	Non utilisée

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

2.7 AC ONCE

2.7.1 OID 1.2.250.1.86.2.6.11.2.1

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	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	Non utilisée

2.7.2 OID 1.2.250.1.86.2.6.12.2.1

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	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	Non utilisée

2.8 AC PRIME G2

2.8.1 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
CertificatePolicies (OID de la PC de l'AC émettrice)	N	(présent) 0.4.0.194112.1.3
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	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-eseal(2)
QcPDS	N	URL vers les CGU-EN

2.8.2 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)
CertificatePolicies (Point de distribution (CPS))	N	(présent) 0.4.0.194112.1.0
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

2.8.3 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 (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

2.8.4 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 (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	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

2.8.5 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

2.8.6 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

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Champ	C	Contenu/Présent/Absent
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

2.8.7 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
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

2.8.8 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

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Champ	C	Contenu/Présent/Absent
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

2.8.9 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)
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

2.8.10 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

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Champ	C	Contenu/Présent/Absent
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

2.8.11 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)
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

2.8.12 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

Champ	C	Contenu/Présent/Absent
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

2.8.13 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)
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

2.9 AC PRIME

2.9.1 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

2.9.2 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
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

2.9.3 OID 1.2.250.1.86.2.3.3.10.1

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)
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	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.9.4 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)

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

2.9.5 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)
QcPDS	N	URL vers les CGU-EN

2.9.6 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

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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

2.9.7 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)
QcPDS	N	URL vers les CGU-EN

2.9.8 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

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

2.9.9 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
Qc Compliance	N	Non utilisée

2.9.10 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

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

2.9.11 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
Qc Compliance	N	(présent)
QcSSCD	N	(présent)
QcType	N	id-etsi-qct-esign(1)
QcPDS	N	URL vers les CGU-EN

2.9.12 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)

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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

2.10AC SAFE

2.10.1 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

2.11AC STANDARD G2

2.11.1 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)

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Champ	C	Contenu/Présent/Absent
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

2.11.2 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

2.11.3 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

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Champ	C	Contenu/Présent/Absent
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

2.11.4 OID 1.2.250.1.86.2.6.2.22.1

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

2.11.5 OID 1.2.250.1.86.2.6.2.30.1

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)

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

2.12AC STANDARD

2.12.1 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

2.12.2 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)

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

2.12.3 OID 1.2.250.1.86.2.3.5.30.1

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

2.13AC TIMESTAMP

2.13.1 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

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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

2.14AC WEB

2.14.1 OID 1.2.250.1.86.2.6.4.20.1

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

2.14.2 OID 1.2.250.1.86.2.6.4.23.1

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)

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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

2.14.3 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

2.14.4 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
Extended KeyUsage *Cf [RFC5280]*	N	tlsServerAuth
Qc Compliance	N	Non utilisée

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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	- 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 complexitéau 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 supportéespar cette PC.

4.1.2 Clés des bénéficiaires

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

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 laclé publique.
Par exemple, pour une clé privée valable 3 ans et une clé publique valable 10 ans, si un documentest 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).

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 dix (10) ans.
La période de validité des clés RSA 4096 bits est d'au plus vingt (20) ans.

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.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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).

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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