Profils des certificats et LCR

Autorité de certification

« CERTEUROPE ADVANCED CA V4 »

Version : 1.0

Date de création : 21 octobre 2013
Dernière MAJ : 22 novembre 2013
Etat du document : Officiel
Rédigé par : CertEurope
Vérifié par : Comité PKI
Approuvé par : Comité PKI

CertEurope, une société du groupe Oodrive
www.certeurope.fr
26, rue du Faubourg Poissonnière, 75010 Paris – France
Tel : +33 (0)1 45 26 72 00 / Fax : +33 (0)1 45 26 72 01

MODIFICATIONS			
Date	Etat	Version	Commentaires
21/10/2013	Officiel	1.0	

SOMMAIRE

MODIFICATIONS 2
SOMMAIRE 3
1. INTRODUCTION 4
1.1. PRESENTATION GENERALE 4
2. PROFILS DES CERTIFICATS 5
2.1. Certificat d'AC 5
2.1.1. Champs primaires du certificat d'AC 5
2.1.2. Extensions du certificat d'AC 5
*2.2. Certificats « Porteurs » RGS*** 6
2.2.1. Champs primaires des certificats 6
2.2.2. Extensions des certificats 6
2.2.2.1. Profil « Authentification » : 6
2.2.2.2. Profil « Signature » : 7
2.2.2.3. Profil « Authentification et signature » : 7
*2.3. Certificats « Porteurs » RGS** 9
2.3.1. Champs primaires des certificats 9
2.3.2. Extensions des certificats 9
2.3.2.1. Profil « Authentification » : 9
2.3.2.2. Profil « Signature » : 10
2.3.2.3. Profil « Authentification et signature » : 10
2.4. Certificats serveurs 12
2.4.1. Champs primaires des certificats 12
2.4.2. Extensions des certificats 12
3. PROFIL DE LCR 16
3.1.1. CHAMPS DES LCR 16
3.1.2. EXTENSIONS DES LCR 16

1. INTRODUCTION

1.1. PRESENTATION GENERALE

Ce document présente les différents profils de certificats délivrés par l'Autorité de Certification CERTEUROPE ADVANCED CA V4 en fonction des niveaux de sécurité et des usages. Il présente également le profil de LCR.

2. PROFILS DES CERTIFICATS

2.1. Certificat d'AC

2.1.1. Champs primaires du certificat d'AC

Le certificat de l'AC CERTEUROPE ADVANCED CA V4 contient les champs primaires suivants :

Champs de base	Valeur
Version	2 (=version 3)
Serial number	02 26 d6
Signature	Sha256WithRSAEncryption (2.16.840.1.101.3.4.2.1)
Hash	Sha256
Issuer DN	CN = Certeurope Root CA 3 OU = 0002 434202180 O = Certeurope C = FR
Valid from	jeudi 26 août 2010 00:00:00
Period of validity	mercredi 26 août 2020 00:00:00
Subject DN	CN = CERTEUROPE ADVANCED CA V4 OU = 0002 434202180 O = Certeurope C = FR
Subject Public Key Info	RSA (2048 bits)

2.1.2. Extensions du certificat d'AC

Le certificat de l'AC CERTEUROPE ADVANCED CA V4 contient les extensions suivantes :

Champ	O	C	Valeur
Subject Key Identifier	TRUE	FALSE	40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.8.1.1.0 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc-root3.pdf
Authority Key Identifier	TRUE	FALSE	ID de la clé=4c 64 44 ff 68 22 69 74
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=http://www.certeurope.fr/reference/root3.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr1.certeurope.fr/cn=Certeurope%20Root%20CA%203,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr2.certeurope.fr/cn=Certeurope%20Root%20CA%203,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList
Basic Constraints	TRUE	TRUE	Type d'objet=Autorité de certification Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Signature du certificat, Signature de la liste de révocation des certificats hors connexion, Signature de la liste de révocation des certificats (06)
Algorithme d'empreinte numérique			sha1
Empreinte numérique			80 92 70 62 d7 b1 05 b9 d8 d8 23 ae 12 51 e7 53 68 31 e6 50

2.2. Certificats « Porteurs » RGS**

2.2.1. Champs primaires des certificats

Les certificats de Porteurs contiennent les champs primaires suivants :

Champs de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'application (exemple : B06C)
Signature	Sha256WithRSAEncryption (2.16.840.1.101.3.4.2.1)
Hash	sha256
Issuer DN	CN = CERTEUROPE ADVANCED CA V4 OU = 0002 434202180 O = Certeurope C = FR
Valid from	Au plus tôt à la date de début de vie de l'AC : 26/08/2010
Period of validity	3 ans (valide au plus tard à la date de fin de vie de l'AC : 26/08/2020)
Subject DN	SERIALNUMBER = HASH (SHA-1) des informations personnelles du porteur contenues dans sa pièce d'identité CN = Prénom et Nom du porteur OU = n° SIREN de l'entité à laquelle le porteur est rattaché O = Raison sociale de l'entité à laquelle le porteur est rattaché C = FR
Subject Public Key Info	RSA (2048 bits)

2.2.2. Extensions des certificats

Les certificats de Porteurs contiennent les extensions suivantes, en fonction des profils :

2.2.2.1. Profil « Authentification » :

Champ	O	C	Valeur
Extended Key Usage	TRUE	FALSE	Authentification du client (1.3.6.1.5.5.7.3.2)
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.10.3.1.3 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc_certeurope_v4_2E_v1.3.pdf
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=http://www.certeurope.fr/reference/certeurope_v4.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr1.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr2.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList
Subject Key Identifier	TRUE	FALSE	Identifiant de la clé publique du porteur
Subject Alternative Name	TRUE	FALSE	Nom RFC822=adresse mail du porteur
1.2.752.34.2.1	TRUE	FALSE	Extension de certificat x.509 v3 permettant d'associer un certificat à une carte à puce physique
Basic Constraints	TRUE	FALSE	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Signature numérique
Algorithme d'empreinte numérique			

Empreinte numérique			

2.2.2.2. Profil « Signature » :

Champ	O	C	Valeur
Extended Key Usage	TRUE	FALSE	Messagerie électronique sécurisée (1.3.6.1.5.5.7.3.4)
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.10.4.1.3 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc_certeurope_v4_2E_v1.3.pdf
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=http://www.certeurope.fr/reference/certeurope_v4.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr1.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%2043420218 0,o=Certeurope,c=FR?certificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr2.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%2043420218 0,o=Certeurope,c=FR?certificateRevocationList
Subject Key Identifier	TRUE	FALSE	Identifiant de la clé publique du porteur
Subject Alternative Name	TRUE	FALSE	Nom RFC822=adresse mail du porteur
1.2.752.34.2.1	TRUE	FALSE	Extension de certificat x.509 v3 permettant d'associer un certificat à une carte à puce physique
Basic Constraints	TRUE	FALSE	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Non-répudiation
qCStatement			esi4-qcStatement-1 esi4-qcStatement-2 esi4-qcStatement-3 esi4-qcStatement-4
Algorithme d'empreinte numérique			
Empreinte numérique			

2.2.2.3. Profil « Authentification et signature » :

Champ	O	C	Valeur
Extended Key Usage	TRUE	FALSE	Authentification du client (1.3.6.1.5.5.7.3.2) Messagerie électronique sécurisée (1.3.6.1.5.5.7.3.4)
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.10.1.1.3 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc_certeurope_v4_2E_v1.3.pdf
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution :

			Nom complet : URL=http://www.certeurope.fr/reference/certeurope_v4.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr1.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr2.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList
Subject Key Identifier	TRUE	FALSE	Identifiant de la clé publique du porteur
Subject Alternative Name	TRUE	FALSE	Nom RFC822=adresse mail du porteur
1.2.752.34.2.1	TRUE	FALSE	Extension de certificat x.509 v3 permettant d'associer un certificat à une carte à puce physique
Basic Constraints	TRUE	FALSE	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Signature numérique, Non-répudiation
Algorithme d'empreinte numérique			
Empreinte numérique			

2.3. Certificats « Porteurs » RGS*

2.3.1. Champs primaires des certificats

Les certificats de Porteurs contiennent les champs primaires suivants :

Champs de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'application (exemple : B06C)
Signature	Sha256WithRSAEncryption (2.16.840.1.101.3.4.2.1)
Hash	sha256
Issuer DN	CN = CERTEUROPE ADVANCED CA V4 OU = 0002 434202180 O = Certeurope C = FR
Valid from	Au plus tôt à la date de début de vie de l'AC : 26/08/2010
Period of validity	3 ans (valide au plus tard à la date de fin de vie de l'AC : 26/08/2020)
Subject DN	SERIALNUMBER = HASH (SHA-1) des informations personnelles du porteur contenues dans sa pièce d'identité CN = Prénom et Nom du porteur OU = n° SIREN de l'entité à laquelle le porteur est rattaché O = Raison sociale de l'entité à laquelle le porteur est rattaché C = FR
Subject Public Key Info	RSA (2048 bits)

2.3.2. Extensions des certificats

Les certificats de Porteurs contiennent les extensions suivantes, en fonction des profils :

2.3.2.1. Profil « Authentification » :

Champ	O	C	Valeur
Extended Key Usage	TRUE	FALSE	Authentification du client (1.3.6.1.5.5.7.3.2)
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.21.3.1.0 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc_certeurope_v4_1E_v1.3.pdf
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=http://www.certeurope.fr/reference/certeurope_v4.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr1.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr2.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList
Subject Key Identifier	TRUE	FALSE	Identifiant de la clé publique du porteur
Subject Alternative Name	TRUE	FALSE	Nom RFC822=adresse mail du porteur
Basic Constraints	TRUE	FALSE	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Signature numérique
Algorithme d'empreinte numérique			
Empreinte			

numérique			

2.3.2.2. Profil « Signature » :

Champ	O	C	Valeur
Extended Key Usage	TRUE	FALSE	Messagerie électronique sécurisée (1.3.6.1.5.5.7.3.4)
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.21.4.1.0 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc_certeurope_v4_1E_v1.3.pdf
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=http://www.certeurope.fr/reference/certeurope_v4.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr1.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%2043420218 0,o=Certeurope,c=FR?certificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr2.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%2043420218 0,o=Certeurope,c=FR?certificateRevocationList
Subject Key Identifier	TRUE	FALSE	Identifiant de la clé publique du porteur
Subject Alternative Name	TRUE	FALSE	Nom RFC822=adresse mail du porteur
Basic Constraints	TRUE	FALSE	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Non-répudiation
Algorithme d'empreinte numérique			
Empreinte numérique			

2.3.2.3. Profil « Authentification et signature » :

Champ	O	C	Valeur
Extended Key Usage	TRUE	FALSE	Authentification du client (1.3.6.1.5.5.7.3.2) Messagerie électronique sécurisée (1.3.6.1.5.5.7.3.4)
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.21.1.1.0 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc_certeurope_v4_1E_v1.3.pdf
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=http://www.certeurope.fr/reference/certeurope_v4.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet :

			URL=ldap://lcr1.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr2.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList
Subject Key Identifier	TRUE	FALSE	Identifiant de la clé publique du porteur
Subject Alternative Name	TRUE	FALSE	Nom RFC822=adresse mail du porteur
Basic Constraints	TRUE	FALSE	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Signature numérique, Non-répudiation
Algorithme d'empreinte numérique			
Empreinte numérique			

2.4. Certificats serveurs

2.4.1. Champs primaires des certificats

Les certificats de serveurs contiennent les champs primaires suivants :

Champs de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'application (exemple : B06C)
Signature	Sha256WithRSAEncryption (2.16.840.1.101.3.4.2.1)
Hash	sha256
Issuer DN	CN = CERTEUROPE ADVANCED CA V4 OU = 0002 434202180 O = Certeurope C = FR
Valid from	Au plus tôt à la date de début de vie de l'AC : 26/08/2010
Period of validity	3 ans (valide au plus tard à la date de fin de vie de l'AC : 26/08/2020)
Subject DN	CN = nom significatif du service applicatif, FQDN du serveur dans le cas d'un serveur de type SSL/TLS OU = n° SIREN de l'entité à laquelle le serveur est rattaché O = Raison sociale de l'entité à laquelle le serveur est rattaché C = FR
Subject Public Key Info	RSA (2048 bits)

2.4.2. Extensions des certificats

Les certificats de serveurs contiennent les extensions suivantes, en fonction des profils :

2.4.2.1. Authentification serveur SSL/TLS RGS*

Champ	O	C	Valeur
Extended Key Usage	TRUE	FALSE	Authentification du serveur (1.3.6.1.5.5.7.3.1)
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.18.1.1.0 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc_certeurope_v4_auth-serveur_v1.0.pdf
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=http://www.certeurope.fr/reference/certeurope_v4.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr1.certeurope.fr/CN=CERTEUROPE%20ADVANCED%20CA%20V4,OU=0002%20434202180,O=Certeurope,C=FR?CertificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr2.certeurope.fr/CN=CERTEUROPE%20ADVANCED%20CA%20V4,OU=0002%20434202180,O=Certeurope,C=FR?CertificateRevocationList
Subject Key Identifier	TRUE	FALSE	Identifiant de la clé publique du porteur
Subject Alternative Name	TRUE	FALSE	Nom RFC822=adresse mail du RCAS
Basic Constraints	TRUE	FALSE	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Chiffrement de la clé
Algorithme d'empreinte numérique			
Empreinte numérique			

2.4.2.2. Authentification serveur client RGS*

Champ	O	C	Valeur
Extended Key Usage	TRUE	FALSE	Authentification du client (1.3.6.1.5.5.7.3.2)
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.18.4.1.0 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc_certeurope_v4_auth-serveur_v1.0.pdf
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=http://www.certeurope.fr/reference/certeurope_v4.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr1.certeurope.fr/CN=CERTEUROPE%20ADVANCED%20CA%20V4,OU=0002%20434202180,O=Certeurope,C=FR?CertificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr2.certeurope.fr/CN=CERTEUROPE%20ADVANCED%20CA%20V4,OU=0002%20434202180,O=Certeurope,C=FR?CertificateRevocationList
Subject Key Identifier	TRUE	FALSE	Identifiant de la clé publique du porteur
Subject Alternative Name	TRUE	FALSE	Nom RFC822=adresse mail du RCAS
Basic Constraints	TRUE	FALSE	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Signature digitale
Algorithme d'empreinte numérique			
Empreinte numérique			

2.4.2.3. Authentification serveur SSL/TLS RGS**

Champ	O	C	Valeur
Extended Key Usage	TRUE	FALSE	Authentification du serveur (1.3.6.1.5.5.7.3.1)
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.18.3.1.0 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc_certeurope_v4_auth-serveur_v1.0.pdf
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=http://www.certeurope.fr/reference/certeurope_v4.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr1.certeurope.fr/CN=CERTEUROPE%20ADVANCED%20CA%20V4,OU=0002%20434202180,O=Certeurope,C=FR?CertificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet :

			URL=ldap://lcr2.certeurope.fr/CN=CERTEUROPE%20ADVANCED%20CA%20V4,OU=0002%20434202180,O=Certeurope,C=FR?CertificateRevocationList
Subject Key Identifier	TRUE	FALSE	Identifiant de la clé publique du porteur
Subject Alternative Name	TRUE	FALSE	Nom RFC822=adresse mail du RCAS
Basic Constraints	TRUE	FALSE	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Chiffrement de la clé
Algorithme d'empreinte numérique			
Empreinte numérique			

2.4.2.4. Cachet serveur RGS*

Champ	O	C	Valeur
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.12.1.1.0 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc_certeurope_v4_auth-serveur_v1.0.pdf
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=http://www.certeurope.fr/reference/certeurope_v4.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr1.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr2.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList
Subject Key Identifier	TRUE	FALSE	Identifiant de la clé publique du sujet
Subject Alternative Name	TRUE	FALSE	Nom RFC822=adresse mail de l'entité ou du RCCS
Basic Constraints	TRUE	FALSE	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Signature numérique, Non-répudiation
Algorithme d'empreinte numérique			
Empreinte numérique			

2.4.2.5. Cachet serveur RGS**

Champ	O	C	Valeur
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
Certificate Policies	TRUE	FALSE	[1]Stratégie du certificat : Identificateur de stratégie=1.2.250.1.105.12.3.1.0 [1,1]Informations sur le qualificatif de stratégie : ID du qualificatif de stratégie =CPS Qualificatif : http://www.certeurope.fr/reference/pc_certeurope_v4_auth-serveur_v1.0.pdf
CRL Distribution Points	TRUE	FALSE	[1]Point de distribution de la liste de révocation des certificats Nom du point de distribution :

			Nom complet : URL=http://www.certeurope.fr/reference/certeurope_v4.crl [2]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr1.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%2043420218 0,o=Certeurope,c=FR?certificateRevocationList [3]Point de distribution de la liste de révocation des certificats Nom du point de distribution : Nom complet : URL=ldap://lcr2.certeurope.fr/cn=CERTEUROPE%20ADVANCED%20CA%20V4,ou=0002%2043420218 0,o=Certeurope,c=FR?certificateRevocationList
Subject Key Identifier	TRUE	FALSE	Identifiant de la clé publique du sujet
Subject Alternative Name	TRUE	FALSE	Nom RFC822= adresse mail de l'entité ou du RCCS
Basic Constraints	TRUE	FALSE	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=Aucun(e)
Key Usage	TRUE	TRUE	Signature numérique, Non-répudiation
Algorithme d'empreinte numérique			
Empreinte numérique			

3. PROFIL DE LCR

3.1.1. CHAMPS DES LCR

Champs de base	Valeur
Version	Version 2
Signature	Sha256WithRSAEncryption (2.16.840.1.101.3.4.2.1)
Hash	sha256
Issuer DN	CN = CERTEUROPE ADVANCED CA V4 OU = 0002 434202180 O = Certeurope C = FR
This Update	Au plus tôt à la date de début de vie de l'AC : 26/08/2010
Next Update	Prochaine date à laquelle la CRL sera mise à jour, soit 7 jours après la date de génération de la présente CRL. Exemple : « mercredi 15 juillet 2011 10 :20 :56 »
Revoked Certificates	N° de série des certificats révoqués. Exemple : « 0C0062 »
Revocation Date	Date à laquelle un Certificat donné à été révoqué. Exemple : « Date de révocation : vendredi 10 novembre 2012 11 :51 :19 »

3.1.2. EXTENSIONS DES LCR

Champ	O	C	Valeur
Authority Key Identifier	TRUE	FALSE	ID de la clé=40 56 5f 59 f3 1c ad 05
CRL Number	TRUE	FALSE	N° de série de la CRL Exemple : « 0115 »