Profils de Certificats et de LCR

AC ChamberSign

-

ChamberSign France

Objet du document :	Ce document spécifie le contenu des certificats et des listes de certificats révoqués de la hiérarchie des autorités de certification ChamberSign France « AC CHAMBERSIGN ».
Version	Diffusion
Date de diffusion	Juin 2011

SOMMAIRE

1 INTRODUCTION....4
1.1 OBJET DU DOCUMENT....4
1.2 DOCUMENTS DE REFERENCE....4
2 CERTIFICATS D'AC....6
2.1 AC RACINE – SIGNATURE DE CERTIFICATS D'AC....6
2.2 AC INTERMEDIAIRE – SIGNATURE DE LAR....7
2.3 AC INTERMEDIAIRES – SIGNATURE DE CERTIFICATS PORTEURS....8
2.4 AC INTERMEDIAIRES – SIGNATURE DE LCR....9
2.5 AC INTERMEDIAIRES – SIGNATURE DE REPONSES OCSP....10
3 CERTIFICATS DE PORTEURS....12
4 LISTES DE CERTIFICATS REVOQUES....15
4.1 LAR....15
4.2 LCR....16

Avertissement

1 Introduction

1.1 Objet du document

Le présent document fait partie des documents de spécification liés à la hiérarchie d'autorité de certification de ChamberSign France « AC CHAMBERSIGN ». Il spécifie le contenu des certificats et des listes de certificats révoqués (LCR) de cette hiérarchie, pour les certificats de porteurs et pour les certificats des différentes AC de la hiérarchie.

Cette hiérarchie couvre la fourniture, à des porteurs professionnels (secteur privé et secteur public), de certificats conformes au Référentiel Général de Sécurité (RGS), à savoir :

- certificats double-usage (signature et authentification) niveau 2*,
- certificats d'authentification niveaux 2* et 3*,
- certificats de signature niveaux 2* et 3*.

Cette hiérarchie est composée de deux niveaux :

- une AC Racine « AC Racine – ChamberSign »,
- une AC intermédiaire par type de certificats porteurs (double usage 2* RGS, authentification 2* RGS, authentification 3* RGS, signature 2* RGS, signature 3* RGS).

L'AC Racine comporte deux bi-clés : une bi-clé, dont le certificat correspondant est autosigné, qui correspond au sommet de la hiérarchie et qui est utilisée pour signer les autres certificats d'AC, une bi-clé, dont le certificat est signé par la bi-clé précédente, utilisée pour signer les LAR (liste des AC révoquées).

Chaque AC intermédiaire comporte trois bi-clés : une bi-clé utilisée pour signer les certificats des porteurs de la classe correspondante, une bi-clé utilisée pour signer les LCR (listes de certificats révoqués) des certificats de la classe correspondante et une bi-clé utilisée pour signer les réponses OCSP pour les certificats de la classe correspondante.

1.2 Documents de référence

Renvoi	Document
[RGS-PROFILS]	Référentiel Général de Sécurité – Politiques de Certification Types – Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques – Version 2.2 du 12/12/2008
[ETSI-CERT]	ETSI TS 102 208 – X.509 v.3 Certificate Profile for Certifcates Issued to Natural Persons – v1.1.1 03/2004
[ETSI-QC]	ETSI TS 101 862 – Qualified Certificate profile – v1.3.3 01/2006
[RFC5280]	RFC5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – 05/2008
[RFC3039]	RFC3039 – Internet X.509 Public Key Infrastructure: Qualified Certificates Profile – 03/2004
[RFC3279]	RFC3279 – Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – 04/2002

Renvoi	Document
[RFC4055]	RFC4055 – Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – 06/2005

2 Certificats d'AC

2.1 AC Racine – Signature de certificats d'AC

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 4096 bits
Issuer	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (notBefore + 20 ans)
Subject	Identique à *Issuer*
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 4096 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de ce certificat authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
Subject Key Identifier	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de ce certificat
Key Usage	Oui	keyCertSign
Certificate Policies	Non	policyIdentifier = OID de la PC « certificats d'AC » policyQualifiers = CPSuri (IA5String) = URI du téléchargement de la PC « certificats d'AC »
Basic Constraints	Oui	cA = TRUE pathLenConstraint = 1

2.2 AC intermédiaire – Signature de LAR

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 4096 bits
Issuer	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notAfter du certificat d'AC Racine CertSign)
Subject	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 4096 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de l'AC Racine CertSign authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
Subject Key Identifier	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de ce certificat
Key Usage	Oui	cRLSign
Certificate Policies	Non	policyIdentifier = OID de la PC « certificats d'AC » policyQualifiers = CPSuri (IA5String) = URI du téléchargement de la PC « certificats d'AC »

2.3 AC Intermédiaires – Signature de certificats porteurs

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
Issuer	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime, la moins éloignée des dates suivantes : notBefore + 10 ans ; notAfter du certificat d'AC Racine ; 2020
Subject	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign - <<type et niveau>>[1]
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de l'AC Racine authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
Subject Key Identifier	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de ce certificat
Key Usage	Oui	keyCertSign
Certificate Policies	Non	policyIdentifier = OID de la PC « certificats d'AC » policyQualifiers = CPSuri (IA5String) = URI du téléchargement de la PC « certificats d'AC »

[1] « Signature et authentification 2* », « Signature 2* », « Signature 3* », « Authentification 2* », « Authentification 3* »

Extension	Criticité	Valeur
Basic Constraints	Oui	cA = TRUE pathLenConstraint = 0
CRL Distribution Points	Non	distributionPoint = URL du téléchargement de la LAR (http://crl.chambersign.tm.fr/<<nom du fichier.crl>>) reasons et cRLIssuer ne sont pas utilisés

2.4 AC Intermédiaires – Signature de LCR

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
Issuer	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime, la moins éloignée des dates suivantes : notBefore + 10 ans ; notAfter du certificat d'AC Racine ; 2020
Subject	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign - <<type et niveau>>[2]
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

[2] Cf. chapitre 2.3

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de l'AC Racine CertSign authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
Subject Key Identifier	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de ce certificat
Key Usage	Oui	cRLSign
Certificate Policies	Non	policyIdentifier = OID de la PC « certificats d'AC » policyQualifiers = CPSuri (IA5String) = URI du téléchargement de la PC « certificats d'AC »
CRL Distribution Points	Non	distributionPoint = URL du téléchargement de la LAR (http://crl.chambersign.tm.fr/<<nom du fichier.crl>>) reasons et cRLIssuer ne sont pas utilisés

2.5 AC Intermédiaires – Signature de réponses OCSP

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
Issuer	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime, la moins éloignée des dates suivantes : notBefore + 10 ans ; notAfter du certificat d'AC Racine ; 2020
Subject	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign - <<type et niveau>>[3]
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits

[3] Cf. chapitre 2.3

Champ	Valeur
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de l'AC Racine CertSign authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
Subject Key Identifier	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de ce certificat
Key Usage	Oui	digitalSignature
Certificate Policies	Non	policyIdentifier = OID de la PC « certificats d'AC » policyQualifiers = CPSuri (IA5String) = URI du téléchargement de la PC « certificats d'AC »
Extended Key Usage	Non	id-kp-OCSPSigning (cf. RFC5280)
CRL Distribution Points	Non	distributionPoint = URL du téléchargement de la LAR reasons et cRLIssuer ne sont pas utilisés

3 Certificats de porteurs

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	RSASSA-PSS-SHA256 (cf. [RFC4055]) avec une longueur de clé de 2048 bits
Issuer	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign - <<type et niveau>>[4]
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject	DN encodé en UTF8String *Pour les entités basées en France métropolitaine et dans les DOM :* countryName = FR organizationName = non officiel de l'entité organizationalUnitName = 0002 <<N° Siren de l'entité sur 9 caractères sans espace>> commonName = prénom1 nom serialNumber = numéro séquentiel de 4 chiffres permettant de traiter les cas d'homonymie[5] (givenName et surname ne sont pas utilisés) *Pour les entités basées hors de France métropolitaine et des DOM :* countryName = code ISO du pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère,…) organizationName = non officiel complet de l'entité tel qu'enregistré auprès des autorités compétentes organizationalUnitName = soit (<<ICD pour le pays considéré s'il existe>> <<Identifiant de l'entité pour l'ICD indiqué>>), soit (G+<<code GS1 du pays sur 3 chiffres>> <<Identifiant officiel de l'entité dans le pays considéré>) commonName = prénom1 nom serialNumber = numéro séquentiel de 4 chiffres permettant de traiter les cas d'homonymie[6] (givenName et surname ne sont pas utilisés)
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits

[4] Cf. chapitre 2.3

[5] Par défaut, la valeur de cet attribut est « 0001 ». Si un porteur dont les autres attributs du DN sont identiques (countryName, organizationName, organizationalUnitName et commonName) a déjà été enregistré, la valeur de l'attribut serialNumber pour le nouveau porteur passe à « 0002 » et ainsi de suite.

[6] Par défaut, la valeur de cet attribut est « 0001 ». Si un porteur dont les autres attributs du DN sont identiques (countryName, organizationName, organizationalUnitName et commonName) a déjà été enregistré, la valeur de l'attribut serialNumber pour le nouveau porteur passe à « 0002 » et ainsi de suite.

Champ	Valeur
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de l'AC Intermédiaire correspondante (CertSign) authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
Subject Key Identifier	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de ce certificat
Key Usage	Oui	*Signature et authentification 2* :* digitalSignature, nonRepudiation *Signature 2* et 3* :* nonRepudiation *Authentification 2* et 3* :* digitalSignature
Certificate Policies	Non	policyIdentifier = OID de la PC correspondant au type de certificat porteur policyQualifiers = - CPSuri (IA5String) = URI du téléchargement de la PC correspondant au type de certificat porteur - UserNotice (explicitText, UTF8String) = « Ce certificat est remis en face-à-face, sur support physique sécurisé et est conforme aux normes en vigueur »
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse mél du porteur *Pour les certificats d'authentification uniquement (mono et double-usage) :* OtherName = -type-id = 1.3.6.1.4.1.311.20.2.3 (OID Microsoft pour les UPN) - value = adresse mél du porteur (rfc822Name, chaîne UTF8 codée en ASN.1)
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
Extended key usage	Non	*Pour les certificats d'authentification uniquement (mono et double-usage) :* - 1.3.6.1.4.1.311.20.2.2 (OID Microsoft pour le Smart Card Logon) - 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth, cf. RFC5280)
CRL Distribution Points	Non	distributionPoint = uniformResourceIndicator (IA5String) du téléchargement de la LCR correspondant au type du certificat porteur reasons et cRLIssuer ne sont pas utilisés

Extension	Criticité	Valeur
Authority Information Access	Non	accessMethod = id-ad-ocsp accessLocation = uniformResourceIndicator (IA5String) du serveur OCSP
Qualified Certificate Statements	Non	*Uniquement pour les certificats signature 3** id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD

4 Listes de certificats révoqués

4.1 LAR

Champ	Valeur
Version	1
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
Issuer	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign
This Update	Date de génération de LAR au format UTCTime
Next Update	Date de génération de au plus tard de la prochaine LAR au format UTCTime (= *This Update* + 20ans)
Revoked Certificates	- userCertificate : *Serial Number* du certificat d'AC révoqué - revocationDate :date de révocation du certificat au format UTCTime - crlEntryExtensions : aucune extension d'entrée n'est utilisée
Extensions	Cf. tableau ci-dessous

Extension de LCR	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de l'AC Racine CRLSign authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
CRL Number	Non	Nombre entier séquentiel, codé sur 20 octets

4.2 LCR

Champ	Valeur
Version	1
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
Issuer	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 <<N° Siren de CSF sur 9 caractères sans espace>> commonName = ChamberSign - <<type et niveau>>[7]
This Update	Date de génération de LCR au format UTCTime
Next Update	Date de génération de au plus tard de la prochaine LAR au format UTCTime (= *This Update* + 48h)
Revoked Certificates	- userCertificate : *Serial Number* du certificat porteur révoqué - revocationDate :date de révocation du certificat au format UTCTime - crlEntryExtensions : aucune extension d'entrée n'est utilisée
Extensions	Cf. tableau ci-dessous

Extension de LCR	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de l'AC Intermédiaire correspondante (CRLSign) authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
CRL Number	Non	Nombre entier séquentiel, codé sur 20 octets

[7] Cf. chapitre 2.3