Profils de Certificats et de LCR

AC 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 FRANCE ».
Version	04
Date de diffusion	12/05/2017

SOMMAIRE

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 FRANCE ». Il spécifie le contenu des certificats et des listes de certificats révoqués (LCR) de cette hiérarchie, pour les certificats de porteurs, les certificats de cachets et d'authentification serveur, et pour les certificats des différentes AC de la hiérarchie.

Cette hiérarchie couvre la fourniture à des professionnels (secteur privé et secteur public) les types de certificats suivants :

- **Secteur privé**
  - des certificats de personnes conformes au Référentiel Général de Sécurité (RGS), à savoir :
    - certificats double-usage (signature et authentification) niveaux 1* et 2*, les certificats 2* étant également eIDAS qualifié ;
    - certificats d'authentification niveaux 1*, 2* et 3*,
    - certificats de signature niveaux 1, 2* et 3*, le certificat 3* étant également qualifiés eIDAS ;
  - des certificats de machines conformes au Référentiel Général de Sécurité (RGS), à savoir :
    - certificats de cachets authentification et signature niveau 1*,
    - certificats d'authentification serveur niveau 1*.

- **Secteur public**
  - des certificats de personnes conformes au Référentiel Général de Sécurité (RGS), à savoir :
    - certificats double-usage (signature et authentification) niveaux 1* et 2*, les certificats 2* étant également eIDAS qualifié ;
    - certificats d'authentification niveaux 1* et 2*,
    - certificats de signature niveaux 1*, 2* et 3*, le certificat 3* étant également qualifiés eIDAS ,
  - des certificats de machines conformes au Référentiel Général de Sécurité (RGS), à savoir :
    - certificats de cachets authentification et signature niveau 1*,
    - certificats d'authentification serveur niveau 1*.

Cette hiérarchie est composée de deux niveaux :

- une AC Racine « AC Racine – ChamberSign France » ;
- une AC intermédiaire par niveau d'étoiles de certificats (*, **, ***) pour le secteur privé ;
- une AC intermédiaire par niveau d'étoiles de certificats (*, **), précédé du vocable [Administration] pour le secteur de l'administration ;

L'AC Racine comporte une bi-clé dont le certificat correspondant est auto signé. Elle correspond au sommet de la hiérarchie. Elle est utilisée pour signer les autres certificats d'AC et pour signer les LAR (liste des AC révoquées).

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

1.2 Documents de référence

Renvoi	Document
[RGS-PROFILS-v1]	Référentiel Général de Sécurité version 1.0 – Politiques de Certification Types (annexes A6 à A11) – Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques (annexe A14) – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques (annexe B1 v1.20 du 26/01/2010)
[RGS-PROFILS-v2]	Référentiel Général de Sécurité Draft 0.2 (24/04/2012) de la version 2.0 – Politiques de Certification Types (annexes A2 et A3) – Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques (annexe A4) – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques (annexe B1 v2.00 du 26/04/2012)
[ETSI EN 319 412-1]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[ETSI EN 319 412-3]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[ETSI EN 319 412-5]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[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
[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

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 433702479 commonName = ChamberSign France
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, cRLSign
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.7 policyQualifiers = CPSuri (IA5String) = http://pc.chambersign.fr/rgs/lcr-directes/
Basic Constraints	Oui	cA = TRUE pathLenConstraint = 1

2.2 AC Intermédiaires

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256-RSA-PKCS1avec une longueur de clé de 4096 bits
Issuer	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France
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
Subject	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France - <<type et niveau>>[1]
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 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, cRLSign
Certificate Policies	Non	policyIdentifier = OID de la PC « certificats d'ACR » policyQualifiers = CPSuri (IA5String) = URI du téléchargement de la PC « certificats d'AC »
Basic Constraints	Oui	cA = TRUE pathLenConstraint = 0
CRL Distribution Points	Non	distributionPoint = http://crl.chambersign.fr/crl/rgs/lcr-directes/chambersign-france.crl (URL du téléchargement de la LAR) reasons et cRLIssuer ne sont pas utilisés

[1] « AC 3étoiles », « AC 2étoiles », « AC 1étoile »

2.3 AC Intermédiaire 3* – Signature de réponses OCSP

*Nota – Ce chapitre ne concerne que l'AC intermédiaire 3**

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256-RSA-PKCS1avec une longueur de clé de 4096 bits
Issuer	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France - <<type et niveau>>[2]
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 intermédiaire correspondante
Subject	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France - <<type et niveau>>[3] - OCSP
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 intermédiaire correspondante 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)

[2] Cf. chapitre 2.2
[3] « AC 3étoiles », « AC 2étoiles », « AC 1étoile »,

Extension	Criticité	Valeur
CRL Distribution Points	Non	distributionPoint = uniformResourceIndicator (IA5String) du téléchargement de la LCR correspondant au niveau du certificat porteur e (CRL binaire et LDAP). reasons et cRLIssuer ne sont pas utilisés

3 Certificats de porteurs

3.1 Certificats 1* et 2* RGS

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 433702479 commonName = ChamberSign France - <<type et niveau>>[4]
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject	DN encodé en UTF8String countryName = code ISO sur 2 lettres (cf. ISO3166-1) du pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère,…) organizationName = nom officiel de l'entité (dénomination sociale du siège social) organizationalUnitName = identifiant national de la structure, cf. ci-dessous. organizationalUnitName = le cas échéant, dénomination de l'établissement du porteur, ne commençant ni par 4 chiffres ni par un « S » suivi de 3 chiffres organizationalUnitName = le cas échéant, nom du service où travaille le porteur au sein de sa structure, ne commençant ni par 4 chiffres ni par un « S » suivi de 3 chiffres locality = ville où se trouve l'établissement du porteur commonName = prénom1(,prénom2,prénom3,…)[5] nom serialNumber[6] title = le cas échéant, fonction du porteur au sein de sa structure serialNumber = numéro séquentiel de 4 chiffres permettant de traiter les cas d'homonymie[7] (givenName et surname ne sont pas utilisés))
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

[4] Cf. chapitre 2.2

[5] Les différents prénoms sont mentionnés dans l'ordre indiqué sur la pièce d'identité présentée lors de l'enregistrement et dont la copie est conservée dans le dossier d'enregistrement.

[6] Cf. la note de bas de page n° 7. Cette valeur serialNumber n'est pas renseignée dans le commonName lorsqu'elle est 0001.

[7] 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.

Identifiant national de la structure :

- Pour les entités basées en France Métropolitaine et les DOM : 0002 <<N° SIRET sur 14 caractère>>
- Pour les entités basées en Nouvelle-Calédonie : S540 <<N° RIDET sur 9 caractères maximum>>
- Pour les autres entités basées dans un pays de la communauté européenne : S<<code ISO3166-1 du pays sur 3 chiffres>> <<n° de TVA intracommunautaire sur 14 caractères maximum>>[8]

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 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 1* et 2* :* digitalSignature, contentCommitment *Signature 1* et 2* :* contentCommitment *Authentification 1* et 2* :* 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.
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse mél du porteur *Pour les certificats d'authentification mono-usage uniquement :* 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 mono-usage uniquement :* - 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 niveau du certificat porteur e (CRL binaire et LDAP). reasons et cRLIssuer ne sont pas utilisés

[8] Exemple pour une structure basée en Allemagne : OU = S276 DE123456789

Extension	Criticité	Valeur
Qualified Certificate Statements	Non	Uniquement pour les certificats signature et authentification 2* Id-etsi-qcs-QcCompliance Id-etsi-qcs-QcSSCD

3.2 Certificat 2* RGS et eiDAS

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 433702479 commonName = ChamberSign France - <<type et niveau>>[9]
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject	DN encodé en UTF8String countryName = code ISO sur 2 lettres (cf. ISO3166-1) du pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère,…) organizationName = nom officiel de l'entité (dénomination sociale du siège social) organizationalUnitName = identifiant national de la structure, cf. ci-dessous. organizationalUnitName = le cas échéant, dénomination de l'établissement du porteur, ne commençant ni par 4 chiffres ni par un « S » suivi de 3 chiffres organizationalUnitName = le cas échéant, nom du service où travaille le porteur au sein de sa structure, ne commençant ni par 4 chiffres ni par un « S » suivi de 3 chiffres **OrganizationIdentifier = Information sur le justificatif d'identité de l'établissement du porteur** locality = ville où se trouve l'établissement du porteur commonName = prénom1(,prénom2,prénom3,…)[10] nom serialNumber[11] title = le cas échéant, fonction du porteur au sein de sa structure serialNumber = numéro séquentiel de 4 chiffres permettant de traiter les cas d'homonymie[12] (givenName et surname ne sont pas utilisés))
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

[9] Cf. chapitre 2.2

[10] Les différents prénoms sont mentionnés dans l'ordre indiqué sur la pièce d'identité présentée lors de l'enregistrement et dont la copie est conservée dans le dossier d'enregistrement.

[11] Cf. la note de bas de page n° 7. Cette valeur serialNumber n'est pas renseignée dans le commonName lorsqu'elle est 0001.

[12] 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.

Identifiant national de la structure :

- Pour les entités basées en France Métropolitaine et les DOM : 0002 <<N° SIRET sur 14 caractère>>
- Pour les entités basées en Nouvelle-Calédonie : S540 <<N° RIDET sur 9 caractères maximum>>
- Pour les autres entités basées dans un pays de la communauté européenne : S<<code ISO3166-1 du pays sur 3 chiffres>> <<n° de TVA intracommunautaire sur 14 caractères maximum>>[13]

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 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*RGS - eiDAS* digitalSignature, contentCommitment
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.
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse mél du porteur
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
CRL Distribution Points	Non	distributionPoint = uniformResourceIndicator (IA5String) du téléchargement de la LCR correspondant au niveau du certificat porteur e (CRL binaire et LDAP). reasons et cRLIssuer ne sont pas utilisés
Authority Information Access	**Non**	**caIssuers = http://autorite.chambersign.fr/rgs2eidas.der**
Qualified Certificate Statements	**Non**	**id-etsi-qcs-QcCompliance QcEuPDS : http://pc.chambersign.fr/rgs2Seidas/ id-etsi-qct-esign**
Basic Constraints	**Non**	**cA=False**

[13] Exemple pour une structure basée en Allemagne : OU = S276 DE123456789

3.3 Certificats 3*

3.3.1 RGS authentification

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 433702479 commonName = ChamberSign France - <<type et niveau>>[14]
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject	DN encodé en UTF8String countryName = code ISO sur 2 lettres (cf. ISO3166-1) du pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère,…) organizationName = nom officiel de l'entité (dénomination sociale du siège social) organizationalUnitName = identifiant national de la structure, cf. ci-dessous. organizationalUnitName = le cas échéant, dénomination de l'établissement du porteur, ne commençant ni par 4 chiffres ni par un « S » suivi de 3 chiffres organizationalUnitName = le cas échéant, nom du service où travaille le porteur au sein de sa structure, ne commençant ni par 4 chiffres ni par un « S » suivi de 3 chiffres locality = ville où se trouve l'établissement du porteur commonName = prénom1(,prénom2,prénom3,…)[15] nom serialNumber[16] title = le cas échéant, fonction du porteur au sein de sa structure serialNumber = numéro séquentiel de 4 chiffres permettant de traiter les cas d'homonymie[17] (givenName et surname ne sont pas utilisés))
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

[14] Cf. chapitre 2.2

[15] Les différents prénoms sont mentionnés dans l'ordre indiqué sur la pièce d'identité présentée lors de l'enregistrement et dont la copie est conservée dans le dossier d'enregistrement.

[16] Cf. la note de bas de page n° 17. Cette valeur serialNumber n'est pas renseignée dans le commonName lorsqu'elle est 0001.

[17] 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.

Identifiant national de la structure :

- Pour les entités basées en France Métropolitaine et les DOM : 0002 <<N° SIRET sur 14 caractère>>
- Pour les entités basées en Nouvelle-Calédonie : S540 <<N° RIDET sur 9 caractères maximum>>
- Pour les autres entités basées dans un pays de la communauté européenne : S<<code ISO3166-1 du pays sur 3 chiffres>> <<n° de TVA intracommunautaire sur 14 caractères maximum>>[18]

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	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.
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse mél du porteur 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	- 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 niveau du certificat porteur e (CRL binaire et LDAP). reasons et cRLIssuer ne sont pas utilisés
Authority Information Access	Non	accessMethod = id-ad-ocsp accessLocation = uniformResourceIndicator (IA5String) du serveur OCSP : http://ocsp.chambersign.fr
Qualified Certificate Statements	Non	*Uniquement pour les certificats signature 3** id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD

[18] Exemple pour une structure basée en Allemagne : OU = S276 DE123456789

3.3.2 Eidas Qualifié Signature

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 433702479 commonName = ChamberSign France - <<type et niveau>>[19]
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject	DN encodé en UTF8String countryName = code ISO sur 2 lettres (cf. ISO3166-1) du pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère,…) organizationName = nom officiel de l'entité (dénomination sociale du siège social) organizationalUnitName = identifiant national de la structure, cf. ci-dessous. organizationalUnitName = le cas échéant, dénomination de l'établissement du porteur, ne commençant ni par 4 chiffres ni par un « S » suivi de 3 chiffres organizationalUnitName = le cas échéant, nom du service où travaille le porteur au sein de sa structure, ne commençant ni par 4 chiffres ni par un « S » suivi de 3 chiffres **OrganizationIdentifier = Information sur le justificatif d'identité de l'établissement du porteur** locality = ville où se trouve l'établissement du porteur commonName = prénom1(,prénom2,prénom3,…)[20] nom serialNumber[21] title = le cas échéant, fonction du porteur au sein de sa structure serialNumber = numéro séquentiel de 4 chiffres permettant de traiter les cas d'homonymie[22] (givenName et surname ne sont pas utilisés))
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

[19] Cf. chapitre 2.2
[20] Les différents prénoms sont mentionnés dans l'ordre indiqué sur la pièce d'identité présentée lors de l'enregistrement et dont la copie est conservée dans le dossier d'enregistrement.
[21] Cf. la note de bas de page n° 17. Cette valeur serialNumber n'est pas renseignée dans le commonName lorsqu'elle est 0001.
[22] 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.

Identifiant national de la structure :

- Pour les entités basées en France Métropolitaine et les DOM : 0002 <<N° SIRET sur 14 caractère>>
- Pour les entités basées en Nouvelle-Calédonie : S540 <<N° RIDET sur 9 caractères maximum>>
- Pour les autres entités basées dans un pays de la communauté européenne : S<<code ISO3166-1 du pays sur 3 chiffres>> <<n° de TVA intracommunautaire sur 14 caractères maximum>>[23]

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	nonRepudiation
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.
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse mél du porteur
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
CRL Distribution Points	Non	distributionPoint = uniformResourceIndicator (IA5String) du téléchargement de la LCR correspondant au niveau du certificat porteur e (CRL binaire et LDAP). reasons et cRLIssuer ne sont pas utilisés
Authority Information Access	Non	accessMethod = id-ad-ocsp accessLocation = uniformResourceIndicator (IA5String) du serveur OCSP : http://ocsp.chambersign.fr
Qualified Certificate Statements	Non	*Uniquement pour les certificats signature 3** id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD
Authority Information Access	**Non**	**calssuers = http://autorite.chambersign.fr/rgs3eidas.der**
Qualified Certificate Statements	**Non**	**id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD QcEuPDS : http://pc.chambersign.fr/rgs3Seidas/ id-etsi-qct-esign**
Basic Constraints	**Non**	**cA=False**

[23] Exemple pour une structure basée en Allemagne : OU = S276 DE123456789

4 Certificats de cachet et d'authentification serveur 1*

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 433702479 commonName = ChamberSign France - <<type et niveau>>[24]
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject	DN encodé en UTF8String countryName = code ISO sur 2 lettres (cf. ISO3166-1) du pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée (tribunal de commerce, ministère,…) organizationName = nom officiel de l'entité (dénomination sociale du siège social) organizationalUnitName = identifiant national de la structure, cf. ci-dessous. organizationalUnitName = le cas échéant, dénomination de l'établissement du serveur, ne commençant ni par 4 chiffres ni par un « S » suivi de 3 chiffres organizationalUnitName = le cas échéant, nom du service du serveur au sein de la structure, ne commençant ni par 4 chiffres ni par un « S » suivi de 3 chiffres locality = ville où se trouve l'établissement du service proposé commonName = FQDN du service serialNumber[25] serialNumber = numéro séquentiel de 4 chiffres permettant de traiter les cas d'homonymie[26] (givenName et surname ne sont pas utilisés)
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Identifiant national de la structure :

- Pour les entités basées en France Métropolitaine et les DOM : 0002 <<N° SIRET sur 14 caractère>>
- Pour les entités basées en Nouvelle-Calédonie : S540 <<N° RIDET sur 9 caractères maximum>>

[24] Cf. chapitre 2.2

[25] Cf. la note de bas de page n° 7. Cette valeur serialNumber n'est pas renseignée dans le commonName lorsqu'elle est 0001.

[26] 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.

- Pour les autres entités basées dans un pays de la communauté européenne : S<<code ISO3166-1 du pays sur 3 chiffres>> <<n° de TVA intracommunautaire sur 14 caractères maximum>>[27]

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 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	*Cachet serveur signature et courriel 1* :* contentCommitment, digitalSignature *Cachet serveur authentification 1* :* digitalSignature,
Certificate Policies	Non	policyIdentifier = OID de la PC correspondant au type de certificat policyQualifiers = - CPSuri (IA5String) = URI du téléchargement de la PC correspondant au type de certificat.
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du service
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
Extended key usage	Non	*Cachet serveur authentification SSL/TLS 1* :* id-kp-clientAuth

[27] Exemple pour une structure basée en Allemagne : OU = S276 DE123456789

5 Listes de certificats révoqués

5.1 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 433702479 commonName = ChamberSign France
This Update	Date de début de validité de la LAR au format UTCTime
Next Update	Date de début de validité au plus tard de la prochaine LAR au format UTCTime (= *This Update* + 365j) Si la clé de l'AC émettrice du certificat est sur le point d'expirer, une dernière LCR est publiée ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s
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 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
Expired Certs on CRL	Non	GeneralizedTime ? (X509)

5.2 LCR

5.2.1 AC Intermédiaire 2* et 3*

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 433702479 commonName = ChamberSign France - <<type et niveau>>[28]
This Update	Date de génération de la LCR au format UTCTime
Next Update	Date de génération au plus tard de la prochaine LCR au format UTCTime (= *This Update* + 96h) Si la clé de l'AC émettrice du certificat est sur le point d'expirer, une dernière LCR est publiée ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s
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 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

5.2.2 Autres AC intermédiaire

Champ	Valeur
Version	1
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits

[28] Cf. chapitre 2.2

Champ	Valeur
Issuer	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName 0002 433702479 commonName = ChamberSign France - <<type et niveau>>[29]
This Update	Date de génération de la LCR au format UTCTime
Next Update	Date de génération au plus tard de la prochaine LCR au format UTCTime (= *This Update* + 96h) Si la clé de l'AC émettrice du certificat est sur le point d'expirer, une dernière LCR est publiée ayant une fin de validité positionnée au 31 décembre 9999, 23h59m59s
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 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
Expired Certs on CRL	Non	GeneralizedTime ? (X509)

[29] Cf. chapitre 2.2

6 Nommage de la hiérarchie

6.1 OID

Abréviation		OID	OID des PC	
ACR		1.2.250.1.96.1.7	*1.2.250.1.96.1.7*	
	AC 1 étoile	1.2.250.1.96.1.7.3	*Sign*	*1.2.250.1.96.1.7.3.1.2*
			Auth	*1.2.250.1.96.1.7.3.2.2*
			Sign-Auth	*1.2.250.1.96.1.7.3.3.2*
	AC 2 étoiles	1.2.250.1.96.1.7.2	*Sign*	*1.2.250.1.96.1.7.2.1.2*
			Auth	*1.2.250.1.96.1.7.2.2.2*
			Sign-Auth	*1.2.250.1.96.1.7.2.3.2*
	AC 3 étoiles	1.2.250.1.96.1.7.1	*Sign*	*1.2.250.1.96.1.7.1.1.2*
			Auth	*1.2.250.1.96.1.7.1.2.2*
	AC cachet 1 étoile	1.2.250.1.96.1.7.4	*SSL auth*	*1.2.250.1.96.1.7.4.1.2*
			Srv Sign-Auth	*1.2.250.1.96.1.7.4.2.2*

6.2 Noms communs des AC Filles

Abréviation	Nom Commun
AC 1 étoile	ChamberSign France – AC 1 étoile
AC 2 étoiles	ChamberSign France – AC 2 étoiles
AC 3 étoiles	ChamberSign France – AC 3 étoiles
AC cachet 1 étoile	ChamberSign France – Cachet 1 étoile