

# Profils de Certificats et de LCR

**AC ChamberSign France**



<b>Objet du document :</b>	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 ».
<b>Version</b>	03
<b>Date de diffusion</b>	12/05/2017

## SOMMAIRE

<b>1</b>	<b>INTRODUCTION.....</b>	<b>4</b>
1.1	OBJET DU DOCUMENT.....	4
1.2	DOCUMENTS DE REFERENCE .....	5
<b>2</b>	<b>CERTIFICATS D'AC.....</b>	<b>6</b>
2.1	AC RACINE.....	6
2.2	AC INTERMEDIAIRES.....	7
2.3	AC INTERMEDIAIRE 3* – SIGNATURE DE REPONSES OCSP .....	8
<b>3</b>	<b>CERTIFICATS DE PORTEURS .....</b>	<b>10</b>
3.1	CERTIFICATS 1* ET 2* RGS .....	10
3.2	CERTIFICAT 2* RGS ET EIDAS .....	13
3.3	CERTIFICATS 3* .....	15
3.3.1	<i>RGS authentication</i> .....	15
3.3.2	<i>Eidas Qualifié Signature</i> .....	17
<b>4</b>	<b>CERTIFICATS DE CACHET ET D'AUTHENTIFICATION SERVEUR 1*.....</b>	<b>19</b>
<b>5</b>	<b>LISTES DE CERTIFICATS REVOQUES .....</b>	<b>21</b>
5.1	LAR .....	21
5.2	LCR.....	22
5.2.1	<i>AC Intermédiaire 2* et 3*</i> .....	22
5.2.2	<i>Autres AC intermédiaire</i> .....	22
<b>6</b>	<b>NOMMAGE DE LA HIERARCHIE.....</b>	<b>24</b>
6.1	OID.....	24
6.2	NOMS COMMUNS DES AC FILLES .....	24

## Avertissement

Le présent document est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1<sup>er</sup> juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de **CHAMBERSIGN FRANCE**. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par **CHAMBERSIGN FRANCE** ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'article L.122-5, d'une part, que « *les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective* » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « *toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite* » (article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

Le présent document, propriété de **CHAMBERSIGN FRANCE**, peut être concédée par des accords de licence à toutes entités privées ou publiques qui souhaiteraient l'utiliser dans le cadre de leurs propres services de certification.

# 1 Introduction

## 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 signée. 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
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 4096 bits
<i>Issuer</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (notBefore + 20 ans)
<i>Subject</i>	Identique à <i>Issuer</i>
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 4096 bits
<i>Unique Identifiers</i>	Vide (non utilisé)
<i>Extensions</i>	Cf. tableau suivant

Extension	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de ce certificat authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
<i>Subject Key Identifier</i>	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de ce certificat
<i>Key Usage</i>	Oui	keyCertSign, cRLSign
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.7 policyQualifiers = CPSuri (IA5String) = <a href="http://pc.chambersign.fr/rgs/lcr-directes/">http://pc.chambersign.fr/rgs/lcr-directes/</a>
<i>Basic Constraints</i>	Oui	cA = TRUE pathLenConstraint = 1

## 2.2 AC Intermédiaires

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 4096 bits
<i>Issuer</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France
<i>Validity</i>	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
<i>Subject</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France - <<type et niveau>> <sup>1</sup>
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 4096 bits
<i>Unique Identifiers</i>	Vide (non utilisé)
<i>Extensions</i>	Cf. tableau suivant

Extension	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de l'AC Racine authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
<i>Subject Key Identifier</i>	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de ce certificat
<i>Key Usage</i>	Oui	keyCertSign, cRLSign
<i>Certificate Policies</i>	Non	policyIdentifier = OID de la PC « certificats d'ACR » policyQualifiers = CPSuri (IA5String) = URI du téléchargement de la PC « certificats d'AC »
<i>Basic Constraints</i>	Oui	cA = TRUE pathLenConstraint = 0
<i>CRL Distribution Points</i>	Non	distributionPoint = <a href="http://crl.chambersign.fr/crl/rgs/lcr-directes/chambersign-france.crl">http://crl.chambersign.fr/crl/rgs/lcr-directes/chambersign-france.crl</a> (URL du téléchargement de la LAR ) reasons et cRLIssuer ne sont pas utilisés

<sup>1</sup> « AC 3 étoiles », « AC 2 étoiles », « AC 1 étoile »

### 2.3 AC Intermédiaire 3\* – Signature de réponses OCSP

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

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 4096 bits
<i>Issuer</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France - <<type et niveau>> <sup>2</sup>
<i>Validity</i>	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
<i>Subject</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France - <<type et niveau>> <sup>3</sup> - OCSP
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 4096 bits
<i>Unique Identifiers</i>	Vide (non utilisé)
<i>Extensions</i>	Cf. tableau suivant

Extension	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de l'AC intermédiaire correspondante authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
<i>Subject Key Identifier</i>	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de ce certificat
<i>Key Usage</i>	Oui	digitalSignature
<i>Certificate Policies</i>	Non	policyIdentifier = OID de la PC « certificats d'AC » policyQualifiers = CPSuri (IA5String) = URI du téléchargement de la PC « certificats d'AC »
<i>Extended Key Usage</i>	Non	id-kp-OCSPSigning (cf. RFC5280)

<sup>2</sup> Cf. chapitre 2.2

<sup>3</sup> « AC 3étoiles », « AC 2étoiles », « AC 1étoile »,



Extension	Criticité	Valeur
<i>CRL Distribution Points</i>	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

PROJET

### 3 Certificats de porteurs

#### 3.1 Certificats 1\* et 2\* RGS

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
<i>Issuer</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France - <<type et niveau>> <sup>4</sup>
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject</i>	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,...) <sup>5</sup> nom serialNumber <sup>6</sup> 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 <sup>7</sup> (givenName et surname ne sont pas utilisés))
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
<i>Unique Identifiers</i>	Vide (non utilisé)
<i>Extensions</i>	Cf. tableau suivant

<sup>4</sup> Cf. chapitre 2.2

<sup>5</sup> 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.

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

<sup>7</sup> 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>><sup>8</sup>

Extension	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de l'AC Intermédiaire correspondante authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
<i>Subject Key Identifier</i>	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de ce certificat
<i>Key Usage</i>	Oui	<u>Signature et authentification 1* et 2*</u> : digitalSignature, contentCommitment <u>Signature 1* et 2*</u> : contentCommitment <u>Authentification 1* et 2*</u> : digitalSignature
<i>Certificate Policies</i>	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.
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse mél du porteur <u>Pour les certificats d'authentification mono-usage uniquement</u> : 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)
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
<i>Extended key usage</i>	Non	<u>Pour les certificats d'authentification mono-usage uniquement</u> : - 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)
<i>CRL Distribution Points</i>	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

<sup>8</sup> Exemple pour une structure basée en Allemagne : OU = S276 DE123456789

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

PROJET

### 3.2 Certificat 2\* RGS et eiDAS

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
<i>Issuer</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France - <<type et niveau>> <sup>9</sup>
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject</i>	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 <b>OrganizationIdentifier = Information sur le justificatif d'identité de l'établissement du porteur</b> locality = ville où se trouve l'établissement du porteur commonName = prénom1(,prénom2,prénom3,...) <sup>10</sup> nom serialNumber <sup>11</sup> 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 <sup>12</sup> (givenName et surname ne sont pas utilisés))
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
<i>Unique Identifiers</i>	Vide (non utilisé)
<i>Extensions</i>	Cf. tableau suivant

<sup>9</sup> Cf. chapitre 2.2

<sup>10</sup> 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.

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

<sup>12</sup> 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>><sup>13</sup>

Extension	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de l'AC Intermédiaire correspondante authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
<i>Subject Key Identifier</i>	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de ce certificat
<i>Key Usage</i>	Oui	<u><i>Signature et authentification 2*RGS - eIDAS</i></u> digitalSignature, contentCommitment
<i>Certificate Policies</i>	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.
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse mél du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
<i>CRL Distribution Points</i>	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
<b><i>Authority Information Access</i></b>	<b>Non</b>	<b>caIssuers =</b> <b>http://autorite.chambersign.fr/rgs2eidass.der</b>
<b><i>Qualified Certificate Statements</i></b>	<b>Non</b>	<b>id-etsi-qcs-QcCompliance</b> <b>QcEuPDS : http://pc.chambersign.fr/rgs2Seidas/</b> <b>id-etsi-qct-esign</b>
<b><i>Basic Constraints</i></b>	<b>Non</b>	<b>cA=False</b>

<sup>13</sup> Exemple pour une structure basée en Allemagne : OU = S276 DE123456789

### 3.3 Certificats 3\*

#### 3.3.1 RGS authentification

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
<i>Issuer</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France - <<type et niveau>> <sup>14</sup>
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject</i>	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,...) <sup>15</sup> nom serialNumber <sup>16</sup> 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 <sup>17</sup> (givenName et surname ne sont pas utilisés)
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
<i>Unique Identifiers</i>	Vide (non utilisé)
<i>Extensions</i>	Cf. tableau suivant

<sup>14</sup> Cf. chapitre 2.2

<sup>15</sup> 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.

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

<sup>17</sup> 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>><sup>18</sup>

Extension	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de l'AC Intermédiaire correspondante (CertSign) authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
<i>Subject Key Identifier</i>	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de ce certificat
<i>Key Usage</i>	Oui	digitalSignature
<i>Certificate Policies</i>	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.
<i>Subject Alternative Name</i>	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)
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
<i>Extended key usage</i>	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)
<i>CRL Distribution Points</i>	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
<i>Authority Information Access</i>	Non	accessMethod = id-ad-ocsp accessLocation = uniformResourceIndicator (IA5String) du serveur OCSP : <a href="http://ocsp.chambersign.fr">http://ocsp.chambersign.fr</a>
<i>Qualified Certificate Statements</i>	Non	<u>Uniquement pour les certificats signature 3*</u> id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD

<sup>18</sup> Exemple pour une structure basée en Allemagne : OU = S276 DE123456789



### 3.3.2 Eidas Qualifié Signature

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
<i>Issuer</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France - <<type et niveau>> <sup>19</sup>
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject</i>	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 <b>OrganizationIdentifier = Information sur le justificatif d'identité de l'établissement du porteur</b> locality = ville où se trouve l'établissement du porteur commonName = prénom1(,prénom2,prénom3,...) <sup>20</sup> nom serialNumber <sup>21</sup> 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 <sup>22</sup> (givenName et surname ne sont pas utilisés))
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
<i>Unique Identifiers</i>	Vide (non utilisé)
<i>Extensions</i>	Cf. tableau suivant

<sup>19</sup> Cf. chapitre 2.2

<sup>20</sup> 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.

<sup>21</sup> Cf. la note de bas de page n° 17. Cette valeur serialNumber n'est pas renseignée dans le commonName lorsqu'elle est 0001.

<sup>22</sup> 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>><sup>23</sup>

Extension	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de l'AC Intermédiaire correspondante (CertSign) authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
<i>Subject Key Identifier</i>	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de ce certificat
<i>Key Usage</i>	Oui	nonRepudiation
<i>Certificate Policies</i>	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.
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse mél du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
<i>CRL Distribution Points</i>	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
<i>Authority Information Access</i>	Non	accessMethod = id-ad-ocsp accessLocation = uniformResourceIndicator (IA5String) du serveur OCSP : <a href="http://ocsp.chambersign.fr">http://ocsp.chambersign.fr</a>
<i>Qualified Certificate Statements</i>	Non	<u>Uniquement pour les certificats signature 3*</u> id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD
<b><i>Authority Information Access</i></b>	<b>Non</b>	<b>calssuers =</b> <b><a href="http://autorite.chambersign.fr/rgs3eidas.der">http://autorite.chambersign.fr/rgs3eidas.der</a></b>
<b><i>Qualified Certificate Statements</i></b>	<b>Non</b>	<b>id-etsi-qcs-QcCompliance</b> <b>id-etsi-qcs-QcSSCD</b> <b>QcEuPDS : <a href="http://pc.chambersign.fr/rgs3eidas/">http://pc.chambersign.fr/rgs3eidas/</a></b> <b>id-etsi-qct-esign</b>
<b><i>Basic Constraints</i></b>	<b>Non</b>	<b>cA=False</b>

<sup>23</sup> Exemple pour une structure basée en Allemagne : OU = S276 DE123456789

#### 4 Certificats de cachet et d'authentification serveur 1\*

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
<i>Issuer</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France - <<type et niveau>> <sup>24</sup>
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject</i>	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 <sup>25</sup> serialNumber = numéro séquentiel de 4 chiffres permettant de traiter les cas d'homonymie <sup>26</sup> (givenName et surname ne sont pas utilisés)
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048 bits
<i>Unique Identifiers</i>	Vide (non utilisé)
<i>Extensions</i>	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>>

<sup>24</sup> Cf. chapitre 2.2

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

<sup>26</sup> 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>><sup>27</sup>

Extension	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de l'AC Intermédiaire correspondante authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
<i>Subject Key Identifier</i>	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de ce certificat
<i>Key Usage</i>	Oui	<u>Cachet serveur signature et courriel 1*</u> : contentCommitment, digitalSignature <u>Cachet serveur authentification 1*</u> : digitalSignature,
<i>Certificate Policies</i>	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.
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du service
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
<i>Extended key usage</i>	Non	<u>Cachet serveur authentification SSL/TLS 1*</u> : id-kp-clientAuth

<sup>27</sup> Exemple pour une structure basée en Allemagne : OU = S276 DE123456789

## 5 Listes de certificats révoqués

### 5.1 LAR

Champ	Valeur
<i>Version</i>	1
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
<i>Issuer</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName = 0002 433702479 commonName = ChamberSign France
<i>This Update</i>	Date de début de validité de la LAR au format UTCTime
<i>Next Update</i>	Date de début de validité au plus tard de la prochaine LAR au format UTCTime (= <i>This Update</i> + 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
<i>Revoked Certificates</i>	- userCertificate : <i>Serial Number</i> du certificat d'AC révoqué - revocationDate : date de révocation du certificat au format UTCTime - crlEntryExtensions : aucune extension d'entrée n'est utilisée
<i>Extensions</i>	Cf. tableau ci-dessous

Extension de LCR	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de l'AC Racine authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
<i>CRL Number</i>	Non	Nombre entier séquentiel, codé sur 20 octets
<i>Expired Certs on CRL</i>	Non	GeneralizedTime ? (X509)

## 5.2 LCR

### 5.2.1 AC Intermédiaire 2\* et 3\*

Champ	Valeur
<i>Version</i>	1
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
<i>Issuer</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName 0002 433702479 commonName = ChamberSign France - <<type et niveau>> <sup>28</sup>
<i>This Update</i>	Date de génération de la LCR au format UTCTime
<i>Next Update</i>	Date de génération au plus tard de la prochaine LCR au format UTCTime (= <i>This Update</i> + 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
<i>Revoked Certificates</i>	- userCertificate : <i>Serial Number</i> du certificat porteur révoqué - revocationDate : date de révocation du certificat au format UTCTime - crlEntryExtensions : aucune extension d'entrée n'est utilisée
<i>Extensions</i>	Cf. tableau ci-dessous

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

### 5.2.2 Autres AC intermédiaire

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

<sup>28</sup> Cf. chapitre 2.2

Champ	Valeur
<i>Issuer</i>	DN encodé en UTF8String countryName = FR organizationName = ChamberSign France organizationalUnitName 0002 433702479 commonName = ChamberSign France - <<type et niveau>> <sup>29</sup>
<i>This Update</i>	Date de génération de la LCR au format UTCTime
<i>Next Update</i>	Date de génération au plus tard de la prochaine LCR au format UTCTime (= <i>This Update</i> + 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
<i>Revoked Certificates</i>	- userCertificate : <i>Serial Number</i> du certificat porteur révoqué - revocationDate : date de révocation du certificat au format UTCTime - crlEntryExtensions : aucune extension d'entrée n'est utilisée
<i>Extensions</i>	Cf. tableau ci-dessous

Extension de LCR	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ <i>Subject Public Key Info</i> de l'AC Intermédiaire correspondante authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
<i>CRL Number</i>	Non	Nombre entier séquentiel, codé sur 20 octets
<i>Expired Certs on CRL</i>	Non	GeneralizedTime ? (X509)

---

<sup>29</sup> 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