

Profils de Certificats et de LCR

ChamberSign France CA3



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 CA3 ».
Version	19
Date de diffusion	11/06/2024

Rédigé par responsable d'application	
Vérifié par responsable qualité et sécurité	
Approuvé par le directeur général	

Les informations concernant les AC intermédiaires Chambersign France CA3 RGS, ChamberSign France CA3 Qualified eID, Chambersign France CA3 Standard eID, ChamberSign France CA3 Website, ChamberSign France CA3 Timestamp, ChamberSign France CA3 CEV sont disponibles sur le document [GUI ACC 11 Profils des certificats] en version 08 (ancienne chaîne d'AC).

AVERTISSEMENT	4
1 INTRODUCTION.....	5
1.1 OBJET DU DOCUMENT	5
1.2 DOCUMENTS DE REFERENCE	7
2 CERTIFICATS D'AC.....	8
2.1 AC RACINE	8
2.2 AC INTERMEDIAIRES.....	9
3 VARIABLES UTILISEES DANS LES PROFILS DE CERTIFICATS.....	10
4 CERTIFICATS FINAUX AC « CHAMBERSIGN FRANCE CA3 NG RGS ».....	12
4.1 CERTIFICATS D'AUTHENTIFICATION * RGS PERSONNE PHYSIQUE	12
4.2 CERTIFICATS D'AUTHENTIFICATION ** RGS PERSONNE PHYSIQUE	14
4.3 CERTIFICATS D'AUTHENTIFICATION *** RGS PERSONNE PHYSIQUE	16
4.4 CERTIFICATS DE SIGNATURE * RGS PERSONNE PHYSIQUE	18
4.5 CERTIFICATS DE SIGNATURE ** RGS PERSONNE PHYSIQUE	20
4.6 CERTIFICATS DE SIGNATURE *** RGS PERSONNE PHYSIQUE.....	22
4.7 CERTIFICATS D'AUTHENTIFICATION ET DE SIGNATURE * RGS PERSONNE PHYSIQUE	24
4.8 CERTIFICATS D'AUTHENTIFICATION ET DE SIGNATURE ** RGS PERSONNE PHYSIQUE.....	26
4.9 CERTIFICATS DE PERSONNE MORALE 1*.....	28
4.10 CERTIFICATS D'AUTHENTIFICATION PERSONNE MORALE CLIENT/SERVEUR 1*	30
4.11 CERTIFICATS DE PERSONNE MORALE 2*	32
4.12 CERTIFICATS D'AUTHENTIFICATION DE PERSONNE MORALE CLIENT/SERVEUR 2*	34
5 CERTIFICATS FINAUX AC « CHAMBERSIGN FRANCE CA3 NG QUALIFIED EID »	36
5.1 CERTIFICATS DE SIGNATURE QUALIFIES EIDAS PERSONNE PHYSIQUE	36
5.2 CERTIFICATS D'AUTHENTIFICATION ET DE SIGNATURE QUALIFIES EIDAS PERSONNE PHYSIQUE	38
5.3 CERTIFICATS DE SIGNATURE QUALIFIES EIDAS PERSONNE PHYSIQUE AVEC QSCD	40
5.4 CERTIFICATS DE CACHET QUALIFIES EIDAS PERSONNE MORALE	42
5.5 CERTIFICATS DE CACHET QUALIFIES EIDAS PERSONNE MORALE AVEC QSCD	44
5.6 CERTIFICATS WEB QUALIFIES EIDAS PERSONNE MORALE - QWAC	46
5.7 CERTIFICATS DE CACHET 2D-DOC PERSONNE MORALE	48
5.8 CERTIFICATS D'AUTHENTIFICATION ET DE SIGNATURE QUALIFIES EIDAS PERSONNE PHYSIQUE AVEC QSCD50	
5.9 CERTIFICATS DE SIGNATURE QUALIFIES EIDAS PERSONNE PHYSIQUE AVEC QSCD DUREE VARIABLE 52	
6 CERTIFICATS FINAUX AC « CHAMBERSIGN FRANCE CA3 NG STANDARD EID »	54
6.1 CERTIFICATS LCP ETSI PERSONNE PHYSIQUE	54
.....	55
6.2 CERTIFICATS NCP ETSI PERSONNE PHYSIQUE.....	56
6.3 CERTIFICATS NCP+ ETSI PERSONNE PHYSIQUE	58
6.4 CERTIFICATS LCP ETSI PERSONNE MORALE	60
6.5 CERTIFICATS NCP ETSI PERSONNE MORALE	62
7 CERTIFICATS FINAUX AC « CHAMBERSIGN FRANCE CA3 NG WEBSITE »	64
7.1 CERTIFICATS OVCP ETSI	64
7.2 CERTIFICATS EVCP ETSI	66
8 CERTIFICATS FINAUX AC « CHAMBERSIGN FRANCE CA3 NG TIMESTAMP »	68
8.1 CERTIFICATS DE CACHET HORODATAGE PERSONNE MORALE.....	68
9 CERTIFICATS FINAUX AC « CHAMBERSIGN FRANCE CA3 NG CEV »	70
9.1 CERTIFICATS DE CACHET 2D-DOC PERSONNE MORALE	70
10 LISTES DE CERTIFICATS REVOQUES.....	72

10.1	LAR.....	72
10.2	LCR	73
11	OCSP.....	74
11.1	CERTIFICATS DU SERVICE OCSP	74
11.2	REPONDEUR OCSP	76
11.2.1	REQUETES OCSP	76
11.2.2	REPONSES OCSP	76
12	NOMMAGE DE LA HIERARCHIE	77

Avertissement

Le présent document est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1^{er} 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.

À juste titre, aux termes de l'article L.122-4 du Code de la Propriété Intellectuelle, « *toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayant cause est illicite* ».

Par exception, le Code de la Propriété Intellectuelle autorise, aux termes de l'article L.122-5 dudit Code, d'une part, que « *les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective* » ; d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration.

La représentation ou la 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 « CHAMBERSIGN FRANCE CA3 ». 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, les certificats SSL et pour les certificats techniques des différentes AC et d'horodatage de la hiérarchie.

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



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 branche correspondante, pour signer les LCR (listes de certificats révoqués) des certificats de la branche correspondante et signer les certificats des répondeurs OCSP correspondants.

1.2 Documents de référence

Renvoi	Document
[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 319 412-2]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[ETSI EN 319 412-3]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[ETSI EN 319 412-4]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations
[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
[RFC6960]	RFC6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[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
[PSCE_RGS_EIDAS]	Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet Critères d'évaluation de la conformité au règlement eIDAS
[CAB_FORUM_B]	https://cabforum.org/baseline-requirements-documents/
[CAB_FORUM_E]	https://cabforum.org/extended-validation/

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>	CN=ChamberSign France CA3 Root orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<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

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 Dans le contexte d'un certificat racine, <i>Authority Key Identifier</i> = <i>Subject Key Identifier</i> Note : pour le certificat racine, AKI et SKI sont identiques.
<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>Basic Constraints</i>	Oui	cA = TRUE

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-PKCS1avec une longueur de clé de 4096 bits
<i>Issuer</i>	CN=ChamberSign France CA3 Root orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<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>	CN=[COMMON_NAME_AC] orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<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 = anyPolicy
<i>Basic Constraints</i>	Oui	cA = TRUE
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_Root.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_Root.crl
<i>Authority Information Access</i>	Non	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Root.cer

3 Variables utilisées dans les profils de certificats

Nom du champ	Contenu du champ
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 - Pour les entités immatriculées en France Métropolitaine et les DROM : 0002 <<N° SIRET sur 14 caractères>> - 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>> Le champ peut être itéré 3 fois
organizationIdentifier	Numéro d'immatriculation officiel du porteur ou du responsable de certificat conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « SI:FR- » suivi du numéro SIREN ou SIRET Identifiant de l'entité avec laquelle le porteur est en lien - VAT<code pays>-<numéro de TVA intracommunautaire> - NTR<code pays>-<numéro de SIREN> - LEI<code LEI conforme ISO17442> - PSD<numéro national de référence de fournisseur de service de paiement> Note LEI : Le code pays à deux caractères ISO 3166-1 est positionné à XG Note PSD : La structure des données est celle définie dans ETSI TS 119 495, § 5.2.1 en relation avec la Directive sur les Services des Paiements (EU) 2015/2366
locality	Ville où se trouve l'établissement du porteur
surName	Nom du porteur
givenName	Prénom1(,Prénom2,Prénom3,...) Les différents prénoms sont mentionnés dans l'ordre indiqué lors de l'enregistrement. Lorsque plusieurs prénoms sont indiqués, ils sont concaténés et séparés par des virgules. Exemple : Michel,Paul-Auguste
commonName	- Pour les certificats personne physique correspond à la concaténation des champs givenName et surName séparés par un espace. Exemple: Pauline BIENCONNUE - Pour les certificats personne morale, correspond au nom choisi par le demandeur et qui ne doit pas avoir le format d'une personne physique. Exemple : Ma Société – Service Facturation
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 (multiples certificats pour une seule et même personne) Par défaut, la valeur de cet attribut est « 0100 ». Si un porteur dont tous les autres attributs du DN sont identiques (countryName, organizationName, organizationIdentifier, organizationalUnitName et

	commonName) a déjà été enregistré, la valeur de l'attribut serialNumber pour le nouveau porteur passe à « 0101 » et ainsi de suite. Sur la plateforme historique, le serialNumber est initialisé à « 0001 ».
Authority Key Identifier	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
Subject Key Identifier	Empreinte SHA-1 (160 bits) de la valeur subjectPublicKey du champ Subject Public Key Info du certificat
dnsName	Nom DNS des serveurs (maximum 10 itérations)

Dans les profils ci-après les valeurs des champs sont en oblique lorsque cette valeur est facultative.

4 Certificats finaux AC « ChamberSign France CA3 NG RGS »

4.1 Certificats d'authentification * RGS personne physique

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr

Extension	Criticité	Valeur
<i>Basic Constraints</i>	Oui	CA = False
<i>Key Usage</i>	Oui	digitalSignature
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.1.10 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
<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 = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS

4.2 Certificats d'authentification ** RGS personne physique

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
<i>Basic Constraints</i>	Oui	CA = False
<i>Key Usage</i>	Oui	digitalSignature

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.1.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
<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 = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS

Réserve pour un usage ultérieur

4.3 Certificats d'authentification *** RGS personne physique

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
Issuer	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 4096 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier
Subject Key Identifier	Non	keyIdentifier
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
Basic Constraints	Oui	CA = False
Key Usage	Oui	digitalSignature

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.1.2 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
<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 = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS

Réserve pour un usage ultérieur

4.4 Certificats de signature * RGS personne physique

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
<i>Basic Constraints</i>	Oui	CA = False
<i>Key Usage</i>	Oui	Non Repudiation

Réservé pour un usage ultérieur

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.1.11 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
<i>Extended key usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS

Réserve pour un usage ultérieur

4.5 Certificats de signature ** RGS personne physique

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
Issuer	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 4096 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier
Subject Key Identifier	Non	keyIdentifier
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
Basic Constraints	Oui	CA = False
Key Usage	Oui	Non Repudiation

Reservé pour un usage ultérieur

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.1.3 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
<i>Extended key usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_RGS_Signature_2etoiles.pdf

4.6 Certificats de signature *** RGS personne physique

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
Issuer	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 4096 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier
Subject Key Identifier	Non	keyIdentifier
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
Basic Constraints	Oui	CA = False
Key Usage	Oui	Non Repudiation

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.1.4 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
<i>Extended key usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_RGS_Signature_3etoiles.pdf

Réserve pour un usage ultérieur

4.7 Certificats d'authentification et de signature * RGS personne physique

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Basic Constraints</i>	Oui	CA = False
<i>Key Usage</i>	Oui	digitalSignature, nonRepudiation
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.1.5 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
<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) - 1.3.6.1.4.1.311.10.3.12 (MS Document Signing) - 1.2.840.113583.1.1.5 (Adobe PDF Signing) - 1.3.6.1.5.5.7.3.4 (EmailProtection)

Extension	Criticité	Valeur
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS

Réserve pour un usage ultérieur

4.8 Certificats d'authentification et de signature ** RGS personne physique

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
Issuer	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 4096 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier
Subject Key Identifier	Non	keyIdentifier
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
Basic Constraints	Oui	CA = False
Key Usage	Oui	digitalSignature, nonRepudiation

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.1.6 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
<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) - 1.3.6.1.4.1.311.10.3.12 (MS Document Signing) - 1.2.840.113583.1.1.5 (Adobe PDF Signing) - 1.3.6.1.5.5.7.3.4 (EmailProtection)
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_RGS_Doubleusage_2etoiles.pdf

Réservé pour un usage ultérieur

4.9 Certificats de personne morale 1*

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName = Nom du cachet serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Key Usage</i>	Oui	digitalSignature
<i>Basic Constraints</i>	Oui	CA = False
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.1.7 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
<i>Extended key usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du service

Extension	Criticité	Valeur
<i>Issuer Alternative Name</i>	Non	<i>rfc822Name (IA5String)</i> = autorite@chambersign.fr <i>uniformResourceIdentifier (IA5String)</i> = https://www.chambersign.fr
<i>CRL Distribution Points</i>	Non	<i>distributionPoint</i> = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	<i>calIssuers</i> = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer <i>Répondeur OCSP :</i> <i>accessMethod</i> = id-ad-ocsp <i>accessLocation</i> = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS <i>accessLocation</i> = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS

4.10 Certificats d'authentification personne morale client/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>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName = FQDN du service serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Key Usage</i>	Oui	digitalSignature
<i>Basic Constraints</i>	Oui	CA = False
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.1.9 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du service

Extension	Criticité	Valeur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
<i>Extended key usage</i>	Non	id-kp-clientAuth,
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS

Réserve pour un usage ultérieur

4.11 Certificats de personne morale 2*

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
Issuer	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName = Nom du cachet serialNumber
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 4096 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier
Subject Key Identifier	Non	keyIdentifier
Key Usage	Oui	digitalSignature
Basic Constraints	Oui	CA = False
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.1.8 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du service
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr

Extension	Criticité	Valeur
<i>Extended key usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_RGS_Cachet_2etoiles.pdf

Réserve pour un usage ultérieur

Réserve pour un usage ultérieur

4.12 Certificats d'authentification de personne morale client/serveur 2*

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
Issuer	CN=ChamberSign France CA3 NG RGS orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName = FQDN du service serialNumber
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 4096 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier
Subject Key Identifier	Non	keyIdentifier
Key Usage	Oui	digitalSignature
Basic Constraints	Oui	CA = False
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.1.12 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du service

Extension	Criticité	Valeur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr/
<i>Extended key usage</i>	Non	id-kp-clientAuth, id-kp-serverAuth
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_RGS accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_RGS
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_RGS_Server_auth_2etoiles.pdf

Réservé pour un usage ultérieur

5 Certificats finaux AC « ChamberSign France CA3 NG Qualified eID »

5.1 Certificats de signature qualifiés eIDAS personne physique

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG Qualified eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
<i>Basic Constraints</i>	Non	CA = False
<i>Key Usage</i>	Oui	Non Repudiation

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.2.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.pdf
<i>Extended key usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_Qualified_eID accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Qualified_eID
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance id-etsi-qct-esign QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_Qualified_eID_qcp-n.pdf

Réservé pour un usage ultérieur

5.2 Certificats d'authentification et de signature qualifiés eIDAS personne physique

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG Qualified eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 1,2 ou 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
<i>Basic Constraints</i>	Non	CA = False
<i>Key Usage</i>	Oui	digitalSignature, nonRepudiation

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.2.6 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.pdf
<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) MS Document Signing Adobe PDF Signing EmailProtection
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_Qualified_eID accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Qualified_eID
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance id-etsi-qct-esign QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_Qualified_eID_qcp-n-doubleusage.pdf

5.3 Certificats de signature qualifiés eIDAS personne physique avec QSCD

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG Qualified eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (durée variable, max 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
<i>Basic Constraints</i>	Non	CA = False
<i>Key Usage</i>	Oui	Non Repudiation

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.2.2 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.pdf
<i>Extended key usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_Qualified_eID accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Qualified_eID
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qct-esign QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_Qualified_eID_qcp-n-qscd.pdf

5.4 Certificats de cachet qualifiés eIDAS personne morale

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG Qualified eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName = Nom du cachet serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<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) = https://www.chambersign.fr
<i>Basic Constraints</i>	Non	CA = False
<i>Key Usage</i>	Oui	digitalSignature
<i>Extended Key Usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.2.3 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.pdf

Extension	Criticité	Valeur
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_Qualified_eID accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Qualified_eID
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance id-etsi-qct-eseal QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_Qualified_eID_qcp-l.pdf

5.5 Certificats de cachet qualifiés eIDAS personne morale avec QSCD

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG Qualified eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName = Nom du cachet serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	<i>rfc822Name</i> (IA5String) = Adresse de courriel du service
<i>Issuer Alternative Name</i>	Non	<i>rfc822Name</i> (IA5String) = autorite@chambersign.fr <i>uniformResourceIdentifier</i> (IA5String) = https://www.chambersign.fr
<i>Basic Constraints</i>	Non	CA = False
<i>Key Usage</i>	Oui	digitalSignature
<i>Extended Key Usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.2.4 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.pdf

Extension	Criticité	Valeur
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_Qualified_eID accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Qualified_eID
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qct-eseal QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_Qualified_eID_qcp-l-gscd.pdf

5.6 Certificats WEB qualifiés eIDAS personne morale - QWAC

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
Issuer	CN=ChamberSign France CA3 NG Qualified eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (valeur variable, max 1 an)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName = FQDN du serveur ou valeur choisie à l'enregistrement
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 4096 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier
Subject Key Identifier	Non	keyIdentifier
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du service dnsName = Un ou plusieurs noms de domaine (FQDN) serveur
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
Basic Constraints	Non	CA = False
Key Usage	Oui	digitalSignature, keyEncipherment
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.2.5 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.pdf

Extension	Criticité	Valeur
<i>Extended key usage</i>	Non	id-kp-serverAuth
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_Qualified_eID accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Qualified_eID
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance id-etsi-qct-web QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_Qualified_eID_qncp-w-gen.pdf

Réserve pour un usage ultérieur

5.7 Certificats de cachet 2D-Doc personne morale

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
Issuer	CN=ChamberSign France CA3 NG Qualified eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName = Nom du cachet serialNumber
Subject Public Key Info	algorithm = ECDSA P-256 (NIST)
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier
Subject Key Identifier	Non	keyIdentifier
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du service
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
Basic Constraints	Non	CA = False
Key Usage	Oui	digitalSignature
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.2.7 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.pdf

Extension	Criticité	Valeur
<i>Extended key usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_Qualified_eID accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Qualified_eID

Réserve pour un usage ultérieur

5.8 Certificats d'authentification et de signature qualifiés eIDAS personne physique avec QSCD

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG Qualified eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 1, 2 ou 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
<i>Basic Constraints</i>	Non	CA = False
<i>Key Usage</i>	Oui	digitalSignature, nonRepudiation

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.2.8 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.pdf
<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) MS Document Signing Adobe PDF Signing EmailProtection
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_Qualified_eID accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Qualified_eID
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qct-esign QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_Qualified_eID_qcp-n-qscd-doubleusage.pdf

5.9 Certificats de signature qualifiés eIDAS personne physique avec QSCD durée variable

Champ	Valeur
<i>Version</i>	2
<i>Serial Number</i>	Numéro unique au sein de la hiérarchie de 16 octets
<i>Signature</i>	SHA256withRSA (1.2.840.113549.1.1.11) signée par l'AC
<i>Issuer</i>	CN=ChamberSign France CA3 NG Qualified eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (valeur variable, < 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName pseudonym commonName title serialNumber NB: présence obligatoire de (surName + givenName) ou pseudonym
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
<i>Basic Constraints</i>	Non	CA = False

Extension	Criticité	Valeur
<i>Key Usage</i>	Oui	nonRepudiation
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.2.9 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.pdf
<i>Extended key usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_Qualified_eID accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Qualified_eID
<i>qcStatements</i>	Non	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qct-esign QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_Qualified_eID_qcp-n-qscd-var.pdf

6 Certificats finaux AC « ChamberSign France CA3 NG Standard eID »

1 Certificats LCP ETSI personne physique

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	CN=ChamberSign France CA3 NG Standard eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (valeur variable)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
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
Subject Key Identifier	Non	keyIdentifier
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
Basic Constraints	Oui	CA = False

Réserve pour un usage ultérieur

Extension	Criticité	Valeur
<i>Usage</i>	Oui	<u>Certificat authentification :</u> digitalSignature <u>Certificat signature :</u> nonRepudiation <u>Certificat signature et authentification :</u> digitalSignature, nonRepudiation
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.3.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Standard_eID.pdf
<i>Extended key usage</i>	Non	<u>Certificat authentification :</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) <u>Certificat signature</u> MS Document Signing Adobe PDF Signing <u>Certificat signature et authentification :</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) MS Document Signing Adobe PDF Signing
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.crl
<i>Authority Information Access</i>	Non	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.cer

Réserve pour un usage ultérieur

6.2 Certificats NCP ETSI personne physique

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>	CN=ChamberSign France CA3 NG Standard eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
<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

Extension	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
<i>Basic Constraints</i>	Oui	CA = False

Extension	Criticité	Valeur
Key Usage	Oui	<u>Certificat authentification :</u> digitalSignature <u>Certificat signature</u> nonRepudiation <u>Certificat signature et authentification :</u> digitalSignature, nonRepudiation
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.3.3 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Standard_eID.pdf
Extended key usage	Non	<u>Certificat authentification :</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) <u>Certificat signature</u> MS Document Signing Adobe PDF Signing
CRL Distribution Points	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.crl
Authority Information Access	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.cer

Réserve pour un usage ultérieur

Réserve pour un usage ultérieur

6.3 Certificats NCP+ ETSI personne physique

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>	CN=ChamberSign France CA3 NG Standard eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality surName givenName commonName title serialNumber
<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

Extension	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	rfc822Name (IA5String) = Adresse de courriel du porteur
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
<i>Basic Constraints</i>	Oui	CA = False

Extensio n	Criticité	Valeur
Key Usage	Oui	<u>Certificat authentification :</u> digitalSignature <u>Certificat signature</u> nonRepudiation <u>Certificat signature et authentification :</u> digitalSignature, nonRepudiation
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.3.5 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Standard_eID.pdf
Extended key usage	Non	<u>Certificat authentification :</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) <u>Certificat signature</u> MS Document Signing Adobe PDF Signing
CRL Distribution Points	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.crl
Authority Information Access	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.cer

Réservé pour un usage ultérieur

Réserve pour un usage ultérieur

6.4 Certificats LCP ETSI personne morale

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>	CN=ChamberSign France CA3 NG Standard eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName = Nom du cachet serialNumber
<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

Extension	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier
<i>Subject Key Identifier</i>	Non	keyIdentifier
<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) = https://www.chambersign.fr
<i>Basic Constraints</i>	Oui	CA = False
<i>Key Usage</i>	Oui	digitalSignature

Extensio n	Criticité	Valeur
<i>Extended Key Usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>Certificat e Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.3.2 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Standard_eID.pdf
<i>CRL Distributio n Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.crl
<i>Authority Informatio n Access</i>	Non	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.cer

Réservé pour un usage ultérieur

Réserve pour un usage ultérieur

6.5 Certificats NCP ETSI personne morale

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>	CN=ChamberSign France CA3 NG Standard eID orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName = Nom du cachet serialNumber
<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

Extensio n	Criticité	Valeur
<i>Authority Key Identifier</i>	Non	keyIdentifier
<i>Subject Key Identifier</i>	Non	keyIdentifier
<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) = https://www.chambersign.fr
<i>Basic Constraints</i>	Oui	CA = False
<i>Key Usage</i>	Oui	digitalSignature

Extensio n	Criticité	Valeur
<i>Extended Key Usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.3.4 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Standard_eID.pdf
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.crl
<i>Authority Information Access</i>	Non	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.cer

Réserve pour un usage ultérieur

7 Certificats finaux AC « ChamberSign France CA3 NG Website »

Certificats OVCP ETSI

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	CN=ChamberSign France CA3 NG Website orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (durée variable, <=1 an)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier commonName = FQDN du serveur
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
Subject Key Identifier	Non	keyIdentifier
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du service
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
Basic Constraints	Oui	CA = False
Key Usage	Oui	digitalSignature, keyEncipherment

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.4.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Website.pdf
<i>Subject Alternative Name</i>	Non	Un ou plusieurs noms de domaine dont le FQDN
<i>Extended Key Usage</i>	Non	id-kp-clientAuth id-kp-serverAuth
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Website.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Website.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Website.cer

Réservé pour un usage ultérieur

7.2 Certificats EVCP ETSI

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	CN=ChamberSign France CA3 NG Website orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (durée variable, <=1 an)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier businessCategory= Private Organization serialNumber localityName=Lieu d'enregistrement du subject postalCode=Code postal d'enregistrement du subject commonName = FQDN du serveur
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
Subject Key Identifier	Non	keyIdentifier
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
Basic Constraints	Oui	CA = False
Key Usage	Oui	digitalSignature, keyEncipherment

Extension	Criticité	Valeur
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.4.2 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Website.pdf policyIdentifier = 2.23.140.1.1
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du service Un ou plusieurs noms de domaine dont le FQDN
Extended Key Usage	Non	id-kp-clientAuth id-kp-serverAuth
CRL Distribution Points	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Website.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Website.crl
Authority Information Access	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Website.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_Website accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Website

8 Certificats finaux AC « ChamberSign France CA3 NG Timestamp »

8.1 Certificats de cachet horodatage personne morale

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 2048,3072, 4096 bits
<i>Issuer</i>	CN=ChamberSign France CA3 NG Timestamp orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (durée variable, < 3 ans)
<i>Subject (DN)</i>	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName serialNumber
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072 ou 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Subject Alternative Name</i>	Non	<i>rfc822Name (IA5String)</i> = Adresse de courriel du service
<i>Issuer Alternative Name</i>	Non	<i>rfc822Name (IA5String)</i> = autorite@chambersign.fr <i>uniformResourceIdentifier (IA5String)</i> = https://www.chambersign.fr
<i>Basic Constraints</i>	Oui	CA = False
<i>Key Usage</i>	Oui	digitalSignature

Extension	Criticité	Valeur
<i>Extended Key Usage</i>	Oui	id-kp-timeStamping
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.5.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Timestamp.pdf
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Timestamp.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Timestamp.crl
<i>Authority Information Access</i>	Non	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Timestamp.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_Timestamp accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_Timestamp
<i>Private Key Usage Period</i>	Non	(2.5.29.16) notBefore = date au format UTCTime notAfter = date au format UTCTime (durée variable, <2 ans)

9 Certificats finaux AC « ChamberSign France CA3 NG CEV »

Certificats de cachet 2D-Doc personne morale

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	CN=ChamberSign France CA3 NG CEV orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 3 ans)
Subject (DN)	countryName organizationName organizationalUnitName organizationalUnitName organizationalUnitName organizationIdentifier locality commonName = Nom du cachet serialNumber
Subject Public Key Info	algorithm = ECDSA P-256 (NIST)
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier
Subject Key Identifier	Non	keyIdentifier
Subject Alternative Name	Non	rfc822Name (IA5String) = Adresse de courriel du service
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
Basic Constraints	Oui	CA = False
Key Usage	Oui	digitalSignature

Extension	Criticité	Valeur
<i>Certificate Policies</i>	Non	policyIdentifier = 1.2.250.1.96.1.8.6.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_CEV.pdf
<i>Extended Key Usage</i>	Non	MS Document Signing Adobe PDF Signing
<i>Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_CEV.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_CEV.crl
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_CEV.cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/ChamberSign_France_CA3_NG_CEV accessLocation = http://ocsp-ca3.chambersign.tm.fr/ChamberSign_France_CA3_NG_CEV

10 Listes de certificats révoqués

10.1 LAR

Champ	Valeur
<i>Version</i>	1
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 4096 bits
<i>Issuer</i>	CN=ChamberSign France CA3 Root orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<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> + 364j) À la fin de vie de l'AC et avant que le certificat d'AC expire ou soit révoqué, une dernière LAR est publiée avec 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 : le Reason Code (2.5.29.21), non critique, est utilisé pour tracer la fin de vie des AC révoquées
<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) = https://www.chambersign.fr
<i>CRL Number</i>	Non	Nombre entier séquentiel, codé sur 20 octets

10.2 LCR

Champ	Valeur
<i>Version</i>	1
<i>Signature</i>	SHA256-RSA-PKCS1 avec une longueur de clé de 4096 bits
<i>Issuer</i>	CN=<Common_Name_AC> orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<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> + 4 jours [96 h]) À la fin de vie de l'AC et avant que le certificat expire ou soit révoqué, une dernière LCR est publiée avec une fin de validité positionnée au 31 décembre 9999, 23h59m59s Les LAR sont générées toutes les heures
<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
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
<i>CRL Number</i>	Non	Nombre entier séquentiel, codé sur 20 octets
<i>Expired Certs on CRL</i>	Non	GeneralizedTime (X509)

11 OCSP

11.1 Certificats du service OCSP

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>	CN=<Common_Name_AC> orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Validity</i>	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 1 ans)
<i>Subject</i>	CN=ocsp <Common_Name_AC> orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
<i>Subject Public Key Info</i>	algorithm = rsaEncryption subjectPublicKey = clé de 2048, 3072, 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
<i>Subject Key Identifier</i>	Non	keyIdentifier
<i>Issuer Alternative Name</i>	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = http://www.chambersign.fr
<i>Basic Constraints</i>	Oui	CA = False
<i>Key Usage</i>	Oui	digitalSignature
<i>Certificate Policies</i>	Non	policyIdentifier = OID de la PC correspondant au type de certificat porteur policyQualifiers = https://pc.chambersign.fr/ca3/[Common_Name_AC].pdf
id-pkix-ocsp-nocheck (oid 1.3.6.1.5.5.7.48.1.5)	Non	NULL
<i>Extended Key Usage</i>	Non	id-kp-OCSPSigning
<i>CRL Distribution Points</i>	Non	distributionPoint = http://crl.chambersign.fr/ca3/[Common_Name_AC].crl http://crl.chambersign.tm.fr/ca3/[Common_Name_AC].crl

Extension	Criticité	Valeur
<i>Authority Information Access</i>	Non	caIssuers = https://pc.chambersign.fr/ca3/[Common_Name_AC].cer Répondeur OCSP : accessMethod = id-ad-ocsp accessLocation = http://ocsp-ca3.chambersign.fr/[Common_Name_AC] accessLocation = http://ocsp-ca3.chambersign.tm.fr/[Common_Name_AC]

11.2 Répondeur OCSF

11.2.1 Requêtes OCSF

Les requêtes OCSF acceptées sont celles qui respectent le format décrit par la RFC 6960.
 Le service OCSF ignore la signature si elle est présente.

Les requêtes attendues sont de la forme :

Champ	Commentaires	Valeur attendue
<i>version</i>	<i>Version de la requête</i>	<i>0 (version 1)</i>
<i>requestorName</i>	<i>Nom de l'émetteur de la requête</i>	<i>Valeur absente ou ignorée</i>
<i>requestList</i> - <i>reqCert</i> - <i>singleRequestExtensions</i>	<i>Liste des certificats à vérifier</i>	<i>Un ou plusieurs identifiants de certificats sont acceptés. La valeur des extensions est ignorée</i>
<i>requestExtensions</i>	<i>Extensions</i>	<i>Seule l'extension Nonce est prise en compte, les autres sont ignorées</i>

Les algorithmes d'empreinte acceptés pour les identifiants de certificats sont SHA-1, SHA-256, SHA-384 et SHA-512.

11.2.2 Réponses OCSF

Les réponses OCSF respectent le format décrit par la RFC 6960. Elles sont signées par le service sauf si une erreur s'est produite (requête rejetée ou échec de traitement).

Les réponses sont de la forme BasicOCSPResponse :

Champ	Commentaires	Valeur
<i>version</i>	<i>Version de la requête</i>	<i>0 (version 1)</i>
<i>responderID</i>	<i>Nom du répondeur</i>	<i>Hash de la clé publique du répondeur</i>
<i>producedAt</i>	<i>Heure de production de la réponse</i>	<i>Heure de production à la seconde près</i>
<i>responses</i> - <i>certID</i> - <i>certStatus</i> - <i>revocationDate</i> - <i>thisUpdate</i>	<i>Statut des certificats identifiés dans la requête</i>	<i>Le statut du certificat est le statut actuel du certificat (thisUpdate est la date courante). La date de révocation est fournie le cas échéant, mais pas la raison de révocation</i>
<i>responseExtensions</i>	<i>Extensions</i>	<i>L'extension Nonce fournie par un émetteur est renvoyée dans la réponse</i>

12 Nommage de la hiérarchie

Abréviation		OID des PC		
ChamberSign France CA3 Root				
1.2.250.1.96.1.8	20 ans Expire 04/12/2038	1.2.250.1.96.1.8		20 ans
ChamberSign France CA3 NG RGS	1.2.250.1.96.1.8.1 10 ans Expire 30/11/2029	authentification * (Initio Identité, §4.1)	1.2.250.1.96.1.8.1.10	3 ans
		authentification ** (Audacio Identité, §4.2)	1.2.250.1.96.1.8.1.1	3 ans
		authentification *** (Probatio Identité, §4.3)	1.2.250.1.96.1.8.1.2	3 ans
		signature * (Initio Signature, §4.4)	1.2.250.1.96.1.8.1.11	3 ans
		signature ** (Audacio Signature, §4.5)	1.2.250.1.96.1.8.1.3	3 ans
		signature *** (Probatio Signature, §4.6)	1.2.250.1.96.1.8.1.4	3 ans
		authentification & signature * lcp-n (Initio, §4.7)	1.2.250.1.96.1.8.1.5	3 ans
		authentification & signature ** (Audacio, §4.8)	1.2.250.1.96.1.8.1.6	3 ans
		personne morale * lcp-l (Negocio, §4.9)	1.2.250.1.96.1.8.1.7	3 ans
		personne morale ** (Comercio, §4.11)	1.2.250.1.96.1.8.1.8	3 ans
		authentification client TLS * lcp-l (Certiserv, §4.10)	1.2.250.1.96.1.8.1.9	3 ans
		authentification serveur ** (§4.12)	1.2.250.1.96.1.8.1.12	3 ans
	ChamberSign France CA3 NG Qualified eID	qcp-n (Eiducio Signature, §5.1)	1.2.250.1.96.1.8.2.1	3 ans
		qcp-n double usage authentification & signature ** (Eiducio, §5.2)	1.2.250.1.96.1.8.2.6	1, 2, 3 ans
		qcp-n-qscd signature*** (EuroProbatio ; §5.3)	1.2.250.1.96.1.8.2.2	Variable, <3 ans
		qcp-l personne morale ** (EuroComercio, §5.4)	1.2.250.1.96.1.8.2.3	3 ans
1.2.250.1.96.1.8.2	10 ans Expire 30/11/2029			

Abréviation		OID des PC		
		qcp-l-qscd personne morale ** (EuroComercio+, §5.5)	1.2.250.1.96.1.8.2.4	3 ans
		qncp-w-gen authentification serveur TLS * (QWAC serveur, §5.6)	1.2.250.1.96.1.8.2.5	Variable, <1 an
		2D-Doc (§5.7)	1.2.250.1.96.1.8.2.7	3 ans
		qcp-n-qscd double usage authentification & signature ** (Eiducio+, §5.8)	1.2.250.1.96.1.8.2.8	1, 2, 3 ans
		qcp-n-qscd (§5.9)	1.2.250.1.96.1.8.2.9	Variable, <3 an
	ChamberSign France CA3 NG Standard eID 1.2.250.1.96.1.8.3 10 ans Expire 30/11/2029	LCP-n	1.2.250.1.96.1.8.3.1	
		LCP-I	1.2.250.1.96.1.8.3.2	
		NCP-n	1.2.250.1.96.1.8.3.3	
		NCP-I	1.2.250.1.96.1.8.3.4	
		NCP+-n	1.2.250.1.96.1.8.3.5	
	ChamberSign France CA3 NG Website 1.2.250.1.96.1.8.4 10 ans Expire 30/11/2029	OVCP	1.2.250.1.96.1.8.4.1	variable
		EVCP	1.2.250.1.96.1.8.4.2	variable
	ChamberSign France CA3 NG Timestamp 1.2.250.1.96.1.8.5 10 ans Expire 30/11/2029	Cachet horodatage	1.2.250.1.96.1.8.5.1	variable
	ChamberSign France CA3 NG CEV 1.2.250.1.96.1.8.6 10 ans Expire 30/11/2029	Cachet 2D-Doc	1.2.250.1.96.1.8.6.1	3 ans