Profils de Certificats et de LCR

AC 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	15
Date de diffusion	11/05/2021

Rédigé par Jean-Pierre PRUNARET	Jean-Pierre PRUNARET Signature numérique de Jean-Pierre PRUNARET Date : 2021.05.11 15:50:13 +02'00'
Vérifié par Sylvain ROSSI	
Approuvé par Stéphane GASCH	Stephane GASCH Signature numérique de Stephane GASCH DN : c=FR, o=CHAMBERSIGN FRANCE, ou=CHAMBERSIGN FRANCE, ou=00024337024790004 2, ou=Direction Générale, 2.5.4.97=NTRFR-43370247900042, l=LYON 2EME ARRONDISSEMENT, cn=GASCH, givenName=Stephane, cn=Stephane GASCH, title=Stephane Gasch, serialNumber=0001 Version d'Adobe Acrobat : 2021.001.20150

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

Le document est approuvé avec les marques de révision des modifications réalisées depuis la précédente version approuvée. Un document autonome reprend l'historique des mises à jour.

Avertissement

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

A 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 destinés 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.

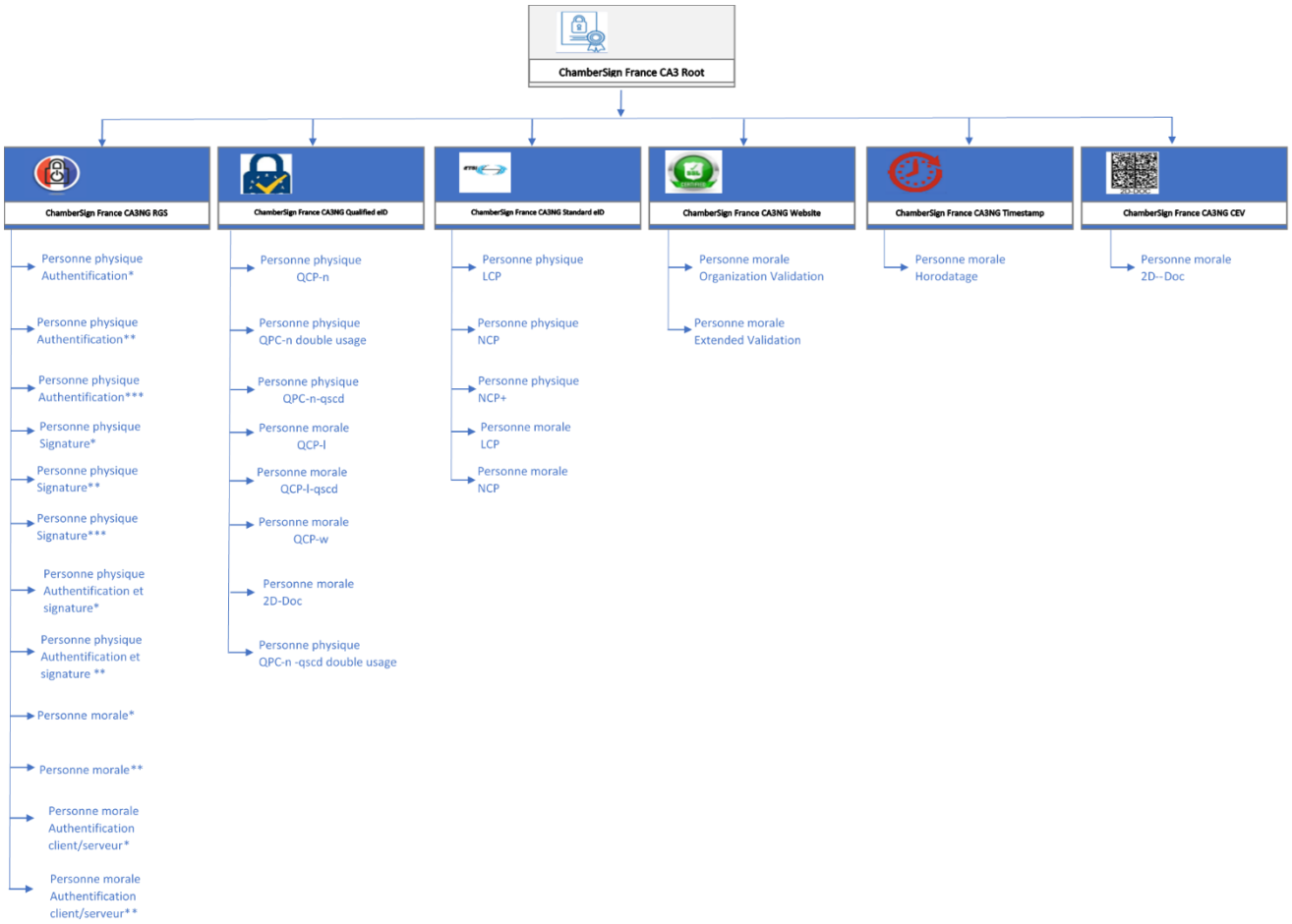
Le présent document, propriété de **CHAMBERSIGN FRANCE,** peut être concédée par des accords de licence à toutes entités privées ou publiques qui souhaiteraient l'utiliser dans le cadre de leurs propres services de certification.

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 « AC 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 :



**Les profils qui ne sont pas à activer immédiatement sont précisés dans le tableau présent au chapitre 12.1 OID*

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

Chaque AC intermédiaire comporte une bi-clé utilisée pour signer les certificats des porteurs de la classe correspondante, pour signer les LCR (listes de certificats révoqués) des certificats de la classe 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
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 4096 bits
Issuer	CN=ChamberSign France CA3 Root orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (notBefore + 20 ans)
Subject	Identique à *Issuer*
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 4096 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de ce certificat authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
Subject Key Identifier	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de ce certificat
Key Usage	Oui	keyCertSign, cRLSign
Basic Constraints	Oui	cA = TRUE

2.2 AC Intermédiaires

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256-RSA-PKCS1avec une longueur de clé de 4096 bits
Issuer	CN=ChamberSign France CA3 Root orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime, la moins éloignée des dates suivantes : notBefore + 10 ans ; notAfter du certificat d'AC Racine
Subject	CN=[COMMON_NAME_AC] orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Subject Public Key Info	algorithm = rsaEncryption subjectPublicKey = clé de 4096 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier = Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de l'AC Racine authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
Subject Key Identifier	Non	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de ce certificat
Key Usage	Oui	keyCertSign, cRLSign
Certificate Policies	Non	policyIdentifier = anyPolicy policyQualifiers = /
Basic Constraints	Oui	cA = TRUE
CRL Distribution Points	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_Root.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_Root.crl
Authority Information Access	Non	caIssuers = 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 basées en France Métropolitaine et les DOM : 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 prestataire 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>
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 sur la pièce d'identité présentée lors de l'enregistrement et dont la copie est conservée dans le dossier d'enregistrement.
commonName	Prénom1(,Prénom2,Prénom3,…) NOM 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.
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 Par défaut, la valeur de cet attribut est « 0001 ». 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 « 0002 » et ainsi de suite.
Authority Key Identifier	Empreinte SHA-1 (160 bit) de la valeur subjectPublicKey du champ *Subject Public Key Info* de l'AC Intermédiaire correspondante authorityCertIssuer et authorityCertSerialNumber ne sont pas utilisés
Subject Key Identifier	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
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 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 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

Extension	Criticité	Valeur
Key Usage	Oui	digitalSignature
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.1.10 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_RGS.pdf
Extended key usage	Non	- 1.3.6.1.4.1.311.20.2.2 (OID Microsoft pour le Smart Card Logon) - 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth, cf. RFC5280)
CRL Distribution Points	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
Authority Information Access	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer

4.2 Certificats d'authentification ** RGS 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 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 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
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.1.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_RGS.pdf
Extended key usage	Non	- 1.3.6.1.4.1.311.20.2.2 (OID Microsoft pour le Smart Card Logon) - 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth, cf. RFC5280)
CRL Distribution Points	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl
Authority Information Access	Non	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer

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	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
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)

Champ	Valeur
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
Key Usage	Oui	digitalSignature
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.1.2 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_RGS.pdf
Extended key usage	Non	- 1.3.6.1.4.1.311.20.2.2 (OID Microsoft pour le Smart Card Logon) - 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth, cf. RFC5280)
CRL Distribution Points	Non	distributionPoint = http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_RGS.crl

Extension	Criticité	Valeur
Authority Information Access	Non	calssuers = 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

4.4 Certificats de signature * RGS 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 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 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier
Subject Key Identifier	Non	keyIdentifier

Extension	Criticité	Valeur
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
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.1.11 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
Extended key usage	Non	MS Document Signing Adobe PDF Signing
CRL Distribution Points	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
Authority Information Access	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer

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	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
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

Champ	Valeur
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
Key Usage	Oui	Non Repudiation
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.1.3 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.pdf
Extended key usage	Non	MS Document Signing Adobe PDF Signing
CRL Distribution Points	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
Authority Information Access	Non	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer
qcStatements	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	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits

Champ	Valeur
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 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
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.1.4 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_RGS.pdf
Extended key usage	Non	MS Document Signing Adobe PDF Signing
CRL Distribution Points	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

Extension	Criticité	Valeur
Authority Information Access	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.fr.tm/ChamberSign_France_CA3_NG_RGS
qcStatements	Non	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_RGS_Signature_3etoiles_en.pdf

4.7 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	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
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 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier

Extension	Criticité	Valeur
Subject Key Identifier	Non	keyIdentifier
Basic Constraints	Oui	CA = False
Key Usage	Oui	digitalSignature, nonRepudiation
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.1.5 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_RGS.pdf
Extended key usage	Non	- 1.3.6.1.4.1.311.20.2.2 (OID Microsoft pour le Smart Card Logon) - 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth, cf. RFC5280) MS Document Signing Adobe PDF Signing EmailProtection
CRL Distribution Points	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
Authority Information Access	Non	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer

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	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
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

Champ	Valeur
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
Key Usage	Oui	digitalSignature, nonRepudiation
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.1.6 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_RGS.pdf
Extended key usage	Non	- 1.3.6.1.4.1.311.20.2.2 (OID Microsoft pour le Smart Card Logon) - 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth, cf. RFC5280) MS Document Signing Adobe PDF Signing EmailProtection
CRL Distribution Points	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
Authority Information Access	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer
qcStatements	Non	id-etsi-qcs-QcCompliance QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_RGS_Doubleusage_2etoiles.pdf

4.9 Certificats de personne morale 1*

Champ	Valeur
Version	2

Champ	Valeur
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 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 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 = 1.2.250.1.96.1.8.1.7 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_RGS.pdf
Extended key usage	Non	MS Document Signing Adobe PDF Signing
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
CRL Distribution Points	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
Authority Information Access	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer

4.10 Certificats d'authentification personne morale client/serveur 1*

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
Issuer	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 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

Extension	Criticité	Valeur
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.1.9 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_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*
Extended key usage	Non	id-kp-clientAuth,
CRL Distribution Points	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
Authority Information Access	Non	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer

4.11 Certificats de personne morale 2*

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 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 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_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
Extended key usage	Non	MS Document Signing Adobe PDF Signing
CRL Distribution Points	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
Authority Information Access	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer
qcStatements	Non	id-etsi-qcs-QcCompliance QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3_ng/PDS_RGS_Cachet_2etoiles.pdf

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	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
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 bits
Unique Identifiers	Vide (non utilisé)
Extensions	Cf. tableau suivant

Extension	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier

Extension	Criticité	Valeur
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_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*
Extended key usage	Non	id-kp-clientAuth, *id-kp-serverAuth*
CRL Distribution Points	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
Authority Information Access	Non	caIssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_RGS.cer
qcStatements	Non	id-etsi-qcs-QcCompliance QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_RGS_Server_auth_2etoiles.pdf

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

5.1 Certificats de signature qualifiés eIDAS 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 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* 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
Key Usage	Oui	Non Repudiation

Extension	Criticité	Valeur
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.2.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf
Extended key usage	Non	MS Document Signing Adobe PDF Signing
CRL Distribution Points	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
Authority Information Access	Non	calssuers = 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
qcStatements	Non	id-etsi-qcs-QcCompliance id-etsi-qct-esign QcEuPDS = https://pc.chambersign.fr/docs/pds/ca3/PDS_Qualified_eID_qcp-n.pdf

5.2 Certificats d'authentification et de signature qualifiés eIDAS 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 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)

Champ	Valeur
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
Key Usage	Oui	digitalSignature, nonRepudiation
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.2.6 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf
Extended key usage	Non	- 1.3.6.1.4.1.311.20.2.2 (OID Microsoft pour le Smart Card Logon) - 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth, cf. RFC5280) MS Document Signing Adobe PDF Signing EmailProtection
CRL Distribution Points	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

Extension	Criticité	Valeur
Authority Information Access	Non	calssuers = 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
qcStatements	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
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 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* 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

Extension	Criticité	Valeur
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
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.2.2 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf
Extended key usage	Non	MS Document Signing Adobe PDF Signing
CRL Distribution Points	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
Authority Information Access	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
qcStatements	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
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 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 = 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
Extended Key Usage	Non	MS Document Signing Adobe PDF Signing

Extension	Criticité	Valeur
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.2.3 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf
CRL Distribution Points	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
Authority Information Access	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
qcStatements	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
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 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

Champ	Valeur
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
Extended Key Usage	Non	MS Document Signing Adobe PDF Signing
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.2.4 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf
CRL Distribution Points	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
Authority Information Access	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

Extension	Criticité	Valeur
qcStatements	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-qscd.pdf

5.6 Certificats SSL qualifiés eIDAS 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 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 = 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*

Extension	Criticité	Valeur
Basic Constraints	Oui	CA = False
Key Usage	Oui	digitalSignature
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.2.5 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf
Subject Altenative Name	Non	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_Qualified_eID.crl http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl
Authority Information Access	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
qcStatements	Non	id-etsi-qcs-QcCompliance id-etsi-qct-web

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	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
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)

Champ	Valeur
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
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.2.7 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf
Extended key usage	Non	MS Document Signing Adobe PDF Signing
CRL Distribution Points	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

Extension	Criticité	Valeur
Authority Information Access	Non	calssuers = 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

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

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 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* *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
Key Usage	Oui	digitalSignature, nonRepudiation

Extension	Criticité	Valeur
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.2.8 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf
Extended key usage	Non	- 1.3.6.1.4.1.311.20.2.2 (OID Microsoft pour le Smart Card Logon) - 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth, cf. RFC5280) MS Document Signing Adobe PDF Signing EmailProtection
CRL Distribution Points	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
Authority Information Access	Non	calssuers = 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
qcStatements	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

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

6.1 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 (= 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 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*

Extension	Criticité	Valeur
Basic Constraints	Oui	CA = False
Key Usage	Oui	Certificat authentification : digitalSignature Certificat signature nonRepudiation Certificat signature et authentification : digitalSignature, nonRepudiation
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.3.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Standard_eID.pdf
Extended key usage	Non	Certificat authentification : - 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) Certificat signature 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	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.cer

6.2 Certificats NCP 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 (= notBefore + 3 ans)

Champ	Valeur
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
Key Usage	Oui	Certificat authentification : digitalSignature Certificat signature nonRepudiation Certificat signature et authentification : 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

Extension	Criticité	Valeur
Extended key usage	Non	Certificat authentification : - 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) Certificat signature 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	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.cer

6.3 Certificats NCP+ 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 (= 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 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	Certificat authentification : digitalSignature Certificat signature nonRepudiation Certificat signature et authentification : 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	Certificat authentification : - 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) Certificat signature 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	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.cer

6.4 Certificats LCP ETSI 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

Champ	Valeur
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 (= 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 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
Extended Key Usage	Non	MS Document Signing Adobe PDF Signing
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.3.2 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Standard_eID.pdf

Extension	Criticité	Valeur
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	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.cer

6.5 Certificats NCP ETSI 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 Standard 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 = 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

Extension	Criticité	Valeur
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
Extended Key Usage	Non	MS Document Signing Adobe PDF Signing
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.3.4 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Standard_eID.pdf
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	calssuers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Standard_eID.cer

7 Certificats finaux AC « ChamberSign France CA3 NG Website »

7.1 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 (= notBefore + 3 ans)
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

Extension	Criticité	Valeur
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.4.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Website.pdf
Subject Altenative Name	Non	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

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 (= notBefore + 3 ans)
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
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 Altenative 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
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 Timestamp 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 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 service*
Issuer Alternative Name	Non	*rfc822Name (IA5String) = autorite@chambersign.fr* *uniformResourceIdentifier (IA5String) = https://www.chambersign.fr*
Basic Constraints	Oui	CA = False

Extension	Criticité	Valeur
Key Usage	Oui	digitalSignature
Extended Key Usage	Oui	id-kp-timeStamping *Adobe TSA URI*
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.5.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Timestamp.pdf
CRL Distribution Points	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
Authority Information Access	Non	caIssuers = 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

9 Certificats finaux AC « ChamberSign France CA3 NG CEV »

9.1 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
Certificate Policies	Non	policyIdentifier = 1.2.250.1.96.1.8.6.1 policyQualifiers = https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_CEV.pdf

Extension	Criticité	Valeur
Extended key usage	Non	MS Document Signing Adobe PDF Signing
CRL Distribution Points	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
Authority Information Access	Non	calssuers = 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
Version	1
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
Issuer	CN=ChamberSign France CA3 Root orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
This Update	Date de début de validité de la LAR au format UTCTime
Next Update	Date de début de validité au plus tard de la prochaine LAR au format UTCTime (= *This Update* + 364j) A la fin de vie de l'AC et avant que le certificat d'AC expire ou soit révoqué, une dernière LCR est publiée avec une fin de validité positionnée au 31 décembre 9999, 23h59m59s
Revoked Certificates	- userCertificate : *Serial Number* du certificat d'AC révoqué - revocationDate : date de révocation du certificat au format UTCTime - crlEntryExtensions : aucune extension d'entrée n'est utilisée
Extensions	Cf. tableau ci-dessous

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

10.2 LCR

Champ	Valeur
Version	1
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
Issuer	CN=Common_Name_AC orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
This Update	Date de génération de la LCR au format UTCTime
Next Update	Date de génération au plus tard de la prochaine LCR au format UTCTime (= *This Update* + 24h) A 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
Revoked Certificates	- userCertificate : *Serial Number* du certificat porteur révoqué - revocationDate : date de révocation du certificat au format UTCTime - crlEntryExtensions : aucune extension d'entrée n'est utilisée
Extensions	Cf. tableau ci-dessous

Extension de LCR	Criticité	Valeur
Authority Key Identifier	Non	keyIdentifier
Issuer Alternative Name	Non	rfc822Name (IA5String) = autorite@chambersign.fr uniformResourceIdentifier (IA5String) = https://www.chambersign.fr
CRL Number	Non	Nombre entier séquentiel, codé sur 20 octets
Expired Certs on CRL	Non	GeneralizedTime (X509)

11 OCSP

11.1 Certificats du service OCSP

Champ	Valeur
Version	2
Serial Number	Numéro unique au sein de la hiérarchie de 16 octets
Signature	SHA256-RSA-PKCS1 avec une longueur de clé de 2048 bits
Issuer	CN=<Common_Name_AC> orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
Validity	notBefore = date au format UTCTime notAfter = date au format UTCTime (= notBefore + 1 ans)
Subject	CN=ocsp <Common_Name_AC> orgID=NTRFR-433702479 OU= 0002 433702479 O=ChamberSign France C=FR
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) = http://www.chambersign.fr
Basic Constraints	Oui	CA = False
Key Usage	Oui	digitalSignature
Certificate Policies	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
Extended Key Usage	Non	id-kp-OCSPSigning
CRL Distribution Points	Non	distributionPoint = http://crl.chambersign.fr/ca3/[Common_Name_AC].crl http://crl.chambersign.tm.fr/ca3/[Common_Name_AC].crl

Extension	Criticité	Valeur
Authority Information Access	Non	calssuers = 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 OCSP

11.2.1 Requêtes OCSP

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

Les requêtes attendues sont de la forme :

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

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

11.2.2 Réponses OCSP

Les réponses OCSP 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
version	Version de la requête	0 (version 1)
responderID	Nom du répondeur	Hash de la clé publique du répondeur
producedAt	Heure de production de la réponse	Heure de production à la seconde près
responses - certID - certStatus - revocationDate - thisUpdate	Statut des certificats identifiés dans la requête	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

responseExtensions	Extensions	L'extension Nonce fournie par un émetteur est renvoyée dans la réponse

12 Nommage de la hiérarchie

12.1 OID

Abréviation		OID	OID des PC		Certificat commercialisé
ChamberSign France CA3 Root		1.2.250.1.96.1.8	*1.2.250.1.96.1.8*		
	ChamberSign France CA3 NG RGS	1.2.250.1.96.1.8.1	authentification *	1.2.250.1.96.1.8.1.10	
			authentification **	1.2.250.1.96.1.8.1.1	X
			authentification ***	1.2.250.1.96.1.8.1.2	
			signature *	1.2.250.1.96.1.8.1.11	
			signature **	1.2.250.1.96.1.8.1.3	
			signature ***	1.2.250.1.96.1.8.1.4	
			authentification & signature *	1.2.250.1.96.1.8.1.5	X
			authentification & signature **	1.2.250.1.96.1.8.1.6	
			personne morale *	1.2.250.1.96.1.8.1.7	X
			personne morale **	1.2.250.1.96.1.8.1.8	
			authentification serveur *	1.2.250.1.96.1.8.1.9	X
			authentification serveur **	1.2.250.1.96.1.8.1.12	
	ChamberSign France CA3 NG Qualified eID	1.2.250.1.96.1.8.2	qcp-n	1.2.250.1.96.1.8.2.1	
			qcp-n double usage	1.2.250.1.96.1.8.2.6	X
			qcp-n-qscd	1.2.250.1.96.1.8.2.2	X
			qcp-l	1.2.250.1.96.1.8.2.3	X
			qcp-l-qscd	1.2.250.1.96.1.8.2.4	
			qcp-w	1.2.250.1.96.1.8.2.5	
			2D-Doc	1.2.250.1.96.1.8.2.7	
			qcp-n-qscd double usage	1.2.250.1.96.1.8.2.8	X
	ChamberSign France CA3 NG Standard eID	1.2.250.1.96.1.8.3	LCP-n	1.2.250.1.96.1.8.3.1	
			LCP-l	1.2.250.1.96.1.8.3.2	
			NCP-n	1.2.250.1.96.1.8.3.3	
			NCP-l	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	OVCP	1.2.250.1.96.1.8.4.1	
			EVCP	1.2.250.1.96.1.8.4.2	

Abréviation		OID	OID des PC		Certificat commercialisé
	ChamberSign France CA3 NG Timestamp	1.2.250.1.96.1.8.5	Cachet horodatage	1.2.250.1.96.1.8.5.1	
	ChamberSign France CA3 NG CEV	1.2.250.1.96.1.8.6	Cachet 2D-Doc	1.2.250.1.96.1.8.6.1	