Profils des certificats, OCSP, LCR
Chaine de confiance « CertEurope eID »

Version : 1.3

Date de création : 1 octobre 2016

Dernière mise à jour : 25 avril 2019

Etat du document : Officiel

Rédigé par : CertEurope

Vérifié par : COSSI

Approuvé par : COSSI

CertEurope, une société du groupe Oodrive

www.certeurope.fr

Modifications

Date	Etat	Version	Commentaire
1 octobre 2016	Projet	1.0	Version initiale
7 février 2017	Officiel	1.1	Correction suite à l'audit. - Ne permettre que l'usage Signature ainsi que le double usage Signature/Authentification pour les profils QCP-N-QSCD et QCP-N
19 juin 2017	Officiel	1.2	Supprimer les identifiants sémantiques, optionnels, pour les certificats de site web. Revue de la liste des profils suite à la décision de l'ANSSI de ne pas permettre la transition pour les SSCD de cachet (QCP-L-QSCD), uniquement pour la signature (QCP-N-QSCD).
25 juin 2019	Officiel	1.3	- Ajout des nouveaux profils RGS et EIDAS - OU optionnel pour les profils non RGS - Ajout des profils PSD2 et des QCStatements correspondants - Correction mineure suite audit interne

Table des matières

Modifications 2
Table des matières 3
1 Introduction 5
2 Profils des certificats 6
2.1 Profils des certificats des Autorités de Certifications 6
2.1.1 CertEurope eID Root 6
2.1.2 CertEurope eID Officer 7
2.1.3 CertEurope eID User 8
2.1.4 CertEurope eID Corp 9
2.1.5 CertEurope eID Website 10
2.2 Socle commun à tous les profils de certificats 12
2.3 Profils des certificats pour personnes physiques 12
2.3.1 Les champs communs aux certificats pour personnes physiques 12
2.3.2 CertEurope User Qualified (RGS et EIDAS) 13
2.3.3 CertEurope User International (EIDAS) 14
2.3.4 CertEurope User France (RGS) 15
2.3.5 CertEurope User Certified 15
2.4 Profils des certificats de cachet pour personnes morales 16
2.4.1 Les champs communs aux certificats de cachet pour personnes morales 16
2.4.2 CertEurope Corp Qualified (RGS et EIDAS) 17
2.4.3 CertEurope Corp International (EIDAS) 18
2.4.4 CertEurope Corp France (RGS) 18
2.4.5 CertEurope Corp PSD2 (EIDAS et PSD2) 19
2.4.6 CertEurope Corp Certified 20
2.5 Profils des certificats pour serveurs 21
2.5.1 Les champs communs aux certificats pour serveurs 21
2.5.2 CertEurope Website Qualified (EIDAS et RGS) 22
2.5.3 CertEurope Website International (EIDAS) 23
2.5.4 CertEurope Website France (RGS) 24
2.5.5 CertEurope Website PSD2 (EIDAS et PSD2) 24
2.5.6 CertEurope EV SSL 26
2.5.7 CertEurope SSLDomain 26
2.5.8 CertEurope SSLOrganisation 26
3 Profil des LCR 27
2.1.1. CHAMPS DES LCR 27

2.1.2. EXTENSIONS DES LCR 27
4 Protocole de vérification de certificat en ligne (OCSP) 27
4.1 Les champs communs aux certificats de signature OCSP 28
4.2 Les profils des certificats OCSP 28

1 Introduction

Ce document présente les différents profils de certificats délivrés par l'Autorité de Certification CertEurope eID CA en fonction des niveaux de sécurité et des usages. Il présente également les profils OCSP et LCR.

Le schéma suivant décrit chaque la hiérarchie des AC et des serveurs OCSP correspondants

Ci-dessous le schéma pour l'offre qualifiée RGS et EIDAS

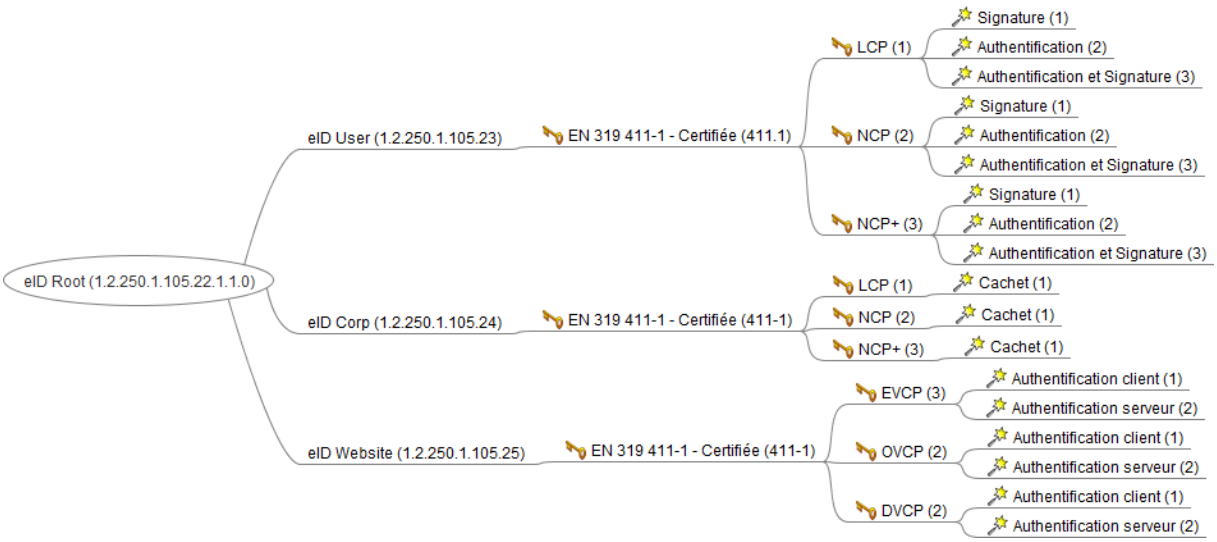
Par exemple, pour l'offre de certificat qualifié sur support crypto, Signature : 1.2.250.1.105.23.411.2.2.3.1.0

- 1.2.250.1.105 : CertEurope
- 23 : eID User (AC)
- 411 : Offre EIDAS
- 2 : Qualifié
- 2 : sur QSCD (Profils particuliers : Logiciel (1), Matériel (2), EIDAS (3), RGS (4) ou PSD2 (5))
- 1 : Signature
- 1 : Version majeure
- 0 : Version mineure

Les profils de certificats pour les serveurs OCSP sont émis à partir de chaque AC intermédiaire et de l'AC racine. Ils sont conformes à la RFC 6960 et suivent donc l'OID de chaque AC. Par exemple :

- 1.2.250.1.105 : CertEurope
- 24 : eID Corp (AC)
- 6960 : Serveur OCSP des cachets pour personnes morales
- 1 : version majeure
- 0 : version

L'offre certifiée ETSI uniquement (sans aucune autre qualification) est décrite ci-après



Ce qui suit décrit l'offre qualifiée EIDAS

Le schéma ci-dessous décrits les profils RGS*

La liste des profils compatibles PSD2 est décrite ci-après

2 Profils des certificats

2.1 Profils des certificats des Autorités de Certifications

2.1.1 CertEurope eID Root

Certificat de l'AC racine dont découle les AC qualifiées EIDAS et certifiées (uniquement ETSI) pour les personnes physiques, les personnes morales et les serveurs web. Etant une racine auto-signée, la RFC 5280 n'impose pas la présence du champ *AuthorityKeyIdentifier* dont la valeur serait dupliquée avec le champ *SubjectKeyIdentifier.*

Le champ *Organizationidentifier (2.5.4.97)*, reprend la nomenclature de l'ANSSI (**SI:FR**) suivi du numéro de SIREN de CertEurope : **SI:FR-434202180**

Le champ *OrganizationUnitName*, reprend les exigences du RGSv2 en spécifiant l'identifiant ICD pour la France (0002) avant le SIREN de CertEurope : **0002 434202180**

La valeur de ces deux champs est la même pour l'AC Racine ainsi que les AC intermédiaires (User, Corp et Website).

La colonne « C » indique si le champ est critique (O) ou non (N).

CertEurope eID Root		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		20 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 20 ans
SubjectPublicKeyInfo		La clé publique avec une longueur de 4096 bits (RSA)
Issuer		
CountryName		FR
CommonName		CertEurope eID Root
OrganisationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Subject		
CountryName		FR
CommonName		CertEurope eID Root
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Extensions		
KeyUsage	***O***	
keyCertSign		Set
crlSigning		Set
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC
BasicConstraints	***O***	
CA		Vraie
pathLenConstraint		None

2.1.2 CertEurope eID Officer

Autorité de certification des opérateurs de confiance CertEurope.

CertEurope eID Officer		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		20 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 20 ans
SubjectPublicKeyInfo		La clé publique avec une longueur de 4096 bits (RSA)
Issuer		

CertEurope eID Officer		
CountryName		FR
CommonName		CertEurope eID Officer
OrganisationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Subject		
CountryName		FR
CommonName		CertEurope eID Officer
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Extensions		
KeyUsage	***O***	
keyCertSign		Set
crlSigning		Set
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.27.1.1.0 (CertEurope eID Root)
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
CRL Distribution Point	***N***	URL(s) de distribution de la CRL de l'AC racine avec au moins une URL avec le protocole HTTP.
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC
BasicConstraints	***O***	
CA		Vraie
pathLenConstraint		0

2.1.3 CertEurope eID User

Certificat intermédiaire pour l'AC des personnes physiques.

CertEurope eID User		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		20 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 20 ans
SubjectPublicKeyInfo		La clé publique avec une longueur de 4096 bits (RSA)
Issuer		
CountryName		FR
CommonName		CertEurope eID Root
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180

CertEurope eID User		
OrganisationIdentifier		SI:FR-434202180
Subject		
CountryName		FR
CommonName		CertEurope eID User
OrganisationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Extensions		
KeyUsage	***O***	
keyCertSign		Set
crlSigning		Set
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.22.1.1.0 (CertEurope eID Root)
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
CRL Distribution Point	***N***	URL(s) de distribution de la CRL de l'AC racine avec au moins une URL avec le protocole HTTP.
Authority Information Access	***N***	Renseignement de l'extension « Authority Information Access »: - accessMethod OID avec id-ad-caIssuers - accessLocation URL http de téléchargement du certificat de l'AC : http://www.certeurope.fr/reference/eid_root.crt Un répondeur OCSP est mis en œuvre pour respecter les bonnes pratiques décrites par le CA/B Forum : - accessMethod OID avec id-ad-ocsp - accessLocation URL d'accès au répondeur OCSP de l'AC : http://ocsp.certeurope.fr/root/
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC émettrice (eID Root)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC
BasicConstraints	***O***	
CA		Vraie
pathLenConstraint		0 (Zéro)

2.1.4 CertEurope eID Corp

Certificat intermédiaire pour l'AC des personnes morales.

CertEurope eID Corp		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		20 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 20 ans

CertEurope eID Corp		
Champ	*C*	*Valeur*
SubjectPublicKeyInfo		La clé publique avec une longueur de 4096 bits (RSA)
Issuer		
CountryName		FR
CommonName		CertEurope eID Root
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Subject		
CountryName		FR
CommonName		CertEurope eID Corp
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Extensions		
KeyUsage	***O***	
keyCertSign		Set
crlSigning		Set
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.22.1.1.0 (CertEurope eID Root)
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
CRL Distribution Point	***N***	URL(s) de distribution de la CRL de l'AC racine
Authority Information Access	***N***	Renseignement de l'extension « Authority Information Access »: - accessMethod OID avec id-ad-caIssuers - accessLocation URL http de téléchargement du certificat de l'AC : http://www.certeurope.fr/reference/eid_root.crt Un répondeur OCSP est mis en œuvre pour respecter les bonnes pratiques décrites par le CA/B Forum : - accessMethod OID avec id-ad-ocsp - accessLocation URL d'accès au répondeur OCSP de l'AC : http://ocsp.certeurope.fr/root/
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC
BasicConstraints	***O***	
CA		Vraie
pathLenConstraint		0 (Zéro)

2.1.5 CertEurope eID Website

Certificat intermédiaire pour l'AC des serveurs web.

CertEurope eID Website		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC

CertEurope eID Website		
KeySize		4096 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		20 ans
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 20 ans
SubjectPublicKeyInfo		La clé publique avec une longueur de 4096 bits (RSA)
Issuer		
CountryName		FR
CommonName		CertEurope eID Root
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Subject		
CountryName		FR
CommonName		CertEurope eID Website
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Extensions		
KeyUsage	***O***	
keyCertSign		Set
crlSigning		Set
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.22.1.1.0 (CertEurope eID Root)
policyQualifierId		CPS
Qualifier		https ://www.certeurope.fr/chaine-de-confiance
CRL Distribution Point	***N***	URL(s) de distribution de la CRL de l'AC racine
Authority Information Access	***N***	Renseignement de l'extension « Authority Information Access »: - accessMethod OID avec id-ad-caIssuers - accessLocation URL http de téléchargement du certificat de l'AC : http://www.certeurope.fr/reference/eid_root.crt Un répondeur OCSP est mis en œuvre pour respecter les bonnes pratiques décrites par le CA/B Forum : - accessMethod OID avec id-ad-ocsp - accessLocation URL d'accès au répondeur OCSP de l'AC : http://ocsp.certeurope.fr/root/
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC
BasicConstraints	***O***	
CA		Vraie
pathLenConstraint		0 (Zéro)

2.2 Socle commun à tous les profils de certificats

Champ	Valeur
Version	2=(version 3)
SerialNumber	Unique pour chaque certificat généré par le PSCE
Key Size	2048 bits (RSA)
Issuer	
countryName	Pays de résidence du demandeur
organizationName	Nom officiel complet du de l'entité dont dépend le porteur tel qu'enregistré auprès des autorités compétentes
organisationUnitName	Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - l'ICD est sur 4 caractères ; (0002 pour la France) - l'identification de l'organisation sur 35 caractères - le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. Pour les profils de certificats qui ne dépendent pas du RGS, ce champ peut être **optionnel**.
organizationIdentifier	Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4 • En France, ce numéro d'immatriculation peut également être constitué du préfixe « SI:FR- » ou « NTRFR- » suivi du numéro SIREN ou SIRET. • Pour les profils compatibles PSD2 (SSL et Cachet uniquement), ce champ est constitué du préfixe « PSDFR- » suivi de l'identifiant attribué par l'autorité national compétente (NCA). Il peut s'agir de son SIREN/SIRET, du code de la banque ou tout autre identifiant documenté par le NCA. • Pour les profils de certificats qui ne dépendent pas de la réglementation EIDAS, ce champ peut être **optionnel**.
commonName	Nom du prestataire (peut être identique à « organizationName »)
Subject	Voir les règles applicables à chaque type de certificat dans les sections suivantes
Validity	De 1 à 3 ans selon l'offre
NotBefore	Date de la génération de la bi-clé
NotAfter	Date de la génération de la bi-clé + - 1 an ou 2 ans pour les certificats authentification cliente et serveur : eID Website - 1 an ou 3 ans pour les certificats de signature et/ou d'authentification (eID User) et de cachet (eID Corp)
PublicKeyAlgorithm	rsaEncryption
SignatureAlgorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

2.3 Profils des certificats pour personnes physiques

2.3.1 Les champs communs aux certificats pour personnes physiques

Champ	C	Valeur
Subject		

countryName		Pays de résidence du demandeur
organizationName		Nom officiel complet du de l'entité dont dépend le porteur tel qu'enregistré auprès des autorités compétentes
organizationIdentifier		Numéro d'immatriculation officiel de l'entité dont dépend le porteur conformément à [EN_319_412-1] clause 5.1.4 En France, ce numéro d'immatriculation peut également être constitué du préfixe « SI:FR- » ou de « NTRFR- » suivi du numéro SIREN ou SIRET. Ce préfixe est adapté au pays dont dépend l'organisation. Pour les profils de certificats qui ne dépendent pas de la réglementation EIDAS, ce champ peut être **optionnel**.
organizationUnitName		Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : - l'ICD est sur 4 caractères ; (0002 pour la France) - l'identification de l'organisation sur 35 caractères - le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. Pour les profils de certificats qui ne dépendent pas du RGS, ce champ peut être **optionnel**.
serialNumber		Elément complémentaire permettant de distinguer les homonymes. Il s'agit de l'empreinte (SHA-1) des informations personnelles du porteur contenues dans sa pièce d'identité.
givenName		Le premier prénom, le prénom d'usage, ou les prénoms de l'état civil du porteur
surname		Nom de l'état civil ou le nom d'usage du porteur
commonName		Le nom complet du porteur tel qu'il devrait être affiché par les applications. Il est recommandé d'indiquer le prénom d'usage du porteur, suivi d'un espace, suivi du nom de l'état civil ou du nom d'usage du porteur.
Extensions		
KeyUsage	***O***	Voir pour chaque profil décrit plus bas
CertificatePolicies	***N***	Voir pour chaque profil décrit plus bas
CRL Distribution Point	***N***	URL(s) de distribution de la CRL de l'AC CertEurope eID User
Authority Information Access	***N***	URL(s) du service OCSP de l'AC CertEurope eID User
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC émettrice (eID User)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Identifiant de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		Faux
QCStatements	***N***	Voir pour chaque profil décrit plus bas

2.3.2 CertEurope User Qualified (RGS et EIDAS)

Profils de certificats conformes à la norme ETSI EN 319 411-2. Ces certificats se présentent soit sous la forme logicielle (QCP-N) ou sur un support cryptographique de type QCP-N-QSCD. Ils contiennent la déclaration des certificats qualifiés définie par la norme ETSI EN 319 412-5. Cette offre vise la qualification **EIDAS** ainsi que le **RGSv2**.

Champ	C	Signature	Authentification & signature
QCP-N			
Certificate Policies	***N***		
PolicyIdentifier		1.2.250.1.105.23.411.2.**1**.***1***.1.0	1.2.250.1.105.23.411.2.**1**.***2***.1.0
policyQualifierId		CPS	
Qualifier		https://www.certeurope.fr/chaine-de-confiance	
Key usage	***O***	nonRepudiation	nonRepudiation, digitalSignature
Extended Key Usage	***N***	emailProtection	emailProtection, clientAuth
QcCompliance	***N***	esi4-qcStatement-1	
QcSSCD	***N***	Non utilisé	
QcType	***N***	esi4-qcStatement-6 = id-etsi-qct-esign	
QcPDS	***N***	URL des CGUs en anglais	
QcRetentionPeriod	***N***	10 ans	
QCP-N-QSCD			
Certificate Policies	***N***		
PolicyIdentifier		1.2.250.1.105.23.411.2.**2**.***1***.1.0	1.2.250.1.105.23.411.2.**2**.***2***.1.0
policyQualifierId		CPS	
Qualifier		https://www.certeurope.fr/chaine-de-confiance	
Key usage	***O***	nonRepudiation	nonRepudiation, digitalSignature
Extended Key Usage	***N***	emailProtection	emailProtection, clientAuth
QcCompliance	***N***	esi4-qcStatement-1	
QcSSCD	***N***	esi4-qcStatement-4	
QcType	***N***	id-etsi-qct-esign	
QcPDS	***N***	URL des CGUs en anglais	
QcRetentionPeriod	***N***	10 ans	

2.3.3 CertEurope User International (EIDAS)

Profils de certificats conformes à la norme ETSI EN 319 411-2. Ces certificats se présentent soit sous la forme logicielle (QCP-N) ou sur un support cryptographique de type QCP-N-QSCD. Ils contiennent la déclaration des certificats qualifiés définie par la norme ETSI EN 319 412-5. Cette offre vise la qualification **EIDAS** uniquement.

Champ	C	Authentification & signature
QCP-N		
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.23.411.2.**3**.***1***.1.0
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation, digitalSignature
Extended Key Usage	***N***	emailProtection, clientAuth
QcCompliance	***N***	esi4-qcStatement-1

Champ	C	Authentification & signature
QcSSCD	***N***	Non utilisé
QcType	***N***	esi4-qcStatement-6 = id-etsi-qct-esign
QcPDS	***N***	URL des CGUs en anglais
QcRetentionPeriod	***N***	10 ans
QCP-N-QSCD		
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.23.411.2.**3**.***2***.1.0
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation, digitalSignature
Extended Key Usage	***N***	emailProtection, clientAuth
QcCompliance	***N***	esi4-qcStatement-1
QcSSCD	***N***	esi4-qcStatement-4
QcType	***N***	id-etsi-qct-esign
QcPDS	***N***	URL des CGUs en anglais
QcRetentionPeriod	***N***	10 ans

2.3.4 CertEurope User France (RGS)

Profils de certificats conformes à la norme ETSI EN 319 411-1. Ces certificats se présentent soit sous la forme logicielle (LCP). Cette offre vise la qualification **RGS*** uniquement.

Champ	C	Authentification & signature
LCP		
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.23.411.1.4.***1***.1.0
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation, digitalSignature
Extended Key Usage	***N***	emailProtection, clientAuth

2.3.5 CertEurope User Certified

Profils de certificats conformes à la norme ETSI EN 319 411-1. Ces certificats se présentent soit sous la forme logicielle (LCP, NCP) ou sur support cryptographique de type SSCD (NCP+). Cette offre vise la certification ETSI.

Champ	C	Signature	Authentification	Authentification & signature
LCP				
Certificate Policies	***N***			
PolicyIdentifier		1.2.250.1.105.23.411.1.**1**.***1.***1.0	1.2.250.1.105.23.411.1.**1**.***2***.1.0	1.2.250.1.105.23.411.1.1.***3***.1.0
policyQualifierId		CPS		

Champ	C	Signature	Authentification	Authentification & signature
Qualifier		https://www.certeurope.fr/chaine-de-confiance		
Key usage	***O***	nonRepudiation	digitalSignature	nonRepudiation, digitalSignature
Extended Key Usage	***N***	emailProtection	clientAuth	emailProtection, clientAuth
NCP				
Certificate Policies	***N***			
PolicyIdentifier		1.2.250.1.105.23.411.1.**2**.***1***.1.0	1.2.250.1.105.23.411.1.**2**.***2***.1.0	1.2.250.1.105.23.411.1.**2**.***3***.1.0
policyQualifierId		CPS		
Qualifier		https://www.certeurope.fr/chaine-de-confiance		
Key usage	***O***	nonRepudiation	digitalSignature	nonRepudiation, digitalSignature
Extended Key Usage	***N***	emailProtection	clientAuth	emailProtection, clientAuth
NCP+				
Certificate Policies	***N***			
PolicyIdentifier		1.2.250.1.105.23.411.1.**3**.***1***.1.0	1.2.250.1.105.23.411.1.**3**.***2***.1.0	1.2.250.1.105.23.411.1.**3**.***3***.1.0
policyQualifierId		CPS		
Qualifier		https://www.certeurope.fr/chaine-de-confiance		
Key usage	***O***	nonRepudiation	digitalSignature	nonRepudiation, digitalSignature
Extended Key Usage	***N***	emailProtection	clientAuth	emailProtection, clientAuth

2.4 Profils des certificats de cachet pour personnes morales

2.4.1 Les champs communs aux certificats de cachet pour personnes morales

Champ	C	Valeur
Subject		
countryName		Pays où est établie l'entité responsable du certificat.
organizationName		Nom officiel complet du de l'entité dont dépend le porteur tel qu'enregistré auprès des autorités compétentes
organizationIdentifier		Numéro d'immatriculation officiel de l'entité responsable du 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- » ou « NTRFR- » suivi du numéro SIREN ou SIRET. • Pour les profils compatibles PSD2, ce champ est constitué du préfixe « PSDFR- » suivi de l'identifiant attribué par l'autorité national compétente (NCA). Il peut s'agir de son SIREN/SIRET, du code de la banque ou tout autre identifiant documenté par le NCA. • Pour les profils de certificats qui ne dépendent pas de la réglementation EIDAS, ce champ peut être **optionnel**.
organizationUnitName		Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité : • l'ICD est sur 4 caractères ; (0002 pour la France) • l'identification de l'organisation sur 35 caractères

		• le séparateur entre les deux chaînes est un espace. Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. Pour les profils de certificats qui ne dépendent pas du RGS, ce champ peut être **optionnel**.
commonName		Nom significatif du service mettant en œuvre le certificat de cachet
Extensions		
KeyUsage	***O***	Voir pour chaque profil décrit plus bas
CertificatePolicies	***N***	Voir pour chaque profil décrit plus bas
CRL Distribution Point	***N***	URL(s) de distribution de la CRL de l'AC CertEurope eID Corp
Authority Information Access	***N***	URL du service OCSP de l'AC CertEurope eID Corp
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC émettrice (eID Corp)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Identifiant de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		Faux
QCStatements	***N***	Voir pour chaque profil décrit plus bas

2.4.2 CertEurope Corp Qualified (RGS et EIDAS)

Profils de certificats de cachets (SEAL) conformes à la norme ETSI EN 319 411-2. Ces certificats de cachets se présentent soit sous la forme logicielle (QCP-L) ou sur support cryptographique de type QSCD (QCP-L-QSCD). Ils contiennent la déclaration des certificats qualifiés définie par la norme ETSI EN 319 412-5. Un seul profil est possible, celui de Cachet tel que défini dans le RGS et EIDAS.

Etant donné qu'il n'y a pas de dispositif de création de cachet qualifié, le profil QCP-L-QSCD n'est pas envisagé dans cette version.

Champ	C	Cachet
QCP-L		
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.24.411.2.**1**.***1***.1.0
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation, digitalSignature
Extended Key Usage	***N***	
QcCompliance	***N***	esi4-qcStatement-1
QcSSCD	***N***	Non utilisé
QcType	***N***	esi4-qcStatement-6 = id-etsi-qct-eseal
QcPDS	***N***	URL des CGUs en anglais
QcRetentionPeriod	***N***	10 ans
QCP-L (RGS)**		
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.24.411.2.**2**.***1***.1.0

Champ	C	Cachet
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation
Extended Key Usage	***N***	
QcCompliance	***N***	esi4-qcStatement-1
QcSSCD	***N***	**Non utilisé**
QcType	***N***	id-etsi-qct-eseal
QcPDS	***N***	URL des CGUs en anglais
QcRetentionPeriod	***N***	10 ans

2.4.3 CertEurope Corp International (EIDAS)

Profils de certificats de cachets (SEAL) conformes à la norme ETSI EN 319 411-2. Ces certificats de cachets se présentent soit sous la forme logicielle (QCP-L) ou sur support cryptographique de type QSCD (QCP-L-QSCD). Ils contiennent la déclaration des certificats qualifiés définie par la norme ETSI EN 319 412-5. Cette offre vise la qualification **EIDAS** uniquement.

Etant donné qu'il n'y a pas de dispositif de création de cachet qualifié, le profil QCP-L-QSCD n'est pas envisagé dans cette version.

Champ	C	Cachet
QCP-L		
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.24.411.2.**3**.***1***.1.0
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation, digitalSignature
Extended Key Usage	***N***	
QcCompliance	***N***	esi4-qcStatement-1
QcSSCD	***N***	Non utilisé
QcType	***N***	esi4-qcStatement-6 = id-etsi-qct-eseal
QcPDS	***N***	URL des CGUs en anglais
QcRetentionPeriod	***N***	10 ans

2.4.4 CertEurope Corp France (RGS)

Profils de certificats de cachets (SEAL) conformes à la norme ETSI EN 319 411-1. Ces certificats de cachets se présentent soit sous la forme logicielle (LCP). Cette offre vise la qualification **RGS** uniquement.

Champ	C	Cachet
LCP		
Certificate Policies	***N***	

Champ	C	Cachet
PolicyIdentifier		1.2.250.1.105.24.411.1.**4**.***1***.1.0
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation, digitalSignature
Extended Key Usage	***N***	

2.4.5 CertEurope Corp PSD2 (EIDAS et PSD2)

Profils de certificats de cachets (SEAL) conformes à la norme ETSI EN 319 411-2. Ces certificats de cachets se présentent soit sous la forme logicielle (QCP-L) ou sur support cryptographique de type QSCD (QCP-L-QSCD). Ils contiennent la déclaration des certificats qualifiés définie par la norme ETSI EN 319 412-5. Cette offre vise la qualification **EIDAS** uniquement.

Ci-dessous la description du profil qui correspond au cachet qualifié EIDAS auquel on ajoute les déclarations prévue par la spécification technique sur la PSD2.

Etant donné qu'il n'y a pas de dispositif de création de cachet qualifié, le profil QCP-L-QSCD n'est pas envisagé dans cette version.

Champ	C	Cachet
		QCP-L
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.24.411.2.**5**.***1***.1.0
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation
Extended Key Usage	***N***	
QcCompliance	***N***	esi4-qcStatement-1
QcSSCD	***N***	Non utilisé
QcType	***N***	esi4-qcStatement-6 = id-etsi-qct-eseal
QcPDS	***N***	URL des CGUs en anglais
QcRetentionPeriod	***N***	10 ans
		Champs spécifiques à la PSD2
QcType (PSD2)	***N***	etsi-psd2-qcStatement (0.4.0.19495.2)
RolesOfPSP	***N***	Liste des attributs ci-après

RoleOfPspOid	***N***	Une ou plusieurs valeurs suivantes :
		• itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 1
		  ○ PSP_AS: **0.4.0.19495.1.1**
		• itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 2
		  ○ PSP_PI : **0.4.0.19495.1.2**
		• itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 3
		  ○ PSP_AI : **0.4.0.19495.1.3**
		• itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 4
		  ○ PSP_IC : **0.4.0.19495.1.4**

RoleOfPspName	***N***	Une ou plusieurs valeurs suivantes, selon l'OID drs suivantes, selon lzprvantes, l • **PSP_AS** : Account Servicing Payment Service Provider (Les services de transmission de fonds)

Champ	C	Cachet
		• **PSP_PI** : Payment Initiation Service Provider (Les services d'initiation de paiement) • **PSP_AI** : Account Information Service Provider (Les services dvices dles(1) 4r les comptes) • **PSP_IC** : Payment Service Provider Issuing Card-based payment instruments (Emission d'instruments de paiement) Ce rôle est présent dans l'attestation du NCA et peut être vérifié selon le registre national REGAFI[1] ou européen EBA[2]
NCAName	***N***	Non de l'autorité compétente en anglais. Pour la France : « **Prudential Supervisory and Resolution Authority** », soit le nom en anglais de l'ACPR : Autorité de Contrôle Prudentiel et de Résolution
NCAId	***N***	Identifiant de l'autorité compétente nationale : • CaractèaraISO 3166 du code pays du NCA; • Le symbole "-" (0x2D (ASCII), U+002D (UTF-8)); • 2-8 caractère pour l'identifiant NCA sans code pays (A-Z en majuscule uniquement, sans séparateur). Pour la rancea c**FR-ACPR** La norme ETSI TS 119 495 V1.2.1 (2018-11), dresse une liste des institutions connues en Annexe D.

2.4.6 CertEurope Corp Certified

Profils de cachets (SEAL) conformes à la norme ETSI EN 319 411-1. Ces certificats se présentent soit sous la forme logicielle (LCP, NCP) ou sur support cryptographique de type SSCD (NCP+). Cette offre de certificats de cachet vise la certification ETSI.

Champ	C	Cachet
		LCP
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.24.411.1.**1**.***1***.1.0
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation, digitalSignature
Extended Key Usage	***N***	
		NCP
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.24.411.1.**2**.***1***.1.0
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation, digitalSignature
Extended Key Usage	***N***	

[1] https://www.regafi.fr/
[2] https://euclid.eba.europa.eu/register

Champ	C	Cachet
NCP+		
Certificate Policies	***N***	
PolicyIdentifier		1.2.250.1.105.23.411.1.**3**.***1***.1.0
policyQualifierId		CPS
Qualifier		https://www.certeurope.fr/chaine-de-confiance
Key usage	***O***	nonRepudiation, digitalSignature
Extended Key Usage	***N***	

2.5 Profils des certificats pour serveurs

2.5.1 Les champs communs aux certificats pour serveurs

La durée de validité des certificats varie d'une année à 2 ans pour les toutes offres (qualifiées et certifiées).

Champ	C	Valeur
Subject		
countryName		Pays dans lequel est établi ou réside le demandeur
localityName		Ville dans laquelle est établi ou réside le demandeur
StateorProvinceName		la région ou l'état où est établie la personne physique ou morale à laquelle le certificat a été délivré.
organizationName		Ce champ est **obligatoire** si le demandeur est une **personne morale**, optionnel sinon. Nom officiel complet du de l'entité tel qu'enregistré auprès des autorités compétentes
organizationIdentifier		Ce champ est **obligatoire** si le demandeur est une **personne morale**, optionnel sinon. Numéro d'immatriculation officiel de l'entité conformément à [EN_319_412-1] clause 5.1.4 • En France, ce numéro d'immatriculation peut également être constitué du préfixe « SI:FR- » ou « NTRFR- » suivi du numéro SIREN ou SIRET. • Pour les profils compatibles PSD2, ce champ est constitué du préfixe « PSDFR- » suivi de l'identifiant attribué par l'autorité national compétente (NCA). Il peut s'agir de son SIREN/SIRET, du code de la banque ou tout autre identifiant documenté par le NCA. Pour les profils de certificats qui ne dépendent pas de la réglementation EIDAS, ce champ peut être **optionnel**.
organizationUnitName		Ce champ est **obligatoire** si le demandeur est une **personne morale**, optionnel sinon. Conformément à l'Annexe 2, section VII.1 de [RGS_v2_A4], ce champ doit être présent et contenir l'identification de l'entité dont dépend le porteur : • l'ICD est sur 4 caractères ; (0002 pour la France) • l'identification de l'organisation sur 35 caractères • le séparateur entre les deux chaînes est un espace.

		Si le numéro ICD est égal à 0002, il doit impérativement être suivi d'un numéro SIREN ou SIRET puisqu'il s'agit d'un établissement enregistré en France. Pour les profils de certificats qui ne dépendent pas de la réglementation RGS, ce champ peut être **optionnel**.
commonName		(Optionnel) L'un des noms de domaine présents dans l'extension SubjectAltname
Extensions		
KeyUsage	***O***	Voir pour chaque profil décrit plus bas
SubjectAltName	***O***	Un ou plusieurs noms de domaine contrôlés par le responsable du certificat
CertificatePolicies	***N***	Voir pour chaque profil décrit plus bas
CRL Distribution Point	***N***	URL(s) de distribution de la CRL de l'AC CertEurope eID Website
Authority Information Access	***N***	URL du service OCSP de l'AC CertEurope eID Website
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC émettrice (eID Website)
SubjectKeyIdentifier	***N***	
KeyIdentifier		Identifiant de la clé publique contenue dans le certificat
BasicConstraints	***N***	
CA		Faux
QCStatements	***N***	Voir pour chaque profil décrit plus bas

2.5.2 CertEurope Website Qualified (EIDAS et RGS)

Profils de certificats conformes à la norme ETSI EN 319 411-2. Ces certificats se présentent sur un support cryptographique de type QSCD (QCP-W) ou logiciel. Ils contiennent la déclaration des certificats qualifiés définie par la norme ETSI EN 319 412-5.

Cette offre vise la qualification **EIDAS** et **RGS**.

Concernant les usages, ce qui suit respecte les exigences du RGS[3], qui sont compatibles avec les exigences EIDAS sur la délivrance de certificats qualifiés.

- L'offre **d'authentification SSL/TLS** correspond au profil **« Authentification serveur »** car une clé RSA peut nécessiter d'avoir les deux bits « keyEncipherment » et « digital signature » à 1.
- L'offre des certificats d'**authentification serveur de type client** - Les bits "digitalSignature" ou (exclusif) "keyAgreement" doivent être à "1", tous les autres bits à "0". Cela correspond donc à l'offre **« Authentification client »**

Champ	C	Authentification Client	Authentification Serveur
QCP-W			
Certificate Policies	***N***		
PolicyIdentifier		1.2.250.1.105.25.411.2.**1**.***1***.1.0	1.2.250.1.105.25.411.2.**1**.***2***.1.0
policyQualifierId		CPS	
Qualifier		https://www.certeurope.fr/chaine-de-confiance	
Key usage	***O***	digitalSignature	digitalSignature, keyEncipherment
Extended Key Usage	***N***	clientAuth	clientAuth, serverAuth

[3] RGS_v2_A4, Section II.3.2, page 11.

Champ	C	Authentification Client	Authentification Serveur
QcCompliance	***N***	esi4-qcStatement-1	
QcSSCD	***N***	Non utilisé	
QcType	***N***	esi4-qcStatement-6 = id-etsi-qct-web	
QcPDS	***N***	URL des CGUs en anglais	
QcRetentionPeriod	***N***	10 ans	
QCP-W sur support cryptographique			
Certificate Policies	***N***		
PolicyIdentifier		1.2.250.1.105.25.411.2.**2**.***1***.1.0	1.2.250.1.105.25.411.2.**2**.***2***.1.0
policyQualifierId		CPS	
Qualifier		https://www.certeurope.fr/chaine-de-confiance	
Key usage	***O***	digitalSignature	digitalSignature, keyEncipherment
SubjectAltName	***N***	Un ou plusieurs noms de domaine contrôlés par le responsable du certificat	
Extended Key Usage	***N***	clientAuth	clientAuth, serverAuth
QcCompliance	***N***	esi4-qcStatement-1	
QcSSCD	***N***	Non utilisé	
QcType	***N***	esi4-qcStatement-6 = id-etsi-qct-web	
QcPDS	***N***	URL des CGUs en anglais	
QcRetentionPeriod	***N***	10 ans	

2.5.3 CertEurope Website International (EIDAS)

Profils de certificats conformes à la norme ETSI EN 319 411-2. Ces certificats se présentent sur un support logiciel (QCP-W). Ils contiennent la déclaration des certificats qualifiés définie par la norme ETSI EN 319 412-5.

Cette offre vise uniquement la qualification **EIDAS**.

Concernant les usages qui sont compatibles avec les exigences EIDAS sur la délivrance de certificats qualifiés.

- L'offre **d'authentification SSL/TLS** correspond au profil **« Authentification serveur »** car une clé RSA peut nécessiter d'avoir les deux bits « keyEncipherment » et « digital signature » à 1.
- L'offre des certificats d'**authentification serveur de type client** - Les bits "digitalSignature" ou (exclusif) "keyAgreement" doivent être à "1", tous les autres bits à "0". Cela correspond donc à l'offre **« Authentification client »**

Champ	C	Authentification Client	Authentification Serveur
QCP-W			
Certificate Policies	***N***		
PolicyIdentifier		1.2.250.1.105.25.411.2.**3**.***1***.1.0	1.2.250.1.105.25.411.2.**3**.***2***.1.0
policyQualifierId		CPS	
Qualifier		https://www.certeurope.fr/chaine-de-confiance	
Key usage	***O***	digitalSignature	digitalSignature, keyEncipherment
Extended Key Usage	***N***	clientAuth	clientAuth, serverAuth

Champ	C	Authentification Client	Authentification Serveur
QcCompliance	***N***	esi4-qcStatement-1	
QcSSCD	***N***	Non utilisé	
QcType	***N***	esi4-qcStatement-6 = id-etsi-qct-web	
QcPDS	***N***	URL des CGUs en anglais	
QcRetentionPeriod	***N***	10 ans	

2.5.4 CertEurope Website France (RGS)

Profils de certificats conformes à la norme ETSI EN 319 411-1. Ces certificats se présentent sur un support logiciel (OVCP).

Cette offre vise uniquement la qualification **RGS**.

Concernant les usages qui sont compatibles avec les exigences RGS sur la délivrance de certificats qualifiés.

- L'offre **d'authentification SSL/TLS** correspond au profil **« Authentification serveur »** car une clé RSA peut nécessiter d'avoir les deux bits « keyEncipherment » et « digital signature » à 1.
- L'offre des certificats d'**authentification serveur de type client** - Les bits "digitalSignature" ou (exclusif) "keyAgreement" doivent être à "1", tous les autres bits à "0". Cela correspond donc à l'offre **« Authentification client »**

Champ	C	Authentification Client	Authentification Serveur
OVCP			
Certificate Policies	***N***		
PolicyIdentifier		1.2.250.1.105.25.411.1.**4**.**1**.1.0	1.2.250.1.105.25.411.1.**4**.**2**.1.0
policyQualifierId		CPS	
Qualifier		https://www.certeurope.fr/chaine-de-confiance	
Key usage	***O***	digitalSignature	digitalSignature, keyEncipherment
Extended Key Usage	***N***	clientAuth	clientAuth, serverAuth

2.5.5 CertEurope Website PSD2 (EIDAS et PSD2)

Profils de certificats conformes à la norme ETSI EN 319 411-2. Ces certificats se présentent sur un support logiciel (QCP-W). Ils contiennent la déclaration des certificats qualifiés définie par la norme ETSI EN 319 412-5.

Cette offre vise uniquement la qualification **EIDAS**.

Ci-dessous la description du profil qui correspond au cachet qualifié EIDAS auquel on ajoute les déclarations prévues par la spécification technique sur la **PSD2**.

Concernant les usages qui sont compatibles avec les exigences EIDAS et les usages de la PSD2[4] sur la délivrance de certificats qualifiés.

- L'offre **d'authentification SSL/TLS** correspond au profil **« Authentification serveur »** car une clé RSA peut nécessiter d'avoir les deux bits « keyEncipherment » et « digital signature » à 1.

[4] ETSI TS 119 495 V1.2.1 (2018-11), section *5.3 Requirements for QWAC Profile*

- L'offre des certificats d'**authentification serveur de type client** - Les bits "digitalSignature" ou (exclusif) "keyAgreement" doivent être à "1", tous les autres bits à "0". Cela correspond donc à l'offre **« Authentification client »**

Champ	C	Authentification Client	Authentification Serveur
QCP-W			
Certificate Policies	***N***		
PolicyIdentifier		1.2.250.1.105.25.411.2.**5**.***1***.1.0	1.2.250.1.105.25.411.2.**5**.***2***.1.0
policyQualifierId		CPS	
Qualifier		https://www.certeurope.fr/chaine-de-confiance	
Key usage	***O***	digitalSignature	digitalSignature, keyEncipherment
Extended Key Usage	***N***	clientAuth	clientAuth, serverAuth
QcCompliance	***N***	esi4-qcStatement-1	
QcSSCD	***N***	Non utilisé	
QcType	***N***	esi4-qcStatement-6 = id-etsi-qct-web	
QcPDS	***N***	URL des CGUs en anglais	
QcRetentionPeriod	***N***	10 ans	
Champs spécifiques à la PSD2			
QcType (PSD2)	***N***	etsi-psd2-qcStatement (0.4.0.19495.2)	
RolesOfPSP	***N***	Liste des attributs ci-après	

RoleOfPspOid	***N***	Une ou plusieurs valeurs suivantes :
		• itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 1
		  ○ PSP_AS: **0.4.0.19495.1.1**
		• itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 2
		  ○ PSP_PI : **0.4.0.19495.1.2**
		• itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 3
		  ○ PSP_AI : **0.4.0.19495.1.3**
		• itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 4
		  ○ PSP_IC : **0.4.0.19495.1.4**	

RoleOfPspName	***N***	Une ou plusieurs valeurs suivantes, selon l'OID qui aura été définit dans la section précédente • **PSP_AS** : Account Servicing Payment Service Provider (Les services de transmission de fonds) • **PSP_PI** : Payment Initiation Service Provider (Les services d'initiation de paiement) • **PSP_AI** : Account Information Service Provider (Les services d'information sur les comptes) • **PSP_IC** : Payment Service Provider Issuing Card-based payment instruments (Emission d'instruments de paiement) Ce rôle est présent dans l'attestation du NCA et peut être vérifié selon le registre national REGAFI[5] ou européen EBA[6]	
NCAName	***N***	Non de l'autorité compétente en anglais. Pour la France : « **Prudential Supervisory and Resolution Authority** », soit le nom en anglais de l'ACPR : Autorité de Contrôle Prudentiel et de Résolution	

[5] https://www.regafi.fr/
[6] https://euclid.eba.europa.eu/register

Champ	C	Authentification Client	Authentification Serveur
NCAId	***N***	Identifiant de l'autorité compétente nationale : • Caractère ISO 3166 du code pays du NCA; • Le symbole "-" (0x2D (ASCII), U+002D (UTF-8)); • 2-8 caractère pour l'identifiant NCA sans code pays (A-Z en majuscule uniquement, sans séparateur). Pour la France : **FR-ACPR** L'annexe D du référentiel technique ETSI TS 119 495 V1.2.1 (2018-11), dresse une liste des identifiants par pays.	

2.5.6 CertEurope EV SSL

Profils de certificats conformes à la norme ETSI EN 319 411-1. Ces certificats se présentent soit sous la forme logicielle ou sur support cryptographique de type SSCD. Ce profil requiert une validation étendue (EVCP)

Champ	C	Authentification Client	Authentification Serveur
EVCP			
Certificate Policies	***N***		
PolicyIdentifier		1.2.250.1.105.25.411.1.**3**.***1***.1.0	1.2.250.1.105.25.411.1.3.***2***.1.0
policyQualifierId		CPS	
Qualifier		https://www.certeurope.fr/chaine-de-confiance	
Key usage	***O***	digitalSignature	digitalSignature, keyEncipherment
Extended Key Usage	***N***	clientAuth	clientAuth, serverAuth

2.5.7 CertEurope SSLDomain

Profils de certificats conformes à la norme ETSI EN 319 411-1. Ces certificats se présentent soit sous la forme logicielle ou sur support cryptographique de type SSCD. Ce profil requiert une validation du domaine associé au certificat (DVCP)

Champ	C	Authentification Client	Authentification Serveur
DVCP			
Certificate Policies	***N***		
PolicyIdentifier		1.2.250.1.105.25.411.1.**1**.***1***.1.0	1.2.250.1.105.25.411.1.1.***2***.1.0
policyQualifierId		CPS	
Qualifier		https://www.certeurope.fr/chaine-de-confiance	
Key usage	***O***	digitalSignature	digitalSignature, keyEncipherment
Extended Key Usage	***N***	clientAuth	clientAuth, serverAuth

2.5.8 CertEurope SSLOrganisation

Profils de certificats conformes à la norme ETSI EN 319 411-1. Ces certificats se présentent soit sous la forme logicielle ou sur support cryptographique de type SSCD. Ce profil requiert une validation des données de l'organisation qui demande le certificat (OVCP).

Champ	C	Authentification Client	Authentification Serveur
OVCP			
Certificate Policies	***N***		
PolicyIdentifier		1.2.250.1.105.25.411.1.**2**.***1***.1.0	1.2.250.1.105.25.411.1.**2**.***2***.1.0
policyQualifierId		CPS	
Qualifier		https://www.certeurope.fr/chaine-de-confiance	
Key usage	***O***	digitalSignature	digitalSignature, keyEncipherment
Extended Key Usage	***N***	clientAuth	clientAuth, serverAuth

3 Profil des LCR

2.1.1. CHAMPS DES LCR

Champs de base	Valeur
Version	Version 2
Signature	Sha256WithRSAEncryption (2.16.840.1.101.3.4.2.1)
Hash	sha256
Issuer DN	Selon l'émetteur de chaque AC décrite plus haut
This Update	Au plus tôt à la date de début de vie de l'AC
Next Update	Prochaine date à laquelle la CRL sera mise à jour, soit 6 jours après la date de génération de la présente CRL.
Revoked Certificates	N° de série des certificats révoqués. Exemple : « 0C0062 »
Revocation Date	Date à laquelle un Certificat donné a été révoqué.

2.1.2. EXTENSIONS DES LCR

Champ	O	C	Valeur
Authority Key Identifier	TRUE	FALSE	ID de la clé=voir la clé de chaque AC décrite plus haut
CRL Number	TRUE	FALSE	N° de série de la CRL Exemple : « 0115 »

4 Protocole de vérification de certificat en ligne (OCSP)

Bien que les exigences complémentaires n'imposent pas la mise en place d'un répondeur OCSP, la version 2 du RGS l'impose. C'est aussi une obligation du CA/B Forum.

Les réponses OCSP doivent se conformer à la RFC6960 et / ou RFC5019. Ainsi, il y a deux possibilités :

1. Être signé par l'AC qui a délivré les certificats dont le statut de révocation est vérifié, ou
1. Être signé par un répondeur OCSP dont le certificat est signé par l'AC qui a délivré le certificat dont l'état de révocation est vérifié.

Dans ce dernier cas, le certificat de signature OCSP doit contenir une extension de type id-pkix-ocsp-nocheck, comme défini par RFC6960.

Les AC intermédiaires eID User/Corp/Website ne signent donc pas les réponses OCSP et par conséquent ne contiennent pas le keyUsage digitalSignature comme préconisé par le RGS qui reprend les préconisations du CAB Forum.

4.1 Les champs communs aux certificats de signature OCSP

Chaque AC intermédiaire possède son propre serveur OCSP. Les bi-clés pour chaque AC ont une durée maximum de validité d'un an.

CertEurope eID OCSP		
Champ	*C*	*Valeur*
Version		V3
SerialNumber		Fourni par l'AC
KeySize		2048 bits (RSA)
SignatureAlgorithm		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Signature Value		Fourni par l'AC
Validity		Maximum 1 an
NotBefore		Date de la génération de la bi-clé
NotAfter		Date de la génération de la bi-clé + 1 an au maximum
SubjectPublicKeyInfo		La clé publique avec une longueur de 2048 bits (RSA)
Issuer		
CountryName		FR
CommonName		CertEurope eID Root
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
OrganizationIdentifier		SI:FR-434202180
Subject		
CountryName		FR
CommonName		Chaque AC intermédiaire possède son propre serveur/certificat OCSP : • CertEurope eID OCSP Root • CertEurope eID OCSP User • CertEurope eID OCSP Corp • CertEurope eID OCSP Website
OrganizationName		CertEurope
OrganizationUnitName		0002 434202180
Extensions		
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC émettrice
SubjectKeyIdentifier	***N***	
KeyIdentifier		Empreinte MD5 de l'AC

4.2 Les profils des certificats OCSP

Champ	C	eID OCSP Root	eID OCSP User	eID OCSP Corp	eID OCSP Website
Certificate Policies	***N***				
PolicyIdentifier		1.2.250.1.105.22.6960.1.0	1.2.250.1.105.23.6960.1.0	1.2.250.1.105.24.6960.1.0	1.2.250.1.105.25.6960.1.0
policyQualifierId		CPS			
Qualifier		https://www.certeurope.fr/chaine-de-confiance			
Key usage	***O***	digitalSignature			
Extended Key Usage	***N***	OCSP Signing with no-check			