DECLARATION DES PRATIQUES DE CERTIFICATION

Autorité de certification

« CertEurope eID Website »
Certification d'authentification qualifiés pour des sites web

Identification (OID) : 1.2.250.1.105.32.411.2.1.0

Version : 1.1
Mise à jour : 00
Date de création : 14 novembre 2016
Dernière MAJ : 10 septembre 2019
Etat du document : Officiel
Rédigé par : CertEurope
Vérifié par : COSSI
Approuvé par : COSSI

CertEurope, une société du groupe Oodrive
www.CertEurope.fr
26, rue du Faubourg Poissonnière, 75010 Paris – France
Tel : +33 (0)1 45 26 72 00 / Fax : +33 (0)1 45 26 72 01

MODIFICATIONS			
Date	Etat	Version	Commentaires
14/11/2016	Draft	1.0	
10/09/2019	Officiel	1.1	Ajout de la hiérarchie complète des AC en annexe Revue annuelle de la PSSI Publication des CRLs après terminaison d'une AC

DOCUMENTS REFERENCES		
Date	Version	Commentaires
[PC RGSV3.0]	3.0	PC Type Authentification Serveur V3.0 du référentiel RGS v1.0
[PROFILS]	3.0	Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques
[ETSI_CERT]		Norme ETSI EN 319 411-1/2
[RFC3647]	Novembre 2003	IETF – Internet X509 Public Key Infrastructure – Certificate Policy and Certification Practice Framework.
[RFC3039]		RFC 3039 : profil pour les certificats qualifiés
[CERT_PSSI]		CertEurope : Politique de Sécurité
[PC CERTEUROPE eID Website]	1.0	Politique de Certification de CERTEUROPE eID Website

SOMMAIRE

1. Introduction

1.1. Présentation générale

La « Déclaration des Pratiques de Certification » (DPC) est un énoncé des pratiques qu'une Autorité de Certification utilise dans la gestion des Certificats.
Une DPC donne une description précise des services et des procédures de fonctionnement réels d'une Infrastructure à Clés Publiques (ICP), y compris les services propriétaires ou implémentés de manière particulière.
Cette DPC est donc associée à la PC relative à l'AC CERTEUROPE ; la DPC n'est pas diffusée de la même façon que la PC qui, elle, est publique, et sa consultation doit faire l'objet d'une demande argumentée auprès de l'AC CERTEUROPE.
Les procédures de l'Opérateur de Services de Certification (OSC) auxquelles cette DPC fait référence sont la propriété de CertEurope. Leur consultation doit faire l'objet d'une demande argumentée auprès de CertEurope.
Cette DPC vise la conformité aux documents suivants :

- Exigences du Référentiel Global de Sécurité (RGS) v2.0 aux niveaux (*) (**) pour les profils « Confidentialité », « Authentification et signature », « Authentification » et « Signature ».
- Exigences de la réglementation européenne EIDAS pour le profil QCP-W de la norme ETSI EN 319 411-2
- La RFC3647 de l'IETF [RFC3647]
- La PSSI de CertEurope (Politique de Sécurité). Ce document est revu annuellement par l'équipe sécurité de CertEurope

1.2. Identification du document

La présente Déclaration de Pratiques de Certification est identifiée par l'OID 1.2.250.1.105.32.411.2.1.0

Les OIDs respectent le schéma de numérotation suivant :
1.2.250.1.105.**DPC**.**NORME**.**PARTIE**.**MAJEURE**.**VERSION.MINEURE**

- 1.2.250.1.105 : CertEurope
- DPC : Déclaration des pratiques de certification pour les offres personnes physiques (30), les personnes morales (31) ou les sites web (32)
- NORME : la norme en vigueur (EN 319 411 = **411**)
- PARTIE : partie de la norme (EN 319 411-**2 = 2)**
- VERSION MAJEURE : version majeure de la DPC
- VERSION MINEURE : version mineure de la DPC

Ce document correspond aux Politiques de Certification référencées par les OIDs suivants :

OID	Usages		Niveau de qualification	
	AUTH	CNFD	RGS v2	EIDAS
1.2.250.1.105.**25.411.2.1**.1.*1.0*	X		*	QCP-W
1.2.250.1.105.**25.411.2.1**.2.*1.0*	X	X	*	QCP-W
1.2.250.1.105.**25.411.2.2**.1.*1.0*	X		**	QCP-W
1.2.250.1.105.**25.411.2.2**.2.*1.0*	X	X	**	QCP-W

Les Politique de Certification et Déclaration des Pratiques de Certification sont ci-après désignées sous le nom de "PC" et de "DPC".

1.3. Entités intervenant dans l'ICP

L'Infrastructure à Clés Publiques (ICP) est composée de plusieurs entités, lesquelles sont décrites ci-après.

1.3.1. Autorités de certification

Voir § 1.3.1 de la PC

1.3.2. Autorités d'enregistrement
Voir § 1.3.2 de la PC

1.3.3. Responsable de Certificats d'authentification serveur
Voir § 1.3.3 PC

1.3.4. Utilisateurs de certificats
Voir § 1.3.4 PC

1.3.5. Autres participants
1.3.5.1. Composantes de l'IGC
1.3.5.1.1. Autorité de Certification
L'AC a en charge, au nom et sous la responsabilité du PSCE, l'application de la PC. L'AC est représentée par CertEurope.

1.3.5.1.2. Autorité d'Enregistrement
L'AE a en charge, sous la responsabilité du PSCE, les services suivants :

- service d'enregistrement,
- service de remise au RCAS,
- service de gestion des révocations.

Dans certains cas, l'AE peut disposer d'un service central qui assure les Services d'enregistrement et de gestion des révocations et un service local (bureau d'enregistrement) qui assure le Service de remise du certificat au RCAS.

L'Autorité d'Enregistrement a la possibilité de déléguer certains services à des entités :

- Autorité d'Enregistrement Administrative : AEA, chargée de vérifier l'identité et la qualité d'un demandeur de certificat ;
- Autorité d'Enregistrement Technique : AET, chargée de la génération et de la révocation du certificat d'authentification serveur ;
- Autorité d'Enregistrement Déléguée ou de Délivrance : AED, chargée de l'envoi du certificat contre récépissé, au RCAS. Pour le niveau (**), l'AED peut également être en charge de l'authentification du RCCS en face-à-face. L'AED agit sous la responsabilité exclusive de l'AEA et ne constitue pas un rôle de confiance en soi

L'OC est représentée par CertEurope.

1.3.5.2. Mandataire de certification
Voir § 1.3.5.2 de la PC

1.3.5.3. Opérateur de Certification
L'OC a en charge, sous la responsabilité du PSCE, les services suivants :

- service de génération de certificat,
- service de publication et de diffusion,
- service de gestion des révocations,
- service d'assistance au RCAS.

L'OC doit respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

1.4. Usage des certificats

1.4.1. Domaine d'utilisation applicables

1.4.1.1. Bi-clés et certificats du serveur informatique

Voir § 1.4.1.1 PC

1.4.1.2. Bi-clés et certificats d'AC et de composantes

Voir § 1.4.1.2 PC

1.4.2. Domaine d'utilisation interdits

Voir § 1.4.2. PC

1.5. Gestion de la DPC

1.5.1. Entité gérant la DPC

1.5.1.1. Organisme responsable

Voir § 1.5.1.1 de la PC

1.5.1.2. Personne physique responsable

Voir § 1.5.1.2 de la PC

1.5.2. Point de contact

Voir § 1.5.2 de la PC

1.5.3. Entité déterminant la conformité de la DPC à la PC

La Direction de CertEurope détermine la conformité de la DPC à la PC, après approbation par le Comité PKI de CertEurope. Le document « [36] CertEurope – PV de conformité de la DPC à la PC » est signé par les membres du comité et la Direction de CertEurope.

1.5.4. Procédures d'approbation de la conformité de la DPC

Voir § 1.5.4 de la PC et document « *[07] CERTEUROPE – Rôles et habilitations* ».

1.6. Définitions et acronymes

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AEA	Autorité d'Enregistrement Administrative
AET	Autorité d'Enregistrement Technique
AED	Autorité d'Enregistrement Déléguée
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
C	Country (Pays)
CEN	Comité Européen de Normalisation
CISSI	Commission Interministérielle pour la Sécurité des Systèmes d'Information
CN	Common Name
CSR	Certificate Signing Request
DDS	Dossier de Souscription
DSIC/SGMAP	Direction des systèmes d'information et de communication/Secrétariat général pour la modernisation de l'action publique
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification, ou EPC
DSA	Digital Signature Algorithm

EAR	Entité d'Audit et de Référencement
EPC	Enoncé des Pratiques de Certification, ou DPC
ETSI	European Telecommunications Standards Institute
ICP	Infrastructure à Clés Publiques
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
LDAP	Light Directory Access Protocol
MC	Mandataire de Certification
MD5	Message Digest n°5
MINEFI	Ministère de l'Économie et des Finances
O	Organisation
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organisation Unit
PC	Politique de Certification
PDS	Déclaration de divulgation d'IGC (PKI Disclosure Statement)
PIN	Personal Identification Number
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique
RGS	Référentiel Global de Sécurité
RSA	Rivest Shamir Adelman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SN	Serial Number
SSCD	Dispositif Sécurisé de Création de Signature
SHA256	Secure Hash Algorithm 256
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator

1.6.1. Termes communs au RGS

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du serveur.

Autorités administratives - Ce terme générique désigne les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité d'horodatage - Autorité responsable de la gestion d'un service d'horodatage (cf. politique d'horodatage type du RGS).

Infrastructure de gestion de clés (IGC) - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée

d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Produit de sécurité - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en oeuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Promoteur d'application - Un responsable d'un service de la sphère publique accessible par voie électronique.

Qualification des produits de sécurité - Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS]. La procédure de qualification des produits de sécurité est décrite dans le [DécretRGS]. Le [RGS] précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

1.6.2. Termes spécifiques ou complétés / adaptés pour la présente DPC

Applicatif de vérification d'authentification - Il s'agit de l'application mise en oeuvre par l'utilisateur ou le serveur pour vérifier l'authentification d'un autre serveur et établir une session sécurisée avec ce serveur, notamment générer la clé symétrique de session et la chiffrer avec la clé publique du serveur contenue dans le certificat correspondant.

Autorité de certification (AC) - Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une Politique de Certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette Politique de Certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre 1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la Politique de Certification, répondant aux exigences de la présente PC.

Autorité d'enregistrement - cf. § 1.3.2 de la PC

Certificat électronique - Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente PC Type, le terme "certificat électronique" désigne uniquement un certificat délivré à un serveur informatique sous la responsabilité d'un RCAS et portant sur une bi-clé d'authentification et d'échange de clés symétriques de session, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction ou service de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

Communauté : ensemble de personnes liées entre elles soit par des contrats (exemples : une entreprise et ses fournisseurs, des employés d'une entreprise..) soit par leur qualité (membres d'un ordre….)

Compromission : une clé est dite compromise lorsqu'elle est connue par d'autres personnes que celles habilitées à la mettre en œuvre.

Déclaration des pratiques de certification (DPC) - Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les Politiques de Certification qu'elle s'est engagée à respecter.

Dispositif de protection des clés privées - Il s'agit du dispositif matériel et/ou logiciel utilisé par le serveur pour stocker et mettre en oeuvre sa clé privée.

Dossier de Souscription (DDS) : ensemble des pièces justificatives à fournir à l'AE afin de lui permettre de vérifier les informations demandées par l'AC pour l'émission d'un Certificat. Ces pièces justificatives sont décrites dans la présente PC.

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

Mandataire de certification - cf. § 1.3.5.2 de la PC

Personne autorisée - cf. § 1.3.1 de la PC

Politique de certification (PC) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les RCAS et les utilisateurs de certificats.

Prestataire de services de certification électronique (PSCE) - Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des RCAS et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

Référencement - Opération qui consiste, pour l'Administration, à tenir à jour la liste des offres de certification électronique des PSCE qui répondent à des exigences spécifiées dans le RGS. Seuls les certificats d'offres référencées peuvent être utilisés dans le cadre des échanges dématérialisés de l'Administration. Une offre référencée par rapport à un service donné et un niveau de sécurité donné du RGS peut être utilisée dans toutes les applications d'échanges dématérialisés requérant ce service et ce niveau de sécurité ou un niveau inférieur. Pour les usagers, le référencement permet de connaître quelles offres de certificats électroniques ils peuvent utiliser pour quels échanges dématérialisés.

Responsable du Certificat d'Authentification Serveur : cf § 1.3.1 de la PC

Serveur informatique - Il s'agit d'un service applicatif (disposant d'un certificat fourni par l'AC) rattaché à l'entité, (identifiée dans le certificat) détenant le nom de domaine correspondant au service ou en charge de ce service.

Service d'enregistrement : cf. § 1.3.1 de la PC

Service de génération des certificats cf. § 1.3.1 de la PC
Service de publication et diffusion : cf. § 1.3.1 de la PC
Service de gestion des révocations : cf. § 1.3.1 de la PC
Service d'information sur l'état des certificats : cf. § 1.3.1 de la PC
Service d'assistance aux RCAS : cf. § 1.3.1 de la PC

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une personne morale dans ses relations avec une administration.
Nota - Un agent d'une autorité administrative qui est en relation avec une autre autorité administrative est, pour cette dernière, un usager.

Utilisateur de certificat - cf. § 1.3.1 de la PC

2. Responsabilités concernant la mise à disposition des informations devant être publiées

2.1. Entités chargées de la mise à disposition des informations

Voir le § 2.1 de la PC.

2.2. Informations devant être publiées

Voir le § 2.2 de la PC.

2.3. Délais et fréquences de publication

Voir §2.3 de la PC

2.4. Contrôle d'accès aux informations publiées

Les exigences sont définies dans le § 2.4. de la PC. L'accès en modification du système de publication des informations d'état de certificats nécessite un contrôle d'accès fort via l'utilisation d'un VPN puis une connexion par login / mot de passe. Ce VPN nécessite l'utilisation d'un certificat.

L'accès est autorisé aux personnes habilitées conformément au document « *[07] CERTEUROPE – Rôles et habilitations* ».

3. Identification et authentification

3.1. Nommage

3.1.1. Types de noms

Voir § 3.1.1 de la PC.

3.1.2. Nécessité d'utilisation de noms explicites

Voir § 3.1.2 de la PC.

3.1.3. Anonymisation et pseudonymisation des serveurs

Sans objet

3.1.4. Règles d'interprétation des différentes formes de nom

Voir § 3.1.4 de la PC.

3.1.5. Unicité des noms

Voir § 3.1.5 de la PC.

3.1.6. Identification, authentification et rôle des marques déposées

Voir § 3.1.6 de la PC.

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clé privée

Par l'envoi de la requête de demande de certificat, par le RCAS, l'AC considère que la clé privée est en possession de l'entité demandeur de certificat.

3.2.2. Validation de l'identité d'un organisme

Voir § 3.2.3.

3.2.3. Validation de l'identité d'un individu

La relation entre le RCAS représentant une entité et l'AC est formalisée dans le document « *[24] CERTEUROPE – Contrat d'abonnement* ». Ce contrat est composé de conditions particulières et générales.

Dans le cadre de la présente Politique de Certification, on entend par justificatif d'identité, un document délivré par une autorité administrative comportant la photographie, le(s) nom(s), le(s) prénom(s), la date et le lieu de naissance du titulaire, ainsi qu'un numéro unique et une date de délivrance. Sont notamment acceptés : la carte nationale d'identité française, le passeport et la carte de séjour délivrée par les autorités françaises, sous réserve que ces documents soient en cours de validité. Le permis de conduire français est accepté s'il a été délivré moins de quinze ans avant la demande de certificat. Pour tous les autres documents, tels que les cartes d'identité étrangères ou les cartes professionnelles, l'opérateur AE devra obtenir l'autorisation de l'AC avant de valider le dossier et, le cas échéant, être en mesure de vérifier raisonnablement l'authenticité du document.

3.2.3.1. Enregistrement d'un RCAS sans MC

Le dossier d'enregistrement doit être déposé auprès de l'AE (envoi du dossier par courrier postal) et doit comprendre :

- Une demande de certificat :
  - une demande de certificat écrite, datée de moins de 3 mois, signée par un représentant légal de l'entité et comportant le FQDN/nom du serveur concerné par cette demande, « *[24] CERTEUROPE – Contrat d'abonnement* »
  - les conditions générales d'utilisation signées par le RCAS « *[23] CERTEUROPE – Conditions Générales* »

- Un mandat daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être RCAS pour la ou les machines sur lesquelles sera déployé le certificat d'authentification serveur devant être délivré. Ce mandat est signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCAS, « *[24] CERTEUROPE – Contrat d'abonnement* »

- Les pièces justificatives de l'entité (Entreprise) :
  - une photocopie d'un justificatif d'identité du représentant légal.
  - une pièce valide au moment de l'enregistrement portant le numéro d'identification de l'entreprise (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou répertoire des métiers)
- Les pièces justificatives de l'identité du RCAS :
  - une photocopie d'un justificatif d'identité du RCAS.

Pour le niveau (*), l'authentification du RCAS se fait par l'envoi à l'AE du dossier comprenant toutes les pièces citées ci-dessus. La photocopie des pièces d'identité doit être certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").

Pour le niveau (**), l'authentification du RCAS par l'AE se fait lors d'un face-à-face physique à l'enregistrement. Ce face-à-face fait l'objet de la signature d'un PV de face-à-face « [33] CERTEUROPE – PV de face-à-face pour le niveau (**) »

Des procédures dérogatoires à cet enregistrement peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

3.2.3.2. Enregistrement d'un nouveau RCAS sans MC pour un certificat d'authentification serveur déjà émis

En cas de changement de RCAS pour un certificat d'authentification serveur en cours de validité, il est nécessaire de suivre une procédure d'enregistrement du nouveau RCAS.

Le dossier d'enregistrement du nouveau RCAS doit être déposé auprès de l'AE (envoi du dossier par courrier postal) et doit comprendre :

- Un mandat daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être RCAS pour la ou les machines sur lesquelles sera déployé le certificat d'authentification serveur devant être délivré, en remplacement de l'ancien RCAS. Ce mandat est signé par un représentant légal de l'entité et co-signé, pour acceptation, par le futur RCAS, « *[25] CERTEUROPE – Contrat d'abonnement – Changement de RCAS* »
- les conditions générales d'utilisation signées par le nouveau RCAS « *[23] CERTEUROPE – Conditions Générales* »
- Les pièces justificatives de l'identité du nouveau RCAS
  - une photocopie d'un justificatif d'identité du nouveau RCAS.

Pour le niveau (*), l'authentification du RCAS se fait par l'envoi à l'AE du dossier comprenant toutes les pièces citées ci-dessus. La photocopie de la pièce d'identité doit être certifiée conforme par le RCCS (date, de moins de 3 mois, et signature sur la photocopie précédées de la mention "copie certifiée conforme à l'original").

Pour le niveau (**), l'authentification du RCAS par l'AE se fait lors d'un face-à-face physique à l'enregistrement. Ce face-à-face fait l'objet de la signature d'un PV de face-à-face « [33] CERTEUROPE – PV de face-à-face pour le niveau (**) »

3.2.3.3. Enregistrement du Mandataire de Certification

L'enregistrement d'un RCAS peut se faire via un Mandataire de Certification. Dans ce cas, le MC doit être préalablement enregistré par l'AE.
Une AE est amenée à constituer un dossier d'enregistrement pour un Mandataire de Certification (MC) pour répondre au besoin suivant :

- Utilisation du dossier du MC comme référence pour les données d'identification de l'entité de tous les RCAS présentés par le MC.

Le dossier d'enregistrement d'un MC, déposé directement auprès de l'AE, doit comprendre :

- un mandat, daté de moins de 3 mois, désignant le Mandataire de Certification. Ce mandat doit être signé par le représentant légal et le MC.
  Par ce mandat, le MC s'engage auprès de l'AC, à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs.
  Par ce mandat, le MC s'engage à signaler à l'AE son départ de l'entité.
- Les pièces justificatives de l'identité du MC :
  - une photocopie d'un justificatif d'identité du MC.
- Les pièces justificatives de l'entité (Entreprise) :
  - une photocopie d'un justificatif d'identité du représentant légal.
  - Tout document attestant de la qualité du signataire du mandat ;

Pour le niveau (*), l'authentification du MC se fait par l'envoi à l'AE du dossier comprenant toutes les pièces citées ci-dessus. Les personnes concernées doivent signer cette photocopie et y ajouter la date de signature ainsi que la mention « copie certifiée conforme à l'original ». Cette pièce est considérée valide durant 3 mois à compter de la date de signature.

Pour le niveau (**), l'authentification du MC par l'AE se fait lors d'un face-à-face physique à l'enregistrement. Ce face-à-face fait l'objet de la signature d'un PV de face-à-face « [33] CERTEUROPE – PV de face-à-face pour le niveau (**) »

3.2.3.4. Enregistrement d'un RCAS via un MC pour un certificat d'authentification serveur à émettre

Le dossier d'enregistrement, déposé auprès du MC, doit comprendre :

- une demande de certificat écrite, datée de moins de 3 mois, signée par le MC et comportant le nom du service de création de cachet concerné par cette demande, « *[24] CERTEUROPE – Contrat d'abonnement* »
- les conditions générales d'utilisation signées par le RCAS « *[23] CERTEUROPE – Conditions Générales* »
- Un mandat daté de moins de 3 mois, désignant le futur RCCS comme étant habilité à être RCAS pour le service de création de cachet pour lequel le certificat de cachet doit être délivré. Ce mandat est signé par le MC de l'entité et co-signé, pour acceptation, par le futur RCAS, « *[24] CERTEUROPE – Contrat d'abonnement* »
- Les pièces justificatives de l'identité du RCAS
  - une photocopie d'un justificatif d'identité du RCAS.

Pour le niveau (*), l'authentification du RCAS se fait par l'envoi à l'AE du dossier comprenant toutes les pièces citées ci-dessus. Le RCAS doit signer cette photocopie et y ajouter la date de signature ainsi que la mention « copie certifiée conforme à l'original ». Cette pièce est considérée valide durant 3 mois à compter de la date de signature.

Pour le niveau (**), l'authentification du RCAS par le MC se fait lors d'un face-à-face physique. Ce face-à-face fait l'objet de la signature d'un PV de face-à-face « [33] CERTEUROPE – PV de face-à-face pour le niveau (**) »

3.2.3.5. Enregistrement d'un RCAS via un MC pour un certificat d'authentification serveur déjà émis

Dans le cas de changement d'un RCAS en cours de validité d'un certificat de cachet, le nouveau RCAS est enregistré en tant que tel par l'AC en remplacement de l'ancien RCAS.

L'enregistrement du nouveau RCAS (personne physique) représentant une entité nécessite l'identification de la personne physique et la vérification de son habilitation en tant que représentant de l'entité à laquelle le service de création de cachet est rattaché et en tant que RCAS pour ce service.

Le dossier d'enregistrement, déposé auprès d'un MC, doit au moins comprendre :

- Un mandat daté de moins de 3 mois, désignant le futur RCAS comme étant habilité à être RCAS pour le service de création de cachet pour lequel le certificat de cachet doit être délivré, en remplacement de l'ancien RCAS. Ce mandat est signé par le MC de l'entité et co-signé, pour acceptation, par le futur RCAS, « *[25] CERTEUROPE – Contrat d'abonnement – Changement de RCAS* »
- les conditions générales d'utilisation signées par le RCAS « *[23] CERTEUROPE – Conditions Générales* »
- Les pièces justificatives de l'identité du nouveau RCAS
    - une photocopie d'un justificatif d'identité du nouveau RCAS.

Pour le niveau (*), l'authentification du RCAS se fait par l'envoi à l'AE du dossier comprenant toutes les pièces citées ci-dessus. Le RCAS doit signer cette photocopie et y ajouter la date de signature ainsi que la mention « copie certifiée conforme à l'original ». Cette pièce est considérée valide durant 3 mois à compter de la date de signature.

Pour le niveau (**), l'authentification du RCAS par le MC se fait lors d'un face-à-face physique. Ce face-à-face fait l'objet de la signature d'un PV de face-à-face « [33] CERTEUROPE – PV de face-à-face pour le niveau (**) »

3.2.4. Informations non vérifiées du RCAS et/ou du serveur informatique

Sans objet.

3.2.5. Validation de l'autorité du demandeur

Le dossier d'enregistrement, déposé auprès de l'AE avec ou sans MC, doit comprendre obligatoirement :

- un mandat du représentant légal ou du MC désignant une personne physique comme étant habilité à être RCAS pour la ou les machines sur lesquelles sera déployé le certificat d'authentification serveur devant être délivré. Ce mandat doit être signé pour acceptation par la personne physique bénéficiaire. « *[24] CERTEUROPE – Contrat d'abonnement* »;
- une photocopie d'un justificatif d'identité du représentant légal. Le représentant légal doit signer cette photocopie et y ajouter la date de signature ainsi que la mention « copie certifiée conforme à l'original ». Cette pièce est considérée valide durant 3 mois à compter de la date de signature.
- une pièce valide au moment de l'enregistrement portant le numéro d'identification de l'entreprise (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou répertoire des métiers)

3.2.6. Certification croisée d'AC

Sans objet.

3.3. Identification et validation d'une demande de renouvellement des clés

3.3.1. Identification et validation pour un renouvellement courant

Le renouvellement courant de certificat nécessite la constitution d'un dossier identique à la demande initiale.

3.3.2. Identification et validation pour un renouvellement après révocation

Le renouvellement de certificat après révocation nécessite la constitution d'un dossier identique à la demande initiale.

3.4. Identification et validation d'une demande de révocation

Les demandes de révocation peuvent être réalisées par le RCAS, le MC, le représentant légal, l'AC CERTEUROPE ou l'AE.

Les demandes de révocation peuvent être effectuées :

- par l'envoi d'une demande manuscrite signée (RCAS, MC ou représentant légal) cf. « *[28] CERTEUROPE – Demande de révocation* ». Dans ce cas, elle est adressée par voie postale directement à l'AC.

La demande de révocation manuscrite comprend :

- le document de demande de révocation signé par le RCAS ou par le représentant légal ou encore par le Mandataire de Certification « *[28] CERTEUROPE – Demande de révocation* » ;
- une copie du justificatif d'identité du demandeur.

Dès réception de la demande de révocation, l'AE :

- compare la signature manuscrite présente sur la demande de révocation avec celle présente sur la copie de la pièce d'identité afin d'authentifier le demandeur
- vérifie son autorité par rapport au certificat à révoquer, par tout moyen mis à sa disposition, notamment en consultant le DDS ou en utilisant l'application de suivi du cycle de vie des certificats.

Des procédures dérogatoires à cet enregistrement peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de Certificat

4.1.1. Origine de la demande

Voir § 4.1.1 de la PC

4.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat

La procédure de demande de Certificat figure dans le document « *[30] CERTEUROPE – Guide de l'AE* ».

4.2. Traitement d'une demande de certificat

4.2.1. Exécution des processus d'identification et de validation de la demande

L'AE s'engage à effectuer les tâches suivantes :

- le contrôle du dossier DDS (dossier complet), à savoir : « *[24] CERTEUROPE – Contrat d'abonnement* », « *[23] CERTEUROPE – Conditions Générales* » et « *[26] CERTEUROPE – Procuration du représentant légal – Désignation d'un MC* » dans le cas d'une demande via un MC.
- vérification que le futur RCAS a pris connaissance des modalités applicables pour l'utilisation du certificat. Pour cela, l'AE vérifie que le RCAS a paraphé le document « *[23] CERTEUROPE – Conditions Générales* ».
- la vérification avec un soin raisonnable de la vraisemblance des pièces constitutives du Dossier de Souscription (Pièces d'identité, mandats, …); et en particulier de l'identité du futur RCAS ou MC le cas échéant ;

Dans le cas d'une demande via un MC, celui-ci retransmet le dossier à l'AE après avoir effectué les opérations ci-dessus.

Pour l'ensemble de ces vérifications, l'AE s'appuie sur du personnel dûment identifié par le document « *[07] CERTEUROPE – Rôles et habilitations »* et porteur d'un certificat remis en face à face par l'AC. Les AE ont été spécialement formées aux procédures de vérification, et sont auditées régulièrement par l'AC.
La procédure de traitement d'un Dossier de Souscription (DDS) repose sur les principes formalisés dans le guide « *[30] CERTEUROPE – Guide de l'AE* ».

L'AE effectue ensuite l'archivage du dossier (DDS) conformément à la procédure d'archivage « *[17] CERTEUROPE – Archivage des données de l'IGC* » et « *[29] CERTEUROPE – Contrôle et archivage des dossiers* ».
Des procédures dérogatoires à cet enregistrement peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

4.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le RCAS ou, le MC le cas échéant, par courrier en justifiant le rejet.

4.2.3. Durée d'établissement du certificat

Voir § 4.2.3 de la PC

4.3. Délivrance du certificat

4.3.1. Actions de l'AC concernant la délivrance de certificat

Une fois le DDS contrôlé, l'AE reçoit la demande sous forme de CSR.
Cette CSR contient :

- La clé publique du serveur
- Les informations d'identification choisies par l'entreprise (informations qui figureront dans le certificat)

L'AE transmet la CSR à la plate-forme de certification de CertEurope.

La plate-forme de l'AC CERTEUROPE contrôle les champs du certificat ainsi que l'origine (AE) de la demande. Si ceux-ci sont valides l'AC CERTEUROPE signe le certificat.
L'AE envoie le certificat au RCAS et au MC qui le représente le cas échéant.
Le document « *[30] CERTEUROPE – Guide de l'AE* » décrit de manière plus détaillée la procédure de traitement d'une demande de certificat.

Pour le niveau (**), la transmission de la CSR se fait lors d'un face-à-face physique, sur un support au choix du RCAS (clé USB, cdrom…). Un PV de face-à-face « [33] CERTEUROPE – PV de face-à-face pour le niveau (**) » est établi.

4.3.2. Notification par l'AC de la délivrance du certificat au RCAS

Le RCAS est notifié immédiatement par email dès la génération de son certificat.
La remise du certificat est effectuée par email par l'AE au RCAS, au MC ou au Représentant Légal. A l'issue de cet envoi, le document « *[27] CERTEUROPE – Accusé de réception du certificat* » est cosigné par les deux parties.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

Voir § 4.4.1. de la PC.

Récupération du certificat par le RCAS :
Le certificat est envoyé par email à l'adresse mentionnée par le RCAS dans le DDS.
Une fois le certificat reçu, le RCAS retourne à l'AE le document « *[27] CERTEUROPE – Accusé de réception du certificat* » signé. Le document est ensuite co-signé par l'AE. Celui-ci est conservé par l'AE qui le remonte à l'AC ultérieurement.

Récupération du certificat par le MC :
Le certificat est envoyé par email aux adresses mentionnées dans le DDS par le RCAS et le MC le cas échéant.
Une fois le certificat reçu, le MC retourne à l'AE le document « *[27] CERTEUROPE – Accusé de réception du certificat* » signé. Le document est ensuite co-signé par l'AE. Celui-ci est conservé par l'AE qui le remonte à l'AC ultérieurement.

4.4.2. Publication du certificat

Les certificats des RCAS ne sont pas publiés.

4.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

Notification de l'AC à l'AE :
Le mode de délivrance de certificat décrit dans le chapitre § 4.3.1 indique que l'AE est notifiée par l'AC de la génération du certificat d'authentification serveur. Suite à la demande de certificat envoyée par l'AE, l'AC retourne le certificat à l'AE. Ce retour notifie l'AE de la génération du certificat d'authentification serveur.

Dans le cas de l'enregistrement d'un certificat d'authentification serveur via un MC (voir § 3.2.3.3), l'AE informera ce dernier par email lors de l'envoi du certificat.

4.5. Usages de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat par le RCAS

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée aux usages décrits dans le chapitre § 1.4.1.1 de la PC.

La bi-clé du serveur a comme seuls usages au sens X509 du terme :

- Profil « Authentification » :

    - KeyUsage :
        - DigitalSignature
    - ExtendedKeyUsage :
        - ClientAuthentication
- Profil « Authentification et Signature » :
    - KeyUsage :
        - DigitalSignature
        - NonRepudiation
    - ExtendedKeyUsage :
        - EmailProtection
- Profil « Authentification et Confidentialité » :
    - KeyUsage :
        - KeyEncipherment
        - DigitalSignature
    - ExtendedKeyUsage :
        - ClientAuthentication
        - ServerAuthenticaiton

4.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat
Voir § 1.4 de la PC

4.6. Renouvellement d'un certificat
4.6.1. Causes possibles de renouvellement d'un certificat
Sans objet

4.6.2. Origine d'une demande de renouvellement
Sans objet

4.6.3. Procédure de traitement d'une demande de renouvellement
Sans objet

4.6.4. Notification au RCAS de l'établissement du nouveau certificat
Sans objet

4.6.5. Démarche d'acceptation du nouveau certificat
Sans objet

4.6.6. Publication du nouveau certificat
Sans objet

4.6.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat
Sans objet

4.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé
4.7.1. Causes possibles de changement d'une bi-clé
Voir § 4.7.1 de la PC

4.7.2. Origine d'une demande d'un nouveau certificat
L'origine d'une demande d'un nouveau certificat est identique à celle vu au chapitre § 4.1.1.

4.7.3. Procédure de traitement d'une demande d'un nouveau certificat
Le traitement d'une demande d'un nouveau certificat suit la même procédure que pour une demande initiale. Voir § 3.3.

4.7.4. Notification au RCAS de l'établissement du nouveau certificat
Voir § 4.3.2

4.7.5. Démarche d'acceptation du nouveau certificat
Voir § 4.4.1

4.7.6. Publication du nouveau certificat
Voir § 4.4.2

4.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat
Voir § 4.4.3

4.8. Modification du certificat
4.8.1. Causes possibles de modification d'un certificat
Sans objet

4.8.2. Origine d'une demande de modification d'un certificat
Sans objet

4.8.3. Procédure de traitement d'une demande de modification d'un certificat
Sans objet

4.8.4. Notification au RCAS de l'établissement du certificat modifié
Sans objet

4.8.5. Démarche d'acceptation du certificat modifié
Sans objet

4.8.6. Publication du certificat modifié
Sans objet

4.8.7. Notification par l'AC aux autres entités de la délivrance du certificat modifié
Sans objet

4.9. Révocation et suspension des certificats
Un Certificat CERTEUROPE ne peut être que dans l'un des trois états suivants : valide, expiré ou révoqué.
L'Autorité de Certification CERTEUROPE ne permet pas la suspension des certificats.
Les causes possibles de révocation sont celles indiquées dans la PC.

4.9.1. Causes possibles d'une révocation
4.9.1.1. Certificats d'authentification serveur
Voir § 4.9.1.1 de la PC

4.9.1.2. Certificats d'une composante de l'ICP
Voir § 4.9.1.2 de la PC

4.9.2. Origine d'une demande de révocation
4.9.2.1. Certificats serveur
Voir § 4.9.2.1 de la PC

4.9.2.2. Certificats d'une composante de l'ICP
Voir § 4.9.2.2 de la PC

4.9.3. Procédure de traitement d'une demande de révocation
4.9.3.1. Révocation d'un certificat d'authentification serveur
Les principales opérations à effectuer pour l'AE sont :

- vérifier le numéro du certificat à révoquer grâce aux outils offerts par la plate-forme de CertEurope et au nom du serveur ;
- l'AE se connecte au serveur d'enregistrement à l'aide de son support cryptographique ;
- l'AE demande la révocation du Certificat en demandant à l'AC d'introduire le numéro de série du certificat et la date de révocation du Certificat dans la Liste des Certificats Révoqués.
- Sur réception de la demande de révocation émise par l'AE, l'AC CERTEUROPE génère sans délai une nouvelle LCR et la publie à la place de l'ancienne.
- Des habilitations spécifiques sont mises en place afin de n'autoriser l'accès en modification aux LCR qu'au personnel autorisé.

L'AE envoie un courrier électronique de notification de la révocation au RCAS.
Les opérations effectuées par l'AE sont décrites dans le document « *[30] CERTEUROPE – Guide de l'AE* ».
Des procédures dérogatoires à cet enregistrement peuvent être établies pour des Communautés particulières. Dans ce cadre, ce sont les procédures d'enregistrement spécifiques dument validées par CertEurope qui prévaudront.

4.9.3.2. Révocation d'un certificat d'une composante de l'ICP
Révocation d'un certificat d'AE :
Si la révocation fait suite à une demande de la part de la composante, celle-ci doit la faxer à l'AC afin que l'AC puisse s'assurer de la validité de la demande. Si la demande n'est pas recevable, l'AC en informe la composante.

Si la révocation est décidée unilatéralement par l'AC aucun contrôle particulier n'est réalisé.

Après validation de la demande, l'AC conformément aux documents « *[30] CERTEUROPE – Guide de l'AE* » et « *[20] CERTEUROPE – Cycle de vie d'une AE* » :

- L'AE se connecte au serveur d'enregistrement à l'aide du support cryptographique particulier qu'elle détient aux fins de génération et de révocation de certificat de composantes.
- recherche le certificat à révoquer dans l'annuaire à l'aide du numéro de série ou du DN du certificat.
- signe la demande de révocation du certificat à l'aide du support cryptographique particulier qu'elle détient aux fins de génération et de révocation de certificat de composantes
- demande la révocation du certificat en demandant à l'AC d'introduire le numéro de série du certificat et la date de révocation du certificat dans la Liste des Certificats Révoqués.
- La composante est notifiée par lettre recommandée de la publication de la révocation. Ce courrier mentionnera la cause de la révocation.

Révocation d'un certificat de la chaîne de certification :
La procédure à suivre, en cas de révocation du certificat de signature de l'AC, est précisée dans le document « *[02] CERTEUROPE – Procédures d'exploitation de l'ICP Certeurope* ».

4.9.4. Délai accordé au RCAS pour formuler la demande de révocation
Voir § 4.9.4 de la PC

4.9.5. Délai de traitement par l'AC d'une demande de révocation
4.9.5.1. Révocation d'un certificat d'authentification serveur
Voir § 4.9.5.1 de la PC

4.9.5.2. Révocation d'un certificat d'une composante de l'IGC
Voir § 4.9.5.2 de la PC

4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats
Pour vérifier l'état d'un certificat d'authentification serveur, l'AC CERTEUROPE met à disposition des utilisateurs de certificats d'authentification serveur la LCR à trois adresses de publication distinctes (cf. § 2.2).
Ces adresses de publication de la LCR sont indiquées dans le champ CRLDistributionPoint des certificats d'authentification serveur.

Pour vérifier l'état d'un certificat de la chaîne de certification, CERTEUROPE met à disposition des utilisateurs de certificats d'authentification serveur la LCR de l'AC CertEurope eID Root à trois adresses de publication distinctes :

1) http://www.certeurope.fr/reference/certeurope_eid_root.crl
2) ldap://lcr1.certeurope.fr/cn=Certeurope%20eID%20Root,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList
3) ldap://lcr2.certeurope.fr/cn=Certeurope%20eID%20Root,ou=0002%20434202180,o=Certeurope,c=FR?certificateRevocationList

Ces adresses de publication de la LCR sont indiquées dans le champ CRLDistributionPoint des certificats des AC Certeurope eID Root et CERTEUROPE.

L'utilisateur de certificat d'authentification serveur utilise le moyen de son choix pour récupérer les LCR sur les adresses de publication et vérifie ainsi l'état de la chaîne de confiance.

4.9.7. Fréquence d'établissement des LCR
Voir § 4.9.7 de la PC

4.9.8. Délai maximum de publication d'une LCR
Le délai de publication d'une LCR n'excède jamais 30 minutes suivant sa génération.
Pour atteindre cet objectif, l'OC publie sans délai la LCR sur le premier point de distribution LDAP. Un robot duplique cette LCR sur les deux autres points de distribution à savoir, le second point en LDAP et celui en HTTP.
La réplication est effectuée toutes les 2 minutes.

4.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats
Aucun service OCSP n'est mis en œuvre.

4.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats
Voir § 4.9.6

4.9.11. Autres moyens disponibles d'information sur les révocations
Aucun autre moyen d'information sur les révocations n'a été mis en place.

4.9.12. Exigences spécifiques en cas de compromission de la clé privée

Aucune exigence spécifique en cas de compromission de la clé privée d'un serveur hormis la révocation du certificat (voir § 4.9.12 de la PC).

4.9.13. Causes possibles d'une suspension

Sans objet

4.9.14. Origine d'une demande de suspension

Sans objet

4.9.15. Procédure de traitement d'une demande de suspension

Sans objet

4.9.16. Limites de la période de suspension d'un certificat

Sans objet

4.10. Fonction d'information sur l'état des certificats

4.10.1. Caractéristiques opérationnelles

Voir chapitre § 4.9.6.

Les LCR sont au format dénommé "LCR V2" et accessibles via un annuaire LDAP V3.

4.10.2. Disponibilité de la fonction

Disponible 24 heures sur 24 et 7 jours sur 7. Voir chapitre § 2.2.
La durée maximale par interruption de service est de 4 heures.
La durée totale d'indisponibilité par mois est de 16 heures.

4.10.3. Dispositifs optionnels

Sans objet

4.11. Fin de la relation entre le RCAS et l'AC

Voir § 4.9.3 de la DPC et le § 4.11 de la PC.

4.12. Séquestre de clé et recouvrement

L'AC interdit le séquestre des clés privées des serveurs.

4.12.1. Politique et pratiques de recouvrement par séquestre de clés

Sans objet

4.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet

5. Mesures de sécurité non techniques

Les différents contrôles décrits ici visent, par une gestion des risques adéquate, à assurer un niveau de confiance fort dans le fonctionnement de l'AC CERTEUROPE.

5.1. Mesures de sécurité physique

Une analyse de risque a été menée par Certeurope. Les mesures prises pour assurer la sécurité physique du système informatique de l'AC CERTEUROPE sont décrites dans le document de référence « *[01] CERTEUROPE – Procédures de sécurité de l'ICP Certeurope* ».

5.1.1. Situation géographique

Le système informatique d'émission et de gestion du cycle de vie des Certificats CERTEUROPE est hébergé dans les locaux de EQUINIX situés au :

114, rue Ambroise Croisat, 93200 Saint Denis

Le système informatique secondaire d'émission et de gestion du cycle de vie des Certificats CERTEUROPE est hébergé dans les locaux de Colt Technology Services situés au :

15 Avenue Du Cap Horn, 91400 Les Ulis

5.1.2. Accès physique

Les exigences de sécurité issues de l'analyse de risque sont formalisées dans la « [3] Certeurope – Politique de sécurité ».

Accès physique OSC :

L'accès physique au site de l'Hébergeur, aux salles de production et de cérémonie de clés est contrôlé par des dispositifs de sécurité spécifiques décrits dans la « *[01] CERTEUROPE – Procédures de sécurité de l'ICP Certeurope* ». De plus, le site de production de l'Hébergeur est surveillé 24h/24 7j/7 par du personnel dûment autorisé et contrôlé. L'accès à ses locaux est verrouillé par un système de badge et système biométrique. En dehors des heures ouvrées, un filtrage est effectué par le poste de sécurité, unique moyen d'accès au bâtiment.

Accès physique AE :

Les AE ne disposent sur leur poste de travail que de la partie cliente de l'application d'enregistrement des demandes de certificats. Ces postes ont comme unique besoin de sécurité la disponibilité, aucune information sensible n'y réside. L'accès à ces postes ne fait donc pas l'objet d'un contrôle spécifique (ils sont bien entendu raisonnablement protégés car faisant partie d'un réseau d'entreprise ou d'un réseau d'une communauté.
En plus de ces mesures, les AE s'engagent auprès de l'AC CERTEUROPE à ce que leurs locaux soient fermés à clés. De plus, l'accès aux documents archivés doit être contrôlé au minimum par une clé ou un code confidentiel détenu par le seul porteur du certificat d'AE.

5.1.3. Alimentation électrique et climatisation

Le site de production de l'Hébergeur dispose d'un système d'alimentation secourue : onduleurs et groupes électrogènes. Toutes les salles de production de l'Hébergeur sont équipées d'un système de conditionnement d'air. Les exigences sont contractuellement précisées dans les contrats d'infogérance « [4] CertEurope – Contrat BCS » et « [5] CertEurope – Contrat COLT ».

5.1.4. Vulnérabilité aux dégâts des eaux

Le site de production de l'Hébergeur est protégé contre les risques d'inondation et de dégâts des eaux.
Des mesures équivalentes sont demandées aux AE pour l'archivage des documents relatifs à leurs fonctions.
Les exigences sont contractuellement précisées dans les contrats d'infogérance « [4] CertEurope – Contrat BCS » et « [5] CertEurope – Contrat Colt ».

5.1.5. Prévention et protection incendie

Des procédures spécifiques sont prévues pour la prévention du patrimoine notamment en matière de dégâts du feu sur le site de l'Hébergeur.
Les exigences sont contractuellement précisées dans les contrats d'infogérance « [4] CertEurope – Contrat BCS » et « [5] CertEurope – Contrat Colt ».
Les AE s'engagent à archiver les documents dans un environnement offrant des garanties équivalentes.

5.1.6. Conservation des supports

Les opérations effectuées par les AE sont automatiquement enregistrées dans le journal d'audit de la plate-forme CertEurope. Par conséquent, elles sont archivées par l'AC.
Les médias stockés par l'Hébergeur (bandes magnétiques) sont protégés contre tout excès de température, d'humidité et de rayonnement magnétique. Les mesures prises sont décrites dans le document « *[09] CERTEUROPE – Cycle de vie des supports de données* ».

5.1.7. Mise hors service des supports

Tous les supports servant au stockage des informations sensibles de l'AC sont effacés ou détruits avant leur mise au rebut. Voir les documents « *[02] CERTEUROPE – Procédures d'exploitation de l'ICP Certeurope* » et « *[09] CERTEUROPE – Cycle de vie des supports de données* ».

5.1.8. Sauvegarde hors site

Voir « *[02] CERTEUROPE – Procédures d'exploitation de l'ICP Certeurope* » rubrique « *[10] CERTEUROPE – Procédure de sauvegarde* ».

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance

Les rôles de confiance de l'OSC sont détaillés dans le document « *[07] CERTEUROPE – Rôles et habilitations* ».
Les rôles de confiance de l'AC sont :

- AE qui a pour rôles la génération et la révocation des certificats sous la responsabilité du RSSI de l'OSC et la consultation des archives des DDS. Au sein de la fonction d'Autorité d'Enregistrement, les rôles peuvent être subdivisés ;
    - AEA qui a pour rôle la vérification de l'identité et de la qualité du demandeur ;
    - AET qui a pour rôles la génération du certificat du serveur et la révocation des certificats de cachet ;

5.2.2. Nombre de personnes requises par tâches

Opération	Acteur de l'opération	Entité bénéficiaire de l'opération	Autorisations requises			
			Porteurs de secrets Certeurope	Porteurs de secrets OC	Nombre d'OP	Nombre d'ADM
Génération de bi-clé et certificat	AC RACINE	AC	0	0	0	2
	AC	AE	0	0	1	2
	AC	UF	0	0	1	0
Modification configuration des profils de l'AC	AC	AC,UF	0	0	0	2

Opération	Acteur de l'opération	Entité bénéficiaire de l'opération	Autorisations requises			
			Porteurs de secrets Certeurope	Porteurs de secrets OC	Nombre d'OP	Nombre d'ADM
Stockage et restauration de clé privée	AC	AC	2	1	0	0
Révocation de certificat	AC RACINE	AC	0	0	0	2
	AC	AE	0	0	1	2
	AC	UF	0	0	1	0
Contrôle des journaux d'événements	AC	*	0	0	0	1

5.2.3. Identification et authentification pour chaque rôle
Les procédures d'attributions des rôles sont détaillées dans le document « *[01] CERTEUROPE – Procédures de sécurité de l'ICP Certeurope* ».

5.2.4. Rôles exigeant une séparation des attributions
Les règles de non cumul sont détaillées dans le document « *[07] CERTEUROPE – Rôles et habilitations* ».

5.3. Mesures de sécurité vis-à-vis du personnel
5.3.1. Qualifications, compétences et habilitations requises
Le personnel est recruté suivant la procédure d'embauche « *[11] CERTEUROPE – Procédure d'embauche* ».

5.3.2. Procédures de vérification des antécédants
Cf « *[11] CERTEUROPE – Procédure d'embauche* ».

Préalablement à toute attribution d'un rôle de confiance, l'entité responsable de l'employé concerné vérifie le bulletin n°3 du casier judiciaire de celui-ci.

L'entité responsable d'un employé ayant un rôle de confiance, s'assure que, si ce dernier est sanctionné dans le cadre de son travail, la faute ayant entrainé la sanction n'est pas incompatible avec son rôle de confiance.
De la même façon, si un employé ayant un rôle de confiance, est absent pour purger une peine suite à une condamnation, l'entité responsable de cet employé prend les dispositions nécessaires pour s'assurer que la condamnation n'est pas incompatible avec le rôle de confiance attribué.
Ces vérifications sont faites, au moins tous les 3 ans.
En cas de doute ou d'incompatibilité, elle contacte l'AC pour envisager le remplacement du rôle de confiance.

5.3.3. Exigences en matière de formation initiale
OSC :
Tout nouvel employé de Certeurope suit une formation initiale adaptée au métier qu'il devra exercer au sein de l'ICP, ainsi qu'une formation générique sur la politique de sécurité interne et la gestion de la sécurité au quotidien. Ces formations entrent dans le plan annuel de formation de CertEurope, cf « *[12] CERTEUROPE – Plan de formation* ».

AE :
Les AE suivent une formation et sensibilisation aux tâches liées à la gestion des certificats émis par l'AC AC CERTEUROPE, cf. « *[30] CERTEUROPE – Guide de l'AE* ».
Toute nouvelle AE suit une formation correspondant à l'activité qui lui est demandée et notamment à l'utilisation des postes de travail et les différentes procédures de certification. Cette formation est dispensée par CertEurope. Ce n'est qu'à l'issue de cette formation que le certificat d'AE et le matériel nécessaire sont remis à la personne physique endossant le rôle d'AE.

5.3.4. Exigences et fréquence en matière de formation continue
AE :
Par ailleurs afin d'assurer un niveau de compétence optimal aux intervenants, des formations sont assurées dès que des modifications de procédure surviennent.
Les AE seront formés à chaque nouvelle version de logiciel d'enregistrement ou de la PC/DPC impliquant une modification sensible de la procédure d'enregistrement.

OSC :
Le personnel de l'OSC est formé en continue en fonction des évolutions des procédures. Ces formations sont ajoutées au plan de formation annuel.

5.3.5. Fréquence et séquence de rotation entre différentes attributions
Sans objet.

5.3.6. Sanctions en cas d'actions non-autorisées
Des avertissements ou des sanctions peuvent être pris envers les personnels ne respectant pas les procédures internes ou les consignes de sécurité mises en place.
Documents de référence : « *[13] CERTEUROPE – Charte Informatique* » et « *[14] CERTEUROPE – Règlement Intérieur* ».

5.3.7. Exigences vis-à-vis du personnel des prestataires externes
AC :
Les rôles d'AE sont endossés par le personnel propre à l'AE.

OC :
Le rôle d'OC est attribué au personnel de CertEurope.

5.3.8. Documentation fournie au personnel
AC :
Pour l'AE, les documents (instructions, procédures…) propres à la fonction exercée sont transmis lors de la formation et de la remise de leur certificat d'AE. Il s'agit en particulier du document « *[30] CERTEUROPE – Guide de l'AE* ».

OSC :
La documentation fournie au personnel de CertEurope est disponible sur le CertiEspace. Toute évolution du référentiel documentaire est notifiée à personnes habilitées de CertEurope.

5.4. Procédures de constitution des données d'audit
5.4.1. Types d'évènements à enregistrer
Voir chapitre § 5.4.1 de la PC

5.4.2. Fréquence de traitement des journaux d'évènements
Voir § 5.4.8.

5.4.3. Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins 1 mois et doivent être archivés au plus tard sous le délai d'1 mois.

5.4.4. Protection des journaux d'évènements

La modification ou la suppression des journaux d'événements fait l'objet de contrôles et de droits d'accès spécifiques revus périodiquement.
Afin d'assurer la meilleure sécurité aux journaux d'événement, seuls les journaux centraux (serveur de spool, AC, annuaire LDAP..) contiennent des informations sensibles. Les postes des AE ne contiennent aucune donnée sensible ou ayant à être journalisée
Pour prévenir toute tentative de modification, l'AC effectue un hachage de ses journaux les plus sensibles, chaque entrée faisant elle-même l'objet d'une signature.

5.4.5. Procédure de sauvegarde des journaux d'évènements

Le processus de journalisation est effectué en tâche de fond par les systèmes de CERTEUROPE.
Les postes des AE ne contiennent que les modules d'accès à la plate-forme de certification de CERTEUROPE. Aucune opération liée à la certification ne peut être exécutée seule sur le poste de l'AE. Elles nécessitent toutes une connexion sur la plate-forme de CERTEUROPE. Tous les accès des AE, ainsi que les opérations qu'elles effectuent sont journalisés de façon sécurisée par la plate-forme de CERTEUROPE. Tous les événements relatifs aux accès des AE aux services de l'AC sont journalisés de façon sécurisée par l'AC. Aucun événement informatique n'est donc journalisé au niveau des AE.

Les journaux d'événements sont sauvegardés quotidiennement sur le site d'hébergement selon la procédure décrite dans le manuel « *[01] CERTEUROPE – Procédures de sécurité de l'ICP Certeurope* ». Une copie de ces journaux est également envoyée à la société Certeurope, cet envoi est réalisé via le réseau Internet et utilise des méthodes de chiffrement robustes pour protéger la confidentialité des données.

5.4.6. Système de collecte des journaux d'évènements

Cf procédure de « *[10] CERTEUROPE – Procédure de sauvegarde* ».

5.4.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

5.4.8. Evaluation des vulnérabilités

Toutes les anomalies, les tentatives d'intrusion dans le système ou de corruption des données sont enregistrées dans les journaux d'exploitation, et contrôlées à intervalles réguliers (quotidien par exemple pour le pare-feu et les fichiers systèmes sensibles).
Toute anomalie fait l'objet d'une analyse détaillée par le Responsable de la Sécurité des Systèmes d'Information (RSSI). Celui-ci émet des recommandations et effectue un suivi des corrections apportées et des mesures mises en place pour répondre au type d'incident rencontré.

5.5. Archivage des données

5.5.1. Types de données à archiver

Voir § V.5.1 de la PC

5.5.2. Période de rétention des archives

- Le détail de toutes les données à archiver et leur période de rétention est fourni dans le document « *[08] CERTEUROPE – Inventaire ICP* ».

- La plupart des données électroniques sont conservés pendant 10 ans (cf. « *[08] CERTEUROPE – Inventaire ICP* »)

Toute version antérieure à la version courante de la PC, et de la DPC est conservée selon la procédure d'archivage pour une durée de 10 ans ;

5.5.3. Protection des archives

Voir le document « *[17] CERTEUROPE – Archivage des données de l'IGC* ».

5.5.4. Procédure de sauvegarde des archives

Sans objet.

5.5.5. Exigences d'horodatage des données

Les serveurs mis en œuvre ont leur horloge système synchronisée sur deux serveurs de temps hautement sécurisés, ces serveurs sont ceux de l'Autorité d'horodatage Certid@te, ils reçoivent via une liaison Hertzienne de type DCF 77 l'heure atomique.
Ces serveurs de temps sont situés dans les mêmes locaux que les serveurs de l'ICP et étant redondant l'un de l'autre, ils assurent une continuité du service de temps notamment à destination des serveurs de l'ICP. Ainsi les heures inscrites dans les LCR, les Certificats et les Journaux d'événement sont fiables à 1s près (dérive maximum des serveurs de temps).
Il n'y a pas d'horodatage au sens association d'une date et de l'image d'un fichier signé par une Autorité d'Horodatage.

5.5.6. Système de collecte des archives

Sans objet.

5.5.7. Procédures de récupération et de vérification des archives

Les archives sont récupérées conformément au document « *[02] CERTEUROPE – Procédures d'exploitation de l'ICP Certeurope* ».

5.6. Changement de clé de l'AC

L'AC CERTEUROPE ne peut générer des certificats dont la date de fin serait postérieure à la date d'expiration de l'AC.
Les certificats délivrés par l'AC CERTEUROPE ont une validité de trois ans. L'AC CERTEUROPE ne peut donc plus générer de certificat dans un délai inférieur à trois ans avant la date d'expiration du certificat de l'AC. Elle devra néanmoins assurer la disponibilité de la CRL durant cette période.
Afin de poursuivre la délivrance de certificats, CertEurope devra changer les clés de l'AC CERTEUROPE.

Le changement de clés de l'AC est traité par l'opérateur comme l'initialisation d'une nouvelle AC (Cf « *[02] CERTEUROPE – Procédures d'exploitation de l'ICP Certeurope* » rubrique Changement de clés d'une AC).
Cette nouvelle AC doit également être soumise à un audit RGS Cf. § 8 de la PC. Suite à cet audit, l'AC suivra une procédure de référencement sur les différentes plateformes.
CertEurope doit communiquer sur son site, à l'adresse www.certeurope.fr; la date à partir de laquelle les certificats seront générés par la nouvelle AC.
La nouvelle PC liée à la nouvelle AC sera également publiée sur le site www.certeurope.fr.

5.7. Reprise suite à compromission et sinistre

5.7.1. Procédures de remontée et de traitement des incidents et des compromissions

En cas d'incident majeur lié à la clé privée de l'AC CERTEUROPE (compromission de la clé, vol de la clé privée), la composante de l'IGC ayant constaté l'incident remonte l'information à CertEurope sans délai par téléphone ou email.

Dans le cas où l'OSC constate un incident majeur lié à la clé privée de l'AC, le document « [16] Certeurope – Gestion des incidents » détaille la procédure de remontée et de traitement des incidents.
L'AC CERTEUROPE décide de la nécessité d'une action correctrice à l'incident. En cas de nécessité de révocation de son certificat, l'AC CERTEUROPE doit :

- effectuer une demande de cérémonie de révocation à l'OSC ;
- communiquer sur son site www.certeurope.fr de la révocation imminente de son certificat ;
- contacter la DGME sans délai (le contact est identifié sur le site www.ssi.gouv.fr) ;

Une nouvelle bi-clé pour l'AC CERTEUROPE peut être générée suite à une demande de cérémonie d'initialisation à l'OSC.

5.7.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

La procédure est détaillée dans le document « *[06] CERTEUROPE – Plan de Continuité* ».

5.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante

La procédure est détaillée dans le document « *[06] CERTEUROPE – Plan de Continuité* ».
Dans le cas d'une compromission de la clé privée d'une AE, le certificat est révoqué conformément au document « *[20] CERTEUROPE – Cycle de vie d'une AE* ».

5.7.4. Capacités de continuité d'activité suite à un sinistre

La procédure est détaillée dans le document « *[06] CERTEUROPE – Plan de Continuité* ».

5.8. Fin de vie de l'IGC

5.8.1. Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Le transfert d'activité est effectué conformément au document « *[06] CERTEUROPE – Plan de Continuité* ».

5.8.2. Cessation d'activité affectant l'AC

La cessation d'activité est détaillée plus précisément dans le document « [6] CertEurope – Plan de Continuité ».
Après terminaison d'une de ses AC, CertEurope, en accord avec les exigences de la norme ETSI EN 319 411-1/2, publiera une dernière CRL en assignant la valeur "99991231235959Z" au champ "nextUpdate", sauf exigences complémentaires de l'organe de supervision national (ANSSI).
Les informations sur le statut de révocation (CRL et OCSP) seront disponibles au moins 5 ans après la terminaison de l'AC.
La fin de vie fait l'objet d'une information clairement diffusée au moins sur le site de CertEurope et éventuellement relayée par d'autres moyens (associations, clubs utilisateur, réseaux sociaux, etc.).
En plus des éventuelles recommandations de l'ANSSI, CertEurope doit :
Informer tous les Porteurs, Mandataires de Certification et les autres entités en lien avec l'AC (plateforme de marché, fournisseurs d'identités, etc.)

6. Mesures de sécurité techniques

6.1. Génération et installation de bi-clés

Il est rappelé que les certificats d'authentification serveur gérés par l'AC CERTEUROPE n'ont comme seul usage que le chiffrement de la clé. L'AC CERTEUROPE décline toute responsabilité de l'utilisation de la bi-clé pour une utilisation autre que celle définie dans la PC au chapitre 6.1.1.

6.1.1. Génération des bi-clés

6.1.1.1. Clés d'AC

La bi-clé de l'AC (pour la de signature de certificats et de CRLs) est générée et protégée par un module cryptographique matériel (Bull Trustway).
Ce module est certifié selon les Critères Communs avec assurance EAL4+ au moins ou selon les critères FIPS 140-1 niveau 4.
La génération ou le renouvellement de la bi-clé de l'AC par ce module nécessite la présence d'au moins 3 personnes.
La génération de ce biclé intervient lors de l'initialisation de l'AC (key ceremony), dont le procès verbal détaille l'intégralité des actions effectuées. « [19] CERTEUROPE ADVANCED – KeyCeremony ».
Il convient de se référer à la procédure de l'AC « *[02] CERTEUROPE – Procédures d'exploitation de l'ICP Certeurope* ».

6.1.1.2. Clés serveurs générées par l'AC

Pour le niveau (*) :
La clé privée est générée au niveau du serveur ou dans un module cryptographique sous contrôle du RCAS et n'est pas transmise.

Pour le niveau (**) :
La bi-clé du serveur n'est pas générée par l'AC.

6.1.1.3. Clés serveur générées au niveau du serveur

Sans objet.

6.1.2. Transmission de la clé privée au serveur

Pour le niveau (*) :
La clé privée est générée au niveau du serveur. Si elle est générée par l'AC, elle est hébergée par l'AC dans un module cryptographique sous contrôle exclusif du RCAS. Elle n'est donc pas transmise.

Pour le niveau (**) :
La clé privée n'est pas générée par l'AC.
Un face-à-face physique avec le RCAS est prévu à l'enregistrement pour vérifier son identité.

6.1.3. Transmission de la clé publique à l'AC

Sans objet.

6.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

Le certificat d'AC est disponible sur le site web de l'AC CERTEUROPE, à l'adresse http://www.certeurope.fr/chaine-confiance-numerique.php

6.1.5. Tailles des clés

Les clés RSA des serveurs utilisées ont une taille de 2048 bits et sont associées à la fonction d'empreinte SHA-256. Elles seront mises à niveau au fur et à mesure de l'évolution de la technique et/ou de la législation.
La taille de la clé RSA de l'AC CERTEUROPE est de 2048 bits.
Les clés d'AE ont une longueur de 2048 bits.

6.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

La bi-clé de signature de l'AC est générée sur la carte cryptographique répondant aux exigences des normes européennes précisées par la législation française EAL4+, et mettant en œuvre un mécanisme de secret partagé.
Les bi-clés des AE sont générées directement par le SSCD qui leur est remis à l'issue de la formation.
Les bi-clés des serveurs sont générées conformément aux exigences du RGS.

6.1.7. Objectifs d'usage de la clé

L'utilisation de la clé privée de l'AC est strictement limitée à la signature de certificats et de LCR.
Les usages de la clé privée des serveurs (signature et non-répudiation) sont liés aux modalités d'utilisation des certificats admis par l'AC CERTEUROPE telles que décrites dans la PC.

6.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1. Modules cryptographiques de l'AC

Voir § 6.2.1.1 et §11.

6.2.1.2. Dispositifs de protection de clés privées des serveurs

Voir § 6.2.1.2 et § 12 de la PC.
Cf. « *[24] CERTEUROPE – Contrat d'abonnement* ».

6.2.2. Contrôle de la clé privée de signature de l'AC par plusieurs personnes

Un système de secrets partagés (où 3 personnes doivent s'authentifier chacun à l'aide d'un secret distinct) est mis en place pour toute opération (or la génération de certificat ou de CRL) ayant trait à la clé privée de signature de l'AC. (cf. procédure de l'AC *« [02] CERTEUROPE – Procédures d'exploitation de l'ICP Certeurope* »).
Ce partage des clés est mis en œuvre lors de l'initialisation de l'AC « *[19] CERTEUROPE eID – KeyCeremony* ».

6.2.3. Séquestre de la clé privée

Aucun séquestre.

6.2.4. Copie de secours de la clé privée

Les clés privées des serveurs ne font l'objet d'aucune copie par l'AC.
Une copie de secours de la clé privée de l'AC est réalisée lors de la cérémonie des clés Cf « *[19] CERTEUROPE eID – KeyCeremony* ».

6.2.5. Archivage de la clé privée

Aucun archivage de clé privée.

6.2.6. Transfert de la clé privée vers / depuis le module cryptographique

Conformément au chapitre § 6.1, les clés privées des serveurs sont générés via un dispositif répondant aux exigences du RGS.
Voir § 6.2.4 pour le transfert de clés privées d'AC.

6.2.7. Stockage de la clé privée dans un module cryptographique

Voir chapitres § 6.1.1, § 6.2.4 et §11.

6.2.8. Méthode d'activation de la clé privée

6.2.8.1. Clés privées d'AC

L'activation de la clé privée de l'AC s'effectue conformément au chapitre § 6.2.2.

6.2.8.2. Clés privées des serveurs
Sans objet.

6.2.9. Méthode de désactivation de la clé privée
6.2.9.1. Clés privées d'AC
Le module cryptographique utilisé pour la clé privée de l'AC est une « Bull Trustway » certifiée selon les Critères Communs avec assurance EAL4+. Ce module répond aux exigences du § 11.

6.2.9.2. Clés privées des serveurs
La désactivation de la clé privée d'un serveur est sous le contrôle exclusif du RCAS. Ce dernier s'engage à mettre en œuvre des conditions de désactivation de la clé privée du serveur dont il est rattaché conformément aux exigences du RGS Cf. *[24] CERTEUROPE – Contrat d'abonnement* ».

6.2.10. Méthode de destruction des clés privées
6.2.10.1. Clés privées d'AC
La procédure est détaillée dans le document « *[02] CERTEUROPE – Procédures d'exploitation de l'ICP Certeurope* » (rubrique « Destruction des clés privées d'une AC »).

6.2.10.2. Clés privées des serveurs
La destruction de la clé privée d'un serveur est sous le contrôle exclusif du RCAS. Ce dernier s'engage à mettre en œuvre des conditions de destruction de la clé privée du serveur dont il est rattaché conformément aux exigences du RGS Cf. *[24] CERTEUROPE – Contrat d'abonnement* ».

6.2.11. Niveau de qualification du module cryptographique et des dispositifs de protection de clés privées
Les modules cryptographiques utilisés par l'AC sont évalués selon les critères communs au niveau EAL 4+ et qualifiés au niveau standard par l'ANSSI. Par ailleurs, ils sont, dans les conditions prévues par le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes de technologies de l'information, certifiés conformes par le Premier Ministre aux exigences détaillées à l'annexe de l'arrêté du 26 juillet 2004.

6.3. Autres aspects de la gestion des bi-clés
6.3.1. Archivage des clés publiques
Voir § 6.3.1 de la PC.

6.3.2. Durée de vie des bi-clés et des certificats
Voir § 6.3.2 de la PC.

6.4. Données d'activation
6.4.1. Génération et installation des données d'activation
6.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC
La génération et l'installation des données d'activation des modules cryptographiques de l'IGC interviennent lors de la cérémonie de l'AC dont le procès-verbal détaille l'intégralité des actions effectuées. « *[19] CERTEUROPE eID – KeyCeremony* ».

6.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du serveur
Sans objet. Les clés privées sont générées par les serveurs eux-mêmes. Les données d'activation ne sont donc pas gérées du côté de l'AC.

6.4.2. Protection des données d'activation

6.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC

Suite à la cérémonie de l'AC, les données d'activation de l'AC sont remises entre plusieurs porteurs qui ont la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité. Cette remise des données d'activation est détaillée dans le procès-verbal « [19] CERTEUROPE ADVANCED – KeyCeremony ».
Le document « [9] Certeurope – Cycle de vie des supports de données » décrit la procédure de conservation de ces données d'activation.

6.4.2.2. Protection des données d'activation correspondant à la clé privée des serveurs

Sans objet. Les clés privées sont générées par les serveurs eux-mêmes. Les données d'activation ne sont donc pas gérées du côté de l'AC.

6.4.3. Autres aspects liés aux données d'activation

Sans objet.

6.5. Mesures de sécurité des systèmes informatiques

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Les règles de sécurité sont définies dans le document « *[02] CERTEUROPE – Procédures d'exploitation de l'ICP Certeurope* »

6.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Les règles suivantes sont appliquées sur les systèmes de l'AC CERTEUROPE afin d'assurer un niveau de sécurité optimum :

- tous les ingénieurs système sont des personnels de Certeurope ;
- Aucun compte utilisateur autre que celui des ingénieurs système ou administrateurs de base de données n'est créé ;
- le compte d'un ingénieur est suspendu en cas de départ ou d'absence prolongée ;
- tous les comptes sont individuels et traçables ;
- les systèmes d'audit permettant l'imputabilité des actions de chacun sont mis en place ;
- les fichiers systèmes sensibles sont surveillés quotidiennement afin d'en vérifier l'intégrité ;
- le serveur Pare-feu est surveillé quotidiennement, les éventuelles attaques sont analysées et enregistrées afin de déterminer la stratégie utilisée par les attaquants ;
- l'ensemble du système d'information est protégé par des anti-virus ;
- tous les serveurs sont sauvegardés selon un plan de sauvegarde associé à un plan de reprise en cas de désastre ;
- un dispositif de contrôle d'intégrité assure que les fichiers présents sur chaque machine ne sont pas altérés.

6.6. Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1. Mesures de sécurité liées au développement des systèmes

Les applications de l'AC ont été développées et implémentées dans le strict respect de l'analyse de risque préalable et de la politique de sécurité qui en découle.
L'implémentation, les configurations des systèmes et les modifications sont par ailleurs notifiées dans un journal d'activité du centre de production.
En outre, le système de génération des clés et ses différentes composantes sont décrits dans le document « *[02] CERTEUROPE – Procédures d'exploitation de l'ICP Certeurope* ».
Le contrôle des modules cryptographiques est décrit dans le document « *[09] CERTEUROPE – Cycle de vie des supports de données* ».

6.6.2. Mesures liées à la gestion de la sécurité.

Les accès aux ressources offertes sur le serveur recevant les demandes de génération/révocation de certificats sont établies par profil en fonction des besoins des différents rôles. L'accès aux fonctions d'enregistrement nécessite dans ce cas une authentification préalable de l'AE grâce à son certificat d'AE.
D'une manière générale, seuls les ingénieurs système sont habilités à intervenir sur les matériels du centre de production de l'Hébergeur (ajouts d'options, sauvegardes, etc…). Toutes les actions (installations, changements de mot de passe, désinstallations, sauvegardes) et toutes les tâches d'administration sont enregistrées sur le journal d'activité du centre de production et font l'objet d'un rapport.

6.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

6.7. Mesures de sécurité réseau

Cf. document « *[18] CERTEUROPE – Description de l'infrastructure CertEurope* ».

6.8. Horodatage / Système de datation

Voir § 6.8 de la PC.

7. Profils de certificats et de LCR

Voir § 7. de la PC.

8. Audit de conformité et autres évaluations

8.1. Fréquences et / ou circonstances des évaluations

Voir § 8.1 de la PC

8.2. Identités / qualifications des évaluateurs

Voir § 8.2 de la PC

8.3. Relations entre évaluateurs et entités évaluées

Voir § VIII.3 de la PC

8.4. Sujets couverts par les évaluations

Voir § 8.4 de la PC

8.5. Actions prises suite aux conclusions des évaluations

Voir § 8.5 de la PC

8.6. Communication des résultats

Voir § 8.6 de la PC

9. Autres problématiques métiers et légales

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

Cf. « *[24] CERTEUROPE – Contrat d'abonnement* ».

9.1.2. Tarifs pour accéder aux certificats

Voir § 9.1.2 de la PC

9.1.3. Tarifs pour accéder aux informations d'état et de révocation des certificats

Voir § 9.1.3 de la PC

9.1.4. Tarifs pour d'autres services

Sans objet.

9.1.5. Politique de remboursement

Sans objet.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

Voir § 9.2.1 de la PC

9.2.2. Autres ressources

Sans objet.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Voir § 9.3.1 de la PC

9.3.2. Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3. Responsabilités en terme de protection des informations confidentielles

Voir § 9.3.3 de la PC

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

Voir § 9.4.1 de la PC

9.4.2. Informations à caractère personnel

Les informations considérées comme personnels sont :

- les causes de révocation d'un certificat serveur,
- le dossier d'enregistrement du RCAS.

9.4.3. Informations à caractère non personnel

Les informations à caractères non personnel sont les données ne contenant pas d'information sur l'identité d'un RCAS comme :

- les journaux d'événements contenant un numéro de série de certificat,

- les CRL (les causes de révocation ne sont pas publiées dans la CRL).

9.4.4. Responsabilité en termes de protection des données personnelles

Les composantes de l'IGC s'engagent à protéger toute donnée à caractère personnel qu'elles sont amenées à manipuler pour raison de gestion par :

- utilisation d'une armoire avec dispositif de verrouillage pour protéger les documents papier (dossier d'enregistrement, correspondance avec le RCAS ou le souscripteur, …) ;
- utilisation de dispositif de sécurité physique et logique pour les fichiers contenant les données à caractère personnel.

9.4.5. Notification et consentement d'utilisation des données personnelles

Conformément à la loi no 78-17 du 6 janvier 1978 dite loi « Informatique et Libertés », le souscripteur dispose d'un droit individuel d'accès et de rectification aux informations le concernant, il peut demander leur modification en envoyant un simple courrier à CERTEUROPE à l'adresse suivante : Correspondant Informatique et Libertés, 26 rue du Faubourg Poissonnière, 75010 Paris.

9.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

L'activité de l'AC s'exerce dans le cadre de la législation française, aussi sur requête d'une autorité habilitée, l'AC peut être amenée à fournir certaines informations confidentielles selon la loi L90-1170.

9.4.7. Autres circonstances de divulgation d'informations personnelles

Sur demande du RCAS, l'AC peut lui remettre les informations personnelles qu'elle possède conformément à la loi 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

9.5. Droits sur la propriété intellectuelle et industrielle

Voir § 9.5 de la PC

9.6. Interprétations contractuelles et garanties

9.6.1. Autorités de Certification

L'AC CERTEUROPE s'engage à :

- assurer le lien entre l'identité d'un RCAS et du certificat d'authentification serveur dont il a la responsabilité ;
- tenir à disposition des RCAS et des Utilisateurs, la Liste de Certificats Révoqués (LCR) ;
- s'assurer (en particulier par contrat) que les RCAS connaissent leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'ICP. La relation entre un RCAS et l'AC CERTEUROPE est formalisée par les documents intitulés « *[24] CERTEUROPE – Contrat d'abonnement* » précisant les droits et obligations des parties et notamment les garanties apportées par l'AC ;
- pouvoir démontrer aux applications utilisatrices de ces certificats, qu'elle a émis un certificat pour un serveur donné et que ce serveur a accepté le certificat par l'intermédiaire de son RCAS. Ceci en particulier grâce au contrat « *[24] CERTEUROPE – Contrat d'abonnement* ».

L'AC CERTEUROPE, par le biais de son Comité PKI détermine la conformité de la DPC à la PC soit directement, soit par l'intermédiaire d'experts indépendants spécialisés dans le domaine des Infrastructures à Clé Publique.

Les obligations de l'AC sont définies dans la PC.

L'AC CERTEUROPE et les RCAS sont contractuellement liés :

- « *[24] CERTEUROPE – Contrat d'abonnement* »

9.6.2. Service d'enregistrement

Lorsque l'AE CERTEUROPE est saisie d'une demande de génération de certificat, les différentes entités de l'AE devront effectuer les tâches prévues dans les documents :

- « *[30] CERTEUROPE – Guide de l'AE* ».
- « *[07] CERTEUROPE – Rôles et habilitations* ».

Lorsque l'AE CERTEUROPE est saisie d'une demande de révocation de certificat, les différentes entités de l'AE devront effectuer les tâches prévues dans les documents :

- « *[30] CERTEUROPE – Guide de l'AE* ».
- « *[07] CERTEUROPE – Rôles et habilitations* ».

9.6.3. RCAS

Voir § 9.6.3 de la PC.
Cf. « *[24] CERTEUROPE – Contrat d'abonnement* ».

9.6.4. Utilisateurs de certificats

Voir § 9.6.4 de la PC.

9.6.5. Autres participants

Sans objet.

9.7. Limite de garantie

Sans objet.

9.8. Limite de responsabilité

Sans objet.

9.9. Indemnités

Sans objet.

9.10. Durée et fin anticipée de validité de la PC

9.10.1. Durée de validité

Voir § 9.10.1 de la PC.

9.10.2. Fin anticipée de validité

Voir § 9.10.2 de la PC.

9.10.3. Effets de la fin de validité et clauses restant applicables

Sans objet

9.11. Notifications individuelles et communications entre les participants

En cas de changement de la composante AE, les actions à mener sont :

- faire un avenant au document « *[07] CERTEUROPE – Rôles et habilitations* » ;

9.12. Amendements à la PC

9.12.1. Procédures d'amendements

Voir § 9.12.1 de la PC.

9.12.2. Mécanisme et période d'information sur les amendements

Sans objet.

9.12.3. Circonstances selon lesquelles l'OID doit être changé
Voir § 9.12.3 de la PC.

9.13. Dispositions concernant la résolution de conflits
Cf. « *[23] CERTEUROPE – Conditions Générales* ».

9.14. Juridictions compétentes
Voir § 9.14 de la PC.

9.15. Conformité aux législations et réglementations
Voir § 9.15 de la PC.

9.16. Dispositions diverses
9.16.1. Accord global
Sans objet.

9.16.2. Transfert d'activités
Voir § 5.8.

9.16.3. Conséquences d'une clause non valide
Sans objet.

9.16.4. Application et renonciation
Sans objet.

9.16.5. Force majeure
Voir § 9.16.5 de la PC.

9.17. Autres dispositions
Sans objet.

10. Annexe 1 – Documents cités en reference

10.1. Réglementation

Voir § 10.1 de la PC.

10.2. Documents techniques

Documents OSC :

[01] CERTEUROPE – Procédures de sécurité de l'ICP Certeurope
[02] CERTEUROPE – Procédures d'exploitation de l'ICP Certeurope
[03] CERTEUROPE – Politique de sécurité
[04] CERTEUROPE – Contrat BCS
[05] CERTEUROPE – Contrat TéléHouse
[06] CERTEUROPE – Plan de Continuité
[07] CERTEUROPE – Rôles et habilitations
[08] CERTEUROPE – Inventaire ICP
[09] CERTEUROPE – Cycle de vie des supports de données
[10] CERTEUROPE – Procédure de sauvegarde
[11] CERTEUROPE – Procédure d'embauche
[12] CERTEUROPE – Plan de formation
[13] CERTEUROPE – Charte Informatique
[14] CERTEUROPE – Règlement Intérieur
[15] CERTEUROPE – Contrat LSTI
[16] CERTEUROPE – Gestion des incidents
[17] CERTEUROPE – Archivage des données de l'IGC
[18] CERTEUROPE – Description de l'infrastructure CertEurope

Documents AC :

[19] CERTEUROPE *eID* – KeyCeremony
[20] CERTEUROPE – Cycle de vie d'une AE
[21] CERTEUROPE – Prestations et Qualité de Service
[22] CERTEUROPE – Continuité de service
[23] CERTEUROPE – Conditions Générales
[24] CERTEUROPE – Contrat d'abonnement
[25] CERTEUROPE – Contrat d'abonnement – Changement de RCAS
[26] CERTEUROPE – Procuration du représentant légal – Désignation d'un MC
[27] CERTEUROPE – Accusé de réception du certificat
[28] CERTEUROPE – Demande de révocation
[29] CERTEUROPE – Contrôle et archivage des dossiers
[30] CERTEUROPE – Guide de l'AE
[31] CERTEUROPE – Analyse de risque
[32] CERTEUROPE – PV de conformité de la DPC à la PC
[33] CERTEUROPE – PV de face-à-face pour le niveau (**)

11. Annexe 2 – Exigences de sécurité du module cryptographique de l'AC

11.1. Exigences sur les objectifs de sécurité

Le module cryptographique utilisé est le modèle « Bull Trustway » évalué EAL4+ et qualifié au niveau standard par la ANSSI conformément aux exigences du RGS.

11.2. Exigences sur la certification

Le module cryptographique utilisé est le modèle « Bull Trustway » évalué EAL4+ et qualifié au niveau standard par la ANSSI conformément aux exigences du RGS.

12. Annexe 3 – Exigences de sécurité du dispositif de protection de clés privées

12.1. Exigences sur les objectifs de sécurité

Le RCAS s'engage à mettre en œuvre et à utiliser un dispositif de protection des clés privées conforme aux exigences du RGS (Cf « *[24] CERTEUROPE – Contrat d'abonnement* » et « *[23] CERTEUROPE – Conditions Générales* »).

12.2. Exigences sur la certification

Le RCAS s'engage à mettre en œuvre et à utiliser un dispositif de protection des clés privées conforme aux exigences du RGS (Cf « *[24] CERTEUROPE – Contrat d'abonnement* » et « *[23] CERTEUROPE – Conditions Générales* »).

13. Annexe 4 – Textes législatifs et réglementaires

- Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Directive européenne 95/46/EC relative à la protection des données personnelles
- Directive européenne (1999/93/EC) relative à la signature électronique été adoptée le 13/12//1999
- Loi no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
- Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique
- Décret no 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation.
- Décret no 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptographie dispensées de toute formalité préalable.
- Arrêté du 17 mars 1999 définissant la tome et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptographie.
- Arrêté définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fournitures d'un moyen ou d'une prestation de cryptographie, no PRMX9802730A du 13 mars 1998
- Arrêté définissant le modèle de notification préalable par le fournisseur des identités des intermédiaires utilisés pour la fourniture des moyens ou prestations de cryptographie soumis à autorisation, no PRMX9802732A du 13 mars 1998.
- Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données (J.OC.E., n° L. 281 du 23 novembre 1995, p. 31) ;
- Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 relative à la protection des bases de données (J.O.C.E., n° L. 77 du 27 mars 1996, p. 20) ;
- Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (J.O.C.E., n° L 013 du 19 janvier 2000, p. 12 et s.) ;
- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique ») (J.O.C.E., n° L 178 du 17 juillet 2000, p. 1 et s.) ;
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, (dite « directive vie privée et communications électroniques ») (J.O.C.E., n° L. 201 du 31 juillet 2002, p. 37) ;
- Décision 2003/511/CE du Parlement européen et du Conseil du 14 juillet 2003 relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques conformément à la directive 1999/511/CE du Parlement et du Conseil (J.O.C.E., n° L. 175 du 15 juillet 2003, p. 45) ;
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
- Décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et prestations de cryptologie ;
- Décret n° 2005-973 du 10 août 2005, portant modification du décret n°56-222 du 29 février 1956 concernant le statut des huissiers
- Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;
- Arrêté du 25 mai 2007 définissant la forme et le contenu de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie ;
- Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

14. Annexe 5 – Hiérarchie des AC

Nom de l'AC	Niveau RGS	Niveau EIDAS	Norme ETSI	Numéro de série (root) OID (end users)	Service	AC en fin de vie
Certeurope Advanced CA V4	*	Non qualifié	EN 319 411-1 LCP	1.2.250.1.105.12.1.1.0	Cachet	Oui
Certeurope Advanced CA V4	*	Non qualifié	EN 319 411-1 OVCP	1.2.250.1.105.18.1.1.0	Authentification serveur	Oui
Certeurope Advanced CA V4	**	Non qualifié	EN 319 411-1 NCP	1.2.250.1.105.12.3.1.0	Cachet	Oui
Certeurope Advanced CA V4	*	Non qualifié	EN 319 411-1 OVCP	1.2.250.1.105.18.4.1.0	Authentification serveur client	Oui
Certeurope Advanced CA V4	**	Non qualifié	EN 319 411-1 OVCP	1.2.250.1.105.18.3.1.0	Authentification serveur	Oui
Certeurope Advanced CA V4	**	Non qualifié	EN 319 411-1 NCP+	1.2.250.1.105.10.3.1.3	*Authentification*	Oui
Certeurope Advanced CA V4	*	Non qualifié	EN 319 411-1 LCP	1.2.250.1.105.21.3.1.0	*Authentification*	Oui
Certeurope Advanced CA V4	*	Non qualifié	EN 319 411-1 LCP	1.2.250.1.105.21.4.1.0	Signature	Oui
Certeurope Advanced CA V4	*	Non qualifié	EN 319 411-1 LCP	1.2.250.1.105.21.1.1.0	*Authentification* et signature	Oui
Certeurope Advanced CA V4	**	Non qualifié	EN 319 411-1 NCP+	1.2.250.1.105.10.1.1.3	*Authentification* et signature	Oui
Certeurope Advanced CA V4	**	Qualifié	Art. 51 2 (ETSI EN 319 411-2) QCP Public+SSCD	1.2.250.1.105.10.4.1.3	Signature (RGS_A_8)	Oui
CertEurope eID Root				1.2.250.1.105.22.1.1.0	Racine	Non
CertEurope eID User					Intermédiaire	Non
CertEurope eID User	*	Qualifié	EN 319 411-2 QCP-N	1.2.250.1.105.23.411.2.1.1.1.0	Signature	Non
CertEurope eID User	*	Qualifié	EN 319 411-2 QCP-N	1.2.250.1.105.23.411.2.1.2.1.0	*Authentification* et Signature	Non
CertEurope eID User	**	Qualifié	EN 319 411-2 QCP-N-QSCD	1.2.250.1.105.23.411.2.2.1.1.0	Signature	Non
CertEurope eID User	**	Qualifié	EN 319 411-2 QCP-N-QSCD	1.2.250.1.105.23.411.2.2.2.1.0	*Authentification* et Signature	Non
CertEurope eID User		Non qualifié	EN 319 411-1 LCP	1.2.250.1.105.23.411.1.1.1.1.0	Signature	Non

Nom de l'AC	Niveau RGS	Niveau EIDAS	Norme ETSI	Numéro de série (root) OID (end users)	Service	AC en fin de vie
CertEurope eID User		Non qualifié	EN 319 411-1 LCP	1.2.250.1.105.23.411.1.1.2.1.0	*Authentification*	Non
CertEurope eID User		Non qualifié	EN 319 411-1 LCP	1.2.250.1.105.23.411.1.1.3.1.0	*Authentification* et Signature	Non
CertEurope eID User		Non qualifié	EN 319 411-1 NCP	1.2.250.1.105.23.411.1.2.1.1.0	Signature	Non
CertEurope eID User		Non qualifié	EN 319 411-1 NCP	1.2.250.1.105.23.411.1.2.2.1.0	*Authentification*	Non
CertEurope eID User		Non qualifié	EN 319 411-1 NCP	1.2.250.1.105.23.411.1.2.3.1.0	*Authentification* et Signature	Non
CertEurope eID User		Non qualifié	EN 319 411-1 NCP+	1.2.250.1.105.23.411.1.3.1.1.0	Signature	Non
CertEurope eID User		Non qualifié	EN 319 411-1 NCP+	1.2.250.1.105.23.411.1.3.2.1.0	*Authentification*	Non
CertEurope eID User		Non qualifié	EN 319 411-1 NCP+	1.2.250.1.105.23.411.1.3.3.1.0	*Authentification* et Signature	Non
CertEurope eID Corp					Intermédiaire	Non
CertEurope eID Corp	*	Qualifié	EN 319 411-2 QCP-L	1.2.250.1.105.24.411.2.1.1.1.0	Cachet	Non
CertEurope eID Corp	**	Qualifié	EN 319 411-2 QCP-L	1.2.250.1.105.24.411.2.2.1.1.0	Cachet	Non
CertEurope eID Corp		Non qualifié	EN 319 411-1 LCP	1.2.250.1.105.24.411.1.1.1.1.0	Cachet	Non
CertEurope eID Corp		Non qualifié	EN 319 411-1 NCP	1.2.250.1.105.24.411.1.2.1.1.0	Cachet	Non
CertEurope eID Corp		Non qualifié	EN 319 411-1 NCP+	1.2.250.1.105.24.411.1.3.1.1.0	Cachet	Non
CertEurope eID Website					Intermédiaire	Non
CertEurope eID Website	*	Qualifié	EN 319 411-2 QCP-W	1.2.250.1.105.25.411.2.1.1.1.0	Authentification client (Signature)	Non
CertEurope eID Website	*	Qualifié	EN 319 411-2 QCP-W	1.2.250.1.105.25.411.2.1.2.1.0	Authentification serveur	Non
CertEurope eID Website	**	Qualifié	EN 319 411-2 QCP-W	1.2.250.1.105.25.411.2.2.1.1.0	Authentification client (Signature)	Non
CertEurope eID Website	**	Qualifié	EN 319 411-2 QCP-W	1.2.250.1.105.25.411.2.2.2.1.0	Authentification serveur	Non

AC uniquement qualifiée EIDAS pour répondre aux demandes des clients qui souhaitent une qualification exclusivement européenne.

Nom de l'AC	Niveau RGS	Niveau EIDAS	Norme ETSI	Numéro de série (root) OID (end users)	Service	AC en fin de vie
CertEurope eID User		Qualifié	EN 319 411-2 QCP-N	1.2.250.1.105.23.411.2.**3**.1.1.0	*Authentification* et Signature	Non
CertEurope eID User		Qualifié	EN 319 411-2 QCP-N-QSCD	1.2.250.1.105.23.411.2.**3**.2.1.0	*Authentification* et Signature	Non
CertEurope eID Corp		Qualifié	EN 319 411-2 QCP-L	1.2.250.1.105.24.411.2.**3**.1.1.0	Cachet	Non
CertEurope eID Website		Qualifié	EN 319 411-2 QCP-W	1.2.250.1.105.25.411.2.**3**.1.1.0	Authentification serveur	Non
CertEurope eID Website		Qualifié	EN 319 411-2 QCP-W	1.2.250.1.105.25.411.2.**3**.2.1.0	Authentification Client (Signature)	Non

- **Liste des OIDs uniquement RGS***

Liste des OIDs demandées pour des offres qualifiées RGS* sans exigences sur le face-à-face.

Nom de l'AC	Niveau RGS	Niveau EIDAS	Norme ETSI	Numéro de série (root) OID (end users)	Service	AC en fin de vie
CertEurope eID User	*	Non qualifié	EN 319 411-1 LCP	1.2.250.1.105.23.411.1.**4**.1.1.0	*Authentification* et Signature	Non
CertEurope eID Corp	*	Non qualifié	EN 319 411-1 LCP	1.2.250.1.105.24.411.1.**4**.1.1.0	Cachet	Non
CertEurope eID Website	*	Non qualifié	EN 319 411-1 OVCP	1.2.250.1.105.25.411.1.**4**.1.1.0	Authentification Serveur client	Non
CertEurope eID Website	*	Non qualifié	EN 319 411-1 OVCP	1.2.250.1.105.25.411.1.**4**.2.1.0	Authentification serveur	Non

- **Liste des OIDs pour la directive PSD2**

Liste des OIDs compatibles avec la directive PSD2 avec l'ajout des QCStatements prévus par la norme ETSI TS 119 412-1 V1.2.1 (2018-05) et s'appuie sur la norme ETSI TS 119 495 V1.2.1 (2018-11).

Nom de l'AC	Niveau RGS	Niveau EIDAS	Norme ETSI	Numéro de série (root) OID (end users)	Service	AC en fin de vie
CertEurope eID Corp		Qualifié	EN 319 411-2 QCP-L	1.2.250.1.105.24.411.2.**5**.1.1.0	Cachet	Non
CertEurope eID Website		Qualifié	EN 319 411-2 QCP-W	1.2.250.1.105.25.411.2.**5**.1.1.0	Authentification Client (Signature)	Non
CertEurope eID Website		Qualifié	EN 319 411-2 QCP-W	1.2.250.1.105.25.411.2.**5**.2.1.0	Authentification Serveur	Non

- **Liste des AC opérées par CertEurope après la reprise de Click and Trust**

Nom de l'AC	Niveau RGS	Niveau EIDAS	Norme ETSI	Numéro de série (root) OID (end users)	Service	AC en fin de vie
Mercanteo authentification/ signature**	**	Non qualifié	TS 102 042 NCP+	1.2.250.1.98.1.1.18.1.1.1	*Authentification* et Signature	Oui
Mercanteo authentification**	**	Non qualifié	TS 102 042 NCP+	1.2.250.1.98.1.1.18.1.1.2	*Authentification*	Oui
Mercanteo signature**	**	Non qualifié	TS 102 042 NCP+	1.2.250.1.98.1.1.19.1.1.1	Signature	Oui
Admineo authentification/signature*	*	Non qualifié	TS 102 042 LCP	1.2.250.1.98.1.1.20.1.1.1	*Authentification* et Signature	Oui
Admineo authentification*	*	Non qualifié	TS 102 042 LCP	1.2.250.1.98.1.1.20.1.1.2	*Authentification*	Oui
Admineo signature*	*	Non qualifié	TS 102 042 LCP	1.2.250.1.98.1.1.21.1.1.1	Signature	Oui
Mercanteo EU sign	***	Qualifié	eIDAS Art. 51 2 QCP Public+SSCD	1.2.250.1.98.1.1.22.1.1.1	Signature	Oui
Mercanteo EU sign	***	Non qualifié	ETSI TS 101 456 NCP+	1.2.250.1.98.1.1.22.1.1.2	*Authentification*	Oui
Mercanteo 2		Non qualifié	ETSI EN 319 411-1 NCP+	1.2.250.1.98.1.1.18.3.1.1	*Authentification*	Oui