Politique de Certification et de Déclaration des pratiques de certification

Datasure Root CA
Datasure Global CA
SecuSign QSCD à distance

V 1.4

OID : 1.3.6.1.4.1.58753.2.0.1.1
1.3.6.1.4.1.58753.2.1.1.1
1.3.6.1.4.1.58753.4.1.1.1

Niveau de confidentialité : Public

Datasure

L'historique du document est dans le tableau suivant :

Numéro de version	Date	Commentaire
1.0	09/07/2024	Version initiale du document
1.1	07/09/2024	Revue Direction et mises à jour mineures
1.2	10/10/2024	Ajout du service SecuSign QSCD à distance
1.3	19/10/2024	Relecture direction et corrections orthographiques mineures
1.4	06/11/2024	Changement de périmètre Prise en compte des remarques de LSTI

1 Introduction

Datasure est Prestataire de services de confiance qualifié. Dans le cadre de son offre de services, il opère l'Autorité de Certification Datasure avec l'AC Racine Datasure Root CA et l'AC opérationnelle Datasure Global CA, permettant notamment de délivrer des certificats de signature électronique, de cachet électronique, d'authentification de site Internet.

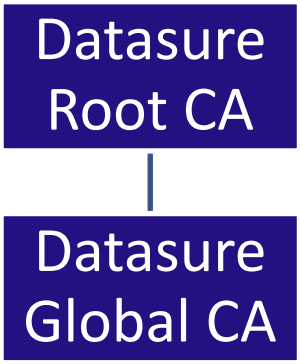
La présente politique vise à être conforme aux référentiels suivants :

- référentiels ETSI EN 319 401, ETSI EN 319 411-1 et ETSI EN 319 411-2,
- référentiels de qualification des services de confiance de l'ANSSI,

La conformité susvisée permet la reconnaissance du service par l'ANSSI comme services qualifiés de délivrance de certificats de signature électronique, de délivrance de certificats de cachet électronique au sens du Règlement européen eIDAS.

L'IGC actuelle est composée de deux AC [OVR-5.4.1-02]

- Une AC racine *offline* nommée Datasure Root CA (ci-après indifféremment appelée l'AC Racine) ;
- Une AC opérationnelle, Datasure Global CA (ci-après indifféremment appelée l'AC Globale), opérée en ligne et visant à émettre différents types de certificats à destination des porteurs de certificats finaux.



Datasure s'engage à ce que l'ensemble des AC de la hiérarchie, existantes et à venir, respecte les termes de la présente Politique de Certification (PC) [OVR-5.4.1-03].

Datasure opère, dans le cadre de l'émission de certificats de signature et de cachet qualifié, un service de gestion de dispositifs de création de signature électronique. Celui-ci vise, pour les catégories de certificats qualifiés, à être lui-même qualifié au titre de l'article 29bis. Le service de gestion de dispositifs de création de signature électronique n'étant pas dissocié du service d'émission de certificats, la présente PC inclue également l'ensemble des exigences applicables à ce service et vise la conformité aux normes suivantes[1] [ETSI TS 119 431-1/OVR-5.1-01]:

- ETSI TS 119 431-1
- ETSI TS 119 431-2
- CEN EN 419 241

1.1 Identification du document

La présente Politique de Certification et Déclaration des Pratiques de Certification (PC/DPC) et les différents types de certificats sont identifiés par des OID [GEN-6.3.3-12].

La PC/DPC de l'AC Racine est identifié par l'OID suivant : 1.3.6.1.4.1.58753.2.0.1.1
La PC/DPC de l'AC Globale est identifié par l'OID suivant : 1.3.6.1.4.1.58753.2.1.1.1

Cet identifiant est composé de la façon suivante :

Racine Datasure	Type de service de confiance	Identifiant du service	Document	Version
1.3.6.1.4.1.58753	2 pour les autorités de certification	0 pour Root CA	1 pour PC	1
		1 pour Global CA	1 pour PC	1
	4 pour les services de signature	1 pour le QSCD opéré à distance	1 pour PC	1

Aux fins de rationalisation, les politiques de Root CA et Global CA forment en effet un seul et même présent document.

[1] En l'absence d'acte d'exécution et de procédure de qualification ANSSI pour ce type de service, ces normes ont été utilisées.

Pour chacun des profils de certificats, un OID est défini :

OID de la présente politique				
1.3.6.1.4.1.58753.2.1.1.1	.1 pour qualifié	.1 pour personne physique	.1	Certificat **QCP-n-QSCD** (personne physique) reposant sur dispositif certifié QSCD carte à puce
1.3.6.1.4.1.58753.2.1.1.1	.1 pour qualifié	.1 pour personne physique	.2	Certificat **QCP-n** (personne physique) ne reposant pas sur dispositif certifié QSCD
1.3.6.1.4.1.58753.2.1.1.1	.1 pour qualifié	.1 pour personne physique	.3	Certificat **QCP-n-QSCD** (personne physique) reposant sur dispositif certifié QSCD opéré à distance
1.3.6.1.4.1.58753.2.1.1.1	.1 pour qualifié	.2 pour personne morale	.1	Certificat **QCP-l-QSCD** (personne morale) reposant sur dispositif certifié QSCD
1.3.6.1.4.1.58753.2.1.1.1	.1 pour qualifié	.2 pour personne morale	.2	Certificat **QCP-l** (personne morale) ne reposant pas sur dispositif certifié QSCD
1.3.6.1.4.1.58753.2.1.1.1	.1 pour qualifié	.2 pour personne morale	.3	Certificat **QCP-l** (personne morale) d'unité d'horodatage
1.3.6.1.4.1.58753.2.1.1.1	.2 pour certifié	.1 pour personne physique	.1	Certificat **NCP+** (personne physique)
1.3.6.1.4.1.58753.2.1.1.1	.2 pour certifié	.2 pour personne morale	.1	Certificat **NCP** (personne morale) authentification
1.3.6.1.4.1.58753.2.1.1.1	.2 pour certifié	.1 pour personne physique	.2	Certificat **LCP** personne physique
1.3.6.1.4.1.58753.2.1.1.1	.2 pour certifié	.2 pour personne morale	.2	Certificat **LCP** personne morale
1.3.6.1.4.1.58753.2.1.1.1	.3 pour non certifié	.1 pour personne physique	.1	Certificat **Biométrie**

Pour chacun des profils de signature, un OID est défini [119431-2/OVR-9-02/ OVR-9-10].

OID de la présente politique				
1.3.6.1.4.1.58753.4.1.1.1	.1 pour qualifié	.1 pour personne physique	.3	Signature avec Certificat **QCP-n-QSCD** (personne physique) reposant sur dispositif certifié QSCD opéré à distance [EUSCP]
1.3.6.1.4.1.58753.4.1.1.1	.1 pour qualifié	.2 pour personne morale	.1	Cachet avec Certificat **QCP-l-QSCD** (personne morale) reposant sur dispositif certifié QSCD [EUSCP]
1.3.6.1.4.1.58753.4.1.1.1	.2 pour certifié	.1 pour personne physique	.1	Signature avec Certificat **NCP+** (personne physique) [NSCP]
1.3.6.1.4.1.58753.4.1.1.1	.2 pour certifié	.1 pour personne physique	.2	Signature avec Certificat **LCP** personne physique [LSCP]
1.3.6.1.4.1.58753.4.1.1.1	.3 pour non certifié	.1 pour personne physique	.1	Signature Certificat **Biométrie**

La politique de signature peut être facilement déduite de la politique de certification [119431-2/OVR-8.2-08]. L'ensemble des politiques sont conforme à la politique de signature avancée s'appuyant sur des certificats x.509 (0.4.0. 19431.2.1.2) définie dans le standard ETSI TS 119431-2 [119431-2/OVR-9-01A]

1.2 Entités intervenant dans l'IGC

1.2.1 Autorité de certification

Une Autorité de Certification (AC) désigne l'autorité en charge de la création, la délivrance, la gestion et la révocation des Certificats au titre de la Politique de Certification.

1.2.2 Autorité d'Enregistrement

L'Autorité d'Enregistrement (AE) est une composante de l'AC, responsable de l'identification et de l'authentification des demandeurs de Certificats.

1.2.3 Porteurs de Certificats

Le Porteur de Certificat est la personne physique ou morale détentrice du Certificat et décrite dans le champ sujet du certificat.
Dans le cadre de la présente PC, le porteur de certificat et le souscripteur au service d'émission de certificat sont confondus.

1.2.4 Tiers utilisateur de certificat

Les tiers utilisateurs (*third parties* au sens de l'ETSI) sont les personnes, physiques ou morales, s'appuyant sur les informations contenues dans un Certificat dans le cadre de leur service.

1.2.5 Autres participants

Datasure s'autorise à faire intervenir d'autres entités [OVR-5.4.3-01]. Le cas échéant, celle-ci pourront être décrites dans la DPC confidentielle.

1.3 Usage des certificats

1.3.1 Domaines autorisés

1.3.1.1 Clé privée et Certificat de l'AC Racine

La clé privée de l'AC Racine est utilisée pour :

- Signer les AC intermédiaires ;
- Signer la liste des autorités révoquées (LAR)

Le certificat associé permet :

- De vérifier le certificat de l'AC intermédiaire ;
- De vérifier l'origine et l'intégrité de la LAR.

1.3.1.2 Clé privée et Certificat de l'AC Globale

La clé privée de l'AC Globale est utilisée pour :

- Signer les certificats des porteurs ;
- Signer la liste des certificats révoqués (LCR).
- Signer les certificats des répondeurs OCSP.

Le certificat associé permet :

- De vérifier le certificat du porteur final ;
- De vérifier l'origine et l'intégrité de la LCR.
- De vérifier les certificats des répondeur OCSP.

1.3.1.3 Clé privée et Certificat des porteurs

Les usages sont décrits dans le tableau ci-dessous [TS 119231-2/OVR-6.1-05] :

Profil	Usage de la clé	Usage du certicat
Offre Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Création de signature électronique qualifiée au sens du règlement eIDAS	Vérification de la signature générée, vérification de l'intégrité du document signé et de l'identité du signataire.
Offre Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3		
Offre Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Création d'une signature avancée avec certificat qualifié	Vérification de la signature générée, vérification de l'intégrité du document signé et de l'identité du signataire.
Offre Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Création de cachet électronique qualifié au sens du règlement eIDAS	Vérification de l'origine et de l'intégrité des données scellées.
Offre Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1		
Offre Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Cachet avancé avec certificat qualifié	Vérification de l'origine et de l'intégrité des données scellées.
Offre Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Création de contremarque de temps	Vérification des contremarques de temps
Offre C1. Certificat signature NCP+ personne physique	Création de signature avancée	Vérification de la signature générée, vérification de l'intégrité du document signé et de l'identité du signataire
Offre C2. Certificat authentification NCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	Authentification client	Vérification de l'identité d'un client
Offre C3. Certificat LCP personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Création de signature avancées	Vérification de la signature générée, vérification de l'intégrité du document signé et de l'identité du signataire
Offre C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Création de cachet avancé	Vérification de l'origine et de l'intégrité des données scellées.
Offre B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Création de signature avancée	Vérification de la signature générée, vérification de l'intégrité du document signé et de l'identité du signataire

1.3.1.4 Autres clés et certificats

Profil	Usage de la clé	Usage du certicat
Certificat des répondeurs OCSP	Création de réponse OCSP	Vérification des jetons OCSP émis

1.3.2 Domaines d'utilisation interdits

Tout autre usage que ceux prévus au paragraphe précédent est interdit.

1.4 Gestion de la PC

1.4.1 Entité gérant la PC

Datasure s'est doté d'une entité de gouvernance ayant la responsabilité globale des activités de l'AC et l'autorité pour approuver la présente PC/DPC [REQ-6.1-06] ainsi que les politiques de signature qu'elle contient [TS 119 431-1/ OVR-9-04].

Cette entité de gouvernance est responsable de la validation et de la gestion de la PC. L'entité de Gouvernance, en tant que responsable de l'AC, a la charge de mettre en œuvre les exigences de la présente PC/DPC [REQ-6.1-07]. Datasure s'offre la possibilité de sous-traiter certaines opérations [OVR-5.4.1-01].
En cas de recours à des sous-traitants, Datasure garde l'entière responsabilité de la bonne mise en œuvre des exigences de la présente PC/DPC même en cas de sous-traitance [REQ-6.3-05/ REQ-7.1.1-08] [119231-2/ OVR-7.13-04]. Cela est réalisé au travers d'accords contractuels définissant les obligations et responsabilités du sous-traitant et au travers de contrôles [REQ-6.3-06/ REQ-7.1.1-07].
Ce point est en particulier applicable en cas de délégation de l'infrastructure technique d'opération du QSCD [TS 119 431-1/OVR-5.3.1-01]

Datasure revoit régulièrement la présente PC/DPC et les politiques et procédures associées. Il réalise également des contrôles (voir §8) afin de s'assurer de la bonne mise en œuvre des mesures énoncées dans la présente PC/DPC [REQ-6.1-08].

1.4.2 Point de contact

Toute demande relative au service est à adresser au point de contact fourni à l'adresse suivante :

Datasure
Autorité de certification
8 rue Alfred Maurel
34120 PÉZENAS (France)

Datasure peut également être contacté au travers du formulaire de contact disponible sur son site internet : https://www.datasure.net

1.4.3 Entité déterminant la conformité d'une DPC avec cette PC

L'AC doit être pourvue d'une direction ayant autorité et une responsabilité finale pour déterminer la conformité de la DPC avec la PC.

1.4.4 Procédures d'approbation de la conformité de la DPC

L'AC met en place un processus d'approbation de la PC et de la conformité de la DPC avec la PC, ainsi que des politiques de signature incluses dans le document [119431-2/OVR-9-06/OVR-9-07].
L'AC est responsable de la gestion (mise à jour, révisions) de la PC/DPC. Toute demande de mise à jour de la PC/DPC doit suivre le processus d'approbation mis en place ainsi que la procédure d'amendement (voir §9.12). Toute nouvelle version de la PC/DPC doit être publiée sans délai, conformément aux exigences du paragraphe 2.2 [REQ-6.1-10].

2 Responsabilité concernant les informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

L'AC Datasure met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats.
La fonction de publication est accessible en HTTP(s) sur le site de publication suivant :
https://www.datasure.net/tsp/.
Le site de publication est accessible publiquement sur internet [DIS-6.1-08, DIS-6.1-09] [ETSI TS 119 431-1/ OVR-5.1-03/ OVR-6.1-04].

La fonction d'information sur l'état des certificats s'appuie sur la mise à disposition d'une ARL et CRL à l'adresse suivante :

AC Racine	http://pki-p.datasure.net/datasure/arl/DATASURE_Root_CA.crl
AC Globale	http://pki-p.datasure.net/datasure/crl/DATASURE_Global_CA.crl

Cette fonction d'information sur l'état des certificats est également complétée par la mise en œuvre d'un répondeur OCSP à l'adresse suivante :

OSCP	http://ocsp-p.datasure.net/DATASURE_Global_CA

2.2 Informations devant être publiées

L'AC Datasure publie les informations suivantes à destination des porteurs et utilisateurs de certificats [REQ-6.1-05A] :

- la présente politique de certification/déclaration des pratiques de certification, couvrant l'ensemble des rubriques de la [RFC3647] et conforme aux PC Type RGS de l'ANSSI, ainsi qu'aux exigences des normes ETSI 319401, ETSI EN 319411-1 et ETSI EN 319411-2 [BRG/OVR-5.2-02] [ETSI TS 119 431-1/ OVR-5.1-01],[TS 119 431-1/ OVR-6.1-01],],[TS 119 431-2/ OVR-9-08];

- les listes des certificats révoqués (porteurs et AC) ;
- les certificats de l'AC, en cours de validité ;
- le certificat de l'AC Racine ainsi que son condensat SHA512 ;
- les CGUs du service d'émission de certificat [REQ-6.2-01/DIS-6.1-04], [TS 119 431-1/ OVR-6.1-01] ;
- le « *PKI Disclosure Statement* ».

Les détails confidentiels de la déclaration de pratiques ne font pas l'objet d'une publication dans la présente PC/DPC et sont consignés dans une DPC confidentielle.
Concernant la PC/DPC, Datasure se conforme à la dernière version du document CABForum « *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates* » publiée sur http://www.cabforum.org. En cas d'inconsistance entre la présente PC/DPC et les exigences du CABForum, ce sont les exigences du CABForum qui seront applicables [BRG].

Les différents documents, y compris la présente PC/DPC et les CGUs sont publiés sous forme électronique, au format PDF scellé par un cachet qualifié Datasure afin d'assurer leur intégrité et leur origine [REQ-6.2-04/REQ-6.2-06].
L'ensemble des documents sont disponibles en langue française [REQ-6.2-05].
Datasure assure une disponibilité du site de publication 24h/24 et 7J/7 [BRG/OVR-5.2-05/DIS-6.1-07A] [ETSI TS 119 431-1/ OVR-5.1-03 / OVR-6.1-03]. En cas de panne technique, ou de tout cas d'indisponibilité qui ne serait pas sous le contrôle de Datasure, Datasure fera tout son possible pour que l'information ne reste pas indisponible plus de 48 heures ouvrées consécutives [DIS-6.1-07A].

2.3 Délais et fréquences de publication

Les informations liées à l'IGC (nouvelle version de la PC/DPC, formulaires, etc.) sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. En particulier, toute nouvelle version est communiquée au porteur ou MC lors d'une demande de renouvellement de clé et fait l'objet d'un nouvel accord. Les systèmes publiant ces informations sont disponibles 24h sur 24 et 7j/7.

Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants et les systèmes les publiant ont une disponibilité de 24h/24 et 7j/7.
Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres 4.10.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).

3 Identification et authentification

3.1 Nommage

3.1.1 Type de nom

Les noms utilisés sont conformes aux spécifications de la norme [X.500].
Dans chaque certificat conforme à la norme [X.509], l'AC émettrice (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" (DN) répondant aux exigences de la norme [X.501].
Des règles sur la construction du DN de ces champs sont précisées dans la section 7 et sont conformes

- Aux exigences de l'Annexe A.4 du RGS ;
- Aux exigences de la série de normes ETSI 319412.

Datasure n'impose pas de limites sur la taille de champs du DN à l'exception des limitations de la RFC 5280 [OVR-5.2-11].

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats sont explicites[119431-2/ OVR-B.1-01/ OVR-B.1-02].
Les pseudonymes ne sont pas autorisés pour cette version de la PC/DPC.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	le DN du porteur est construit à partir des nom et prénom de son état civil tel que porté sur les documents d'identité présentés lors de son enregistrement auprès de l'AE ou, le cas échéant, du MC [RGS].
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Le champ « DN » du certificat du service applicatif contient son nom du service de création de cachet.
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	
Cas C1. Certificat signature NCP+ personne physique	Voir cas Q1

1.3.6.1.4.1.58753.2.1.1.1.2.1.1	
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Voir cas Q4
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Voir cas Q1
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Voir cas Q4
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Voir cas Q1
Certificat d'OCSP	Le DN désigne le service OCSP de façon explicite
Certificat d'AC	Le DN désigne l'AC de façon explicite

3.1.3 Pseudonymisation des porteurs

La présente version de la PC/DPC interdit l'usage de pseudonymes.

3.1.4 Règles d'interprétation des différentes formes de nom

Le chapitre 7 fournit les éventuelles règles d'interprétation.

3.1.5 Unicité des noms

Le DN du champ "subject" de chaque certificat de porteur permet d'identifier de façon unique le porteur (personne physique ou service) correspondant au sein du domaine de l'AC.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Le DN respecte les règles correspondantes définies dans le document [RGS_A4], notamment pour le traitement des cas d'homonymie au sein du domaine de l'AC. Le champ SERIALNUMBER permet d'éviter le cas d'homonymie.
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Le champ « DN » du certificat du service applicatif contient son nom du service de création de cachet et la société, identifié de façon unique par son numéro d'enregistrement au registre du commerce.
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Dans cette version de la PC/DPC, Datasure ne fournit des certificats d'horodatage uniquement que pour le service de

	l'AH Datasure. Datasure s'assure que le DN est unique à l'aide d'un incrément du numéro de l'UH (voir §7)
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	Voir cas Q1
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Voir cas Q4
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Voir cas Q1
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Voir cas Q4
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Voir cas Q1
Certificat d'OCSP	Datasure s'assure que le DN est unique
Certificat d'AC	Datasure s'assure de ne pas donner deux fois le même DN à l'une des AC filles.

Durant toute la durée de vie de l'AC, un DN attribué à un porteur de certificats ne peut être attribué à un autre porteur [GEN-6.3.3-10].

Certificat de personne physique	L'ALEA du champ SERIALNUMBER permet d'éviter que le même DN soit attribuer à deux porteurs différents[2].
Certificat de personne morale ou d'organisation	Durant toute la durée de vie de l'AC, le nom du service de création de cachet rattaché à une entité ne peut être attribué à une autre entité.

En outre, chaque certificat a un numéro de série unique. Ce numéro de série est non-prédictible [GEN-6.3.3-02A].

3.1.6 Identification, authentification et rôle des marques déposées

L'AC est responsable de l'unicité des noms de ses porteurs et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.
En cas d'utilisation indue d'une marque déposée, l'AC pourra révoquer le certificat.

[2] Il est à noter que l'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC, mais que ce numéro est propre au certificat et non pas au porteur et ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un porteur donné. De ce fait, le champ SERIALNUMBER du DN est utilisé pour différentier les porteurs et ne doit pas être confondu avec le numéro de série du certifcat.

3.1.7 Informations non vérifiées du porteur

Non applicable

3.2 Validation initiale de l'identité

L'enregistrement d'un porteur peut se faire soit directement auprès de l'AE ou d'une AED, soit via un mandataire de certification de l'entité dans le cas des certificats délivrés à des agents d'Autorité Administrative, entité publique ou des collaborateurs d'entreprises. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

3.2.1 Méthode pour prouver la possession de la clé privée

Quel que soit le type de certificat, il est fourni à l'AC une preuve de possession de sa clé privée correspondant à la clé publique au travers de la fourniture d'une CSR au format PKCS#10

3.2.2 Validation de l'identité d'un organisme

L'identité d'un organisme est réalisée au travers de la vérification de l'identité du demandeur responsable de certificat. Les modalités de vérification de l'identité du porteur de certificat sont vérifiées conformément au §3.2.3. Le porteur doit être mandaté par le responsable légal de l'organisation, conformément au §3.2.4 dans la cas où le responsable légal n'est pas le demandeur [REG-6.2.2-10].

L'identité de l'organisation doit être justifiée par un document officiel, typiquement un K-BIS de moins de 3 mois pour une société [REG-6.2.2-12/REG-6.2.2-03].

3.2.3 Validation de l'identité d'un individu

3.2.3.1 Enregistrement d'un porteur [Particulier] - Certificat de personne physique

L'AE Datasure doit s'assurer de l'identité du porteur et doit s'assurer que la demande de certificat est complète, autorisée et correcte. Ces éléments doivent être confirmés par des éléments de preuve qui doivent être collectés dans un dossier d'enregistrement [REG-6.2.2-0].

Dossier d'enregistrement :
Le dossier d'enregistrement, déposé auprès de l'AE, doit au moins comprendre :

- une demande de certificat écrite signée, et datée de moins de 3 mois, par le futur porteur,
- un document officiel d'identité en cours de validité du futur porteur comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie,
- l'adresse postale et / ou l'adresse mail permettant à l'AC de contacter le porteur,

- l'acceptation des conditions générales d'utilisation [REQ-6.2-03].

Dans le cas où un QSCD est exigé, l'AC doit s'assurer qu'un QSCD est bien utilisé.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	La présente version de la PC/DPC ne considère que des cas d'usage où l'AC fournit le QSCD à l'utilisateur. De ce fait, l'engagement relatif à l'utilisation d'un dispositif qualifié de création de signature n'est pas demandé dans le dossier.
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	

Concernant les modalités de vérification de l'identité, celle-ci diffèrent selon les cas d'usage.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	La vérification de l'identité du porteur par l'AE est réalisée lors d'un dispositif équivalent au face-à-face au sens du Règlement eIDAS [REG-6.2.2-02]. En particulier, la présente version de la PC/DPC autorise comme dispositif équivalent : - l'utilisation d'un dispositif certifié PVID - L'utilisation d'un dispositif FranceConnect+ (MIE de niveau substantiel) Dans le cas du rattachement à la personne morale, des exigences complémentaires sont applicables (voir 3.2.3.2)
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	Les modalités sont identiques au cas Q1. Le rattachement à la personne morale n'est pas applicable.
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Les modalités sont identiques au cas Q1. Dans le cas du rattachement à la personne morale, des exigences complémentaires sont applicables (voir 3.2.3.2)
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les modalités de vérification de l'identité du responsable de certificat sont identiques au cas Q1. Les modalités de vérification de l'organisation (§3.2.2) et de l'autorité du demandeur (§3.2.4) doivent également être réalisées.
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les modalités sont identiques au cas Q4.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Les modalités sont identiques au cas Q4.
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Le porteur de certificat est un rôle de confiance de Datasure.
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	La vérification de l'identité du porteur par l'AE est réalisée avec un dispositif de vérification d'identité à distance apportant des garanties similaires à un face-à-face [REG-6.2.2-05, REG-6.2.2-08].

	Dans le cas du rattachement à la personne morale, des exigences complémentaires sont applicables (voir 3.2.3.2)
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	La vérification de l'identité du responsable de certificat par l'AE est réalisée avec un dispositif de vérification d'identité à distance apportant des garanties similaires à un face-à-face [REG-6.2.2-05, REG-6.2.2-08]. Les modalités de vérification de l'organisation (§3.2.2) et de l'autorité du demandeur (§3.2.4) doivent également être réalisées.
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	La vérification de l'identité est réalisée avec la transmission électronique d'une pièce d'identité valide (CNI, passeport ou carte de séjour)
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Les modalités du cas C2 sont réalisées sur le responsable de certificat. Les modalités de vérification de l'organisation (§3.2.2) et de l'autorité du demandeur (§3.2.4) doivent également être réalisées.
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	La vérification de l'identité est assurée par le commanditaire de la signature.
Certificat d'OCSP	Processus interne à Datasure
Certificat d'AC	L'identité des différents acteurs de la KC sont vérifiés

Pour tous les cas sauf le B1, la présentation d'une pièce d'identité valide (dont la référence est conservée) permet de s'assurer de l'authenticité des éléments suivants : Nom complet du demandeur, date et lieu de naissance et permet de distinguer la personne d'un homonyme [REG-6.2.2-06].

3.2.3.2 Enregistrement d'un porteur personne physique rattaché à une personne morale[Entreprise] / [Administration] sans mandataire de certification (MC)

Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre :

- Si le demandeur n'est pas le responsable légal, un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le futur porteur auquel le certificat doit être délivré. Ce mandat doit être signé pour acceptation par le futur porteur bénéficiaire ;
- Si la personne morale est une structure privée (entreprise, association…) toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers, ...), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;
- Si la personne morale est une structure privée (entreprise, association…), tout document attestant de la qualité du signataire de la demande de certificat,
- Pour une autorité administrative une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,

- un document officiel d'identité en cours de validité du futur porteur, comportant une photographie d'identité (carte nationale d'identité, passeport ou carte de séjour). Ces documents sont transmis à l'AE qui en conserve une copie ;
- l'adresse postale et / ou l'adresse mail permettant à l'AC de contacter le porteur ;
- l'acceptation des conditions générales d'utilisation.

Le porteur est informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme.

Procédure de vérification de l'identité du porteur : voir §3.2.3.1.

Concernant la vérification de l'association entre le porteur physique et la personne morale, les vérifications suivantes sont réalisées le cas échéant [REG-6.2.2-09].

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Si le demandeur est le représentant légal de la personne morale (par exemple, présence sur le KBIS) le lien est établit *de facto*. Sinon, le mandat suscité doit être fournit, ainsi qu'une copie de la pièce d'identité du responsable légal ou un équivalent. Les modalités de vérification de la personne morale sont indiquées en §3.2.2
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	Le rattachement à la personne morale n'est pas applicable.
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Les modalités sont identiques au cas Q1
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Non applicable (certificat personne morale)
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	Le rattachement à la personne morale n'est pas applicable.
Cas C2 Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Non applicable (certificat personne morale)
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Le rattachement à la personne morale n'est pas applicable.

Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Non applicable (certificat personne morale)
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Le rattachement à la personne morale n'est pas applicable.
Certificat d'OCSP	Non applicable
Certificat d'AC	Non applicable

3.2.3.3 Enregistrement d'un Mandataire de Certification (MC)

Datasure est amené à constituer un dossier d'enregistrement pour un Mandataire de Certification pour répondre aux besoins suivants :

- Utilisation du dossier du MC comme référence pour les données d'identification de l'entité de tous les porteurs présentés par le MC.
- fourniture de certificats électronique au MC pour qu'il puisse signer les dossiers d'enregistrement de porteurs de l'entité qu'il représente, s'authentifier auprès du service d'AC et transmettre les dossiers de façon sécurisée.

Le dossier d'enregistrement d'un MC comprend :

- un mandat signé électroniquement (signature avancée) par un représentant légal de l'entité désignant le MC ;
- un engagement signé, et daté de moins de 3 mois, du MC, auprès de l'AC, à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs, L'engagement indique également l'acceptation de son mandat et l'obligation du MC à signaler à l'AE son départ de l'entité ;
- Une pièce, soumise par le représentant légal, attestant de l'existence de l'organisation (typiquement un KBIS pour une entreprise) ;
- un document officiel d'identité en cours de validité du MC, comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ;

La vérification de l'identité du MC est réalisée par un dispositif équivalent à un face-à-face[3].

3.2.3.4 Enregistrement d'un porteur [Entreprise] / [Administration] via un MC

Le mandataire réalise le face-à-face avec le porteur final et soumet à l'AC :

- Une demande de certificat signé électroniquement à l'aide de son propre certificat ;
- Une copie de la pièce d'identité du demandeur ;

[3] PVID ou FC+

- Le cas échéant, suivant le type de certificat choisi, la CSR.

3.2.4 Validation de l'autorité du demandeur

Datasure ne considère que des cas d'usage où le demandeur (Subject au sens de l'ETSI) et l'abonné (Subscriber au sens de l'ETSI) sont confondus [REG-6.2.2-19/REG-6.2.2-20]. De ce fait, l'abonné ne peut jamais être Datasure, sauf dans le cas où Datasure émet des certificats pour son propre compte [REG-6.2.2-24A]. Datasure dispose d'une procédure specifique pour ce cas [REG-6.2.2-25]. De même, les CGUs ne sont pas scindées en une partie « abonnée » et une partie « porteur » [REG-6.3.4-09/ REG-6.3.4-12].

Pour les certificats de personne physique rattachés à une personne morale, ceci est fait en même temps que l'enregistrement du porteur (voir 3.2.2.2 et 3.2.2.3)

3.2.5 Critères d'interopérabilité

Non applicable pour cette version de la PC/DPC. Aucune certification croisée (« cross-certification ») n'est réalisée [CSS-6.3.9-14].

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

Le renouvellement de la bi-clé d'un porteur entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la bi-clé correspondante.
Le processus de renouvellement est identique au processus de demande initiale.

3.3.1 Identification et validation pour un renouvellement courant

Voir chapitre 3.2.

3.4 Identification et validation d'une demande de révocation

La demande de révocation peut être réalisée en ligne après authentification formelle du porteur à l'adresse url communiquée par l'AE lors de la délivrance du certificat. L'authentification peut s'appuyer :

- Sur un moyen d'authentification fournit par le porteur à l'enregistrement,
- Par une identification correspondant au niveau LCP ou équivalent (vérification pièce d'identité, passeport ou titre de séjour).

Une demande peut également être envoyé au point de contact décrit dans la présente PC.
Dans tous les cas, les demandes de révocation font l'objet d'une authentification et d'une vérification à partir d'une source fiable [REG-6.3.1-01].

4 Exigences opérationnelles sur le cycle de vie des certificats

4.1 **Demande de certificat**

4.1.1 Origine d'une demande de certificat

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	le demandeur ne peut être que le futur porteur du certificat.
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Le demandeur est le responsable légal de la personne morale ou une personne mandatée.
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	Voir cas Q1
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Voir cas Q4
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Voir cas Q1
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Voir cas Q4
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Voir cas Q1
Certificat d'OCSP	Le demandeur est la composante opérant le serveur OCSP
Certificat d'AC	Le demandeur est le responsable de l'AC.

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

Les informations suivantes doivent au moins faire partie de la demande de certificat

<table>
<tr><td>Cas Q1. QCP-n-QSCD sur carte à puce
1.3.6.1.4.1.58753.2.1.1.1.1.1.1</td><td rowspan="3">- le nom du porteur à utiliser dans le certificat (nom réel) ;
- les données personnelles d’identification du porteur
Dans le cas où le certificat est rattaché à une personne morale, les données d'identification de l'entité (sauf si l'enregistrement est effectué par l'intermédiaire d'un MC) doivent également être transmises.</td></tr>
<tr><td>Cas Q2. QCP-n-QSCD à distance
1.3.6.1.4.1.58753.2.1.1.1.1.1.3</td></tr>
<tr><td>Cas Q3. QCP-n (logiciel)
1.3.6.1.4.1.58753.2.1.1.1.1.1.2</td></tr>
<tr><td>Cas Q4. QCP-l-QSCD à distance
1.3.6.1.4.1.58753.2.1.1.1.1.2.1</td><td rowspan="4">- le nom de l’organisation à utiliser dans le certificat (nom réel) ;
- les données personnelles d’identification du responsable de certificat
- les données personnelles d’identification du responsable légal, s’il n’est pas le porteur</td></tr>
<tr><td>Cas Q5. QCP-l-QSCD sur carte à puce
1.3.6.1.4.1.58753.2.1.1.1.1.2.1</td></tr>
<tr><td>Cas Q6. QCP-l (logiciel)
1.3.6.1.4.1.58753.2.1.1.1.1.2.2</td></tr>
<tr><td>Cas Q7. QCP-l (horodatage)
1.3.6.1.4.1.58753.2.1.1.1.1.2.3</td></tr>
<tr><td>Cas C1. Certificat signature NCP+ personne physique
1.3.6.1.4.1.58753.2.1.1.1.2.1.1</td><td>Voir cas Q1</td></tr>
<tr><td>Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel)
1.3.6.1.4.1.58753.2.1.1.1.2.2.1</td><td>Voir cas Q4</td></tr>
<tr><td>Cas C3. Certificat LCP personne physique – signature à distance
1.3.6.1.4.1.58753.2.1.1.1.2.1.2</td><td>Voir cas Q1</td></tr>
<tr><td>Cas C4. Certificat LCP personne morale (logiciel)
1.3.6.1.4.1.58753.2.1.1.1.2.2.2</td><td>Voir cas Q4</td></tr>
<tr><td>Cas B1. Certificat Biométrie
1.3.6.1.4.1.58753.2.1.1.1.3.1.1</td><td>Voir cas Q1</td></tr>
<tr><td>Certificat d’OCSP</td><td>Le CN du répondeur OCSP</td></tr>
<tr><td>Certificat d’AC</td><td>Le CN de la nouvelle AC.</td></tr>
</table>

En particulier, durant le processus d’enregistrement l’AC transmet les CGUs au porteur [OVR-6.3.4-04]. Les CGUs sont écrites au moins en Français [OVR-6.3.4-04]. Les CGUs sont complétées par une déclaration d’applicabilité de l’IGC (« *PKI Disclosure statement* »).
Elles font l’objet d’une signature par le demandeur à l’aide d’une signature avancée.

Par ailleurs, l'AE s'assure de disposer d'une information permettant de contacter le MC ou le futur porteur du certificat.

Pour l'ensemble des signatures à distance, la création d'un certificat est intrinsèquement lié à un processus de signature qui s'assure :

- que le document est présenté au signataire avec un rendu exacte (« what you see is what you sign ») démontré par le calcul de l'empreinte numérique unique (SHA256). Dans la présente version du service de signature, le document au format PDF est affiché dans le navigateur du signataire. Le signataire a la possibilité de le parcourir dans son intégralité [119431-2/ ASI-8.1-03] L'affichage à travers un wrapper PDF suit strictement la norme PDF [119431-2/ ASI-8.1-04/ ASI-8.1-05] et le hash du document calculé au moment de l'affichage est conservé en dossier de preuve. Les futurs versions de la présente PC pourront envisager d'autres documents que le PDF. Le document à signer peut être téléchargé par le signataire [119431-2/ ASI-8.1-10].
- Que le consentement du signataire est explicitement recueilli par une double action du signataire mentionnant explicitement l'action de signature [119431-2/ ASI-8.1-08].
- Que le signataire est bien en mesure d'identifier la politique de signature applicable [119431-2/ ASI-8.2-07].

4.2 Traitement d'une demande de certificat

La présente PC ne considère que l'AE Datasure comme service d'enregistrement [REG-6.3.2-01]. L'AE Datasure est la seule source autorisée d'enregistrement de certificats.

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

Les identités "personne physique" et, le cas échéant, "personne morale" sont vérifiées conformément aux exigences du chapitre 3.2 [REG-6.2.2-01].

L'AE, ou le MC le cas échéant, effectue les opérations suivantes :

- valider l'identité du futur porteur ;
- vérifier la cohérence des justificatifs présentés ;
- vérifier que le futur porteur a pris connaissance des modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation).

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Dans le cas d'une demande via un MC, celui-ci retransmet le dossier à l'AE après avoir effectué les opérations ci-dessus. L'AE doit alors s'assurer que la demande correspond bien au mandat du MC.
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat et, le cas échéant, de la bi-clé vers la fonction adéquate de l'IGC.

L'AE conserve ensuite une trace des justificatifs d'identité présentés, les différents justificatifs ou les informations de traçabilité (sous une forme électronique durable).
Datasure a la possibilité de sous-traiter à une AE déléguée (AED) ou à un opérateur délégué (OED) tout ou partie des tâches d'enregistrement et de révocation. Une convention encadre alors l'ensemble des exigences à respecter.

4.2.2 Acceptation ou rejet de la demande

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

4.2.3 Durée d'établissement du certificat

Les durées d'établissement des certificats sont précisés dans la section relative au profil (§7). De façon générale, les durées suivantes sont appliquées

Certificats de signature électronique éphémère	24 heures
Certificats de signature et cachet électronique persistants	1 à 3 ans
Certificats d'horodatage	5 ans (l'utilisation de la clé privée est limitée à 1 à 3 ans)
Certificats de sites web	1 an au maximum

Datasure n'émet pas de certificat dont la durée de vie excède la durée de vie de l'AC [GEN-6.3.3-05, GEN-6.3.3-06].

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments destinés au porteur, en particulier le certificat. L'AC émet les certificats de façon à assurer leur authenticité [GEN-6.3.3-01]. L'AC met en œuvre des mesures contre la falsification de certificat, en particulier en utilisant une cryptographie à l'état de l'art [GEN-6.3.3-02] et en s'assurant que l'émission du certificat est lié à l'enregistrement [GEN-6.3.3-04].

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

L'AC met à disposition le certificat au demandeur [DIS-6.1-01A], où le cas échéant, au service de signature ou de cachet Datasure mettant en œuvre le certificat de signature pour le compte du

signataire [DIS-6.1-02A]. Les modalités peuvent varier selon le type de certificat. Il n'est pas prévu de mécanisme de diffusion des certificats à l'intention de tiers [DIS-6.1-01B/DIS-6.1-01C].

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Datasure s'assure que le certificat est bien remis au bon porteur par l'envoi d'un recommandé avec accusé de réception
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	Dans le cas du QSCD à distance, l'AC Datasure n'a pas généré elle-même la bi-clé du porteur, cependant, Datasure, dans son rôle d'opérateur de QSCD à distance, garantit que le certificat est bien associé à la clé privée correspondante. Le processus de remise est un processus automatisé interne à Datasure.
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	La remise du certificat est faîte par email à l'adresse fournie par le porteur
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	S'agissant également de l'usage du QSCD à distance, similaire au cas Q2.
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les modalités sont similaires au cas Q1.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Les modalités sont similaires au cas Q3.
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Datasure ne générant des certificats d'horodatage que pour son propre usage, la délivrance du certificat est encadrée par une procédure interne
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	S'agissant également de l'usage du QSCD à distance, similaire au cas Q2.
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Les modalités sont similaires au cas Q3.
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Similaire au cas Q2.
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Les modalités sont similaires au cas Q3.
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Similaire au cas Q2.
Certificat d'OCSP	Datasure ne générant des certificats d'OCSP que pour son propre usage, la délivrance du certificat est encadrée par une procédure interne
Certificat d'AC	La délivrance du certificat est réalisée durant la cérémonie des clés.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

L'acceptation du certificat est réalisée de façon explicite ou im^plicite.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	L'acceptation du certificat se fait sous forme électronique avant sa génération. Les données contenues dans le certificat à générer sont présentées au porteur qui accepte celui-ci à l'aide d'une case à cocher et d'un bouton « accepter ». Le porteur dispose de 15 jours pour accepter son certificat après la vérification effective de son identité.
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	Le certificat étant éphémère, l'acceptation se fait explicitement après la vérification de l'identité et la génération du certificat et avant de générer la signature. Les données du certificat sont présentées au porteur qui, à l'aide d'une case à cocher, en accepte le contenu. L'acceptation du certificat doit se faire au maximum une heure après la fin du processus PVID.
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Les modalités sont similaires au cas Q1.
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les modalités sont similaires au cas Q1.
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les modalités sont similaires au cas Q1.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Les modalités sont similaires au cas Q1.
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Datasure ne générant des certificats d'horodatage que pour son propre usage, l'acceptation du certificat est encadrée par une procédure interne
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	Les modalités sont similaires au cas Q2.
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Les modalités sont similaires au cas Q1.
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Les modalités sont similaires au cas Q2.
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Les modalités sont similaires au cas Q1.
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Les modalités sont similaires au cas Q2.

Certificat d'OCSP	Datasure ne générant des certificats d'OCSP que pour son propre usage, l'acceptation du certificat est encadrée par une procédure interne
Certificat d'AC	L'acceptation du certificat est réalisée durant la cérémonie des clés.

Le processus d'acceptation du certificat est précisé au porteur dans les CGUs [OVR-6.3.4-01]

Le processus complet de signature est limité dans le temps [REG-6.3.1-00D]

- Un délai de 15 jours est mis en place entre la finalisation du PVID et l'acceptation explicite du certificat pour les certificats permanents
- Une délai de 1 heure est mis en place entre la finalisation du PVID et l'acceptation explicite du certificat pour les certificats éphémères.

4.4.2 Publication du certificat

Le certificat ne fait pas l'objet d'une publication [DIS-6.1-01B/DIS-6.1-01C]

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

L'ensemble des échanges sont réalisés au travers d'appel API.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la fonction de sécurité concernée.
Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.
L'usage autorisé de la bi-clé du porteur et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.
Cet usage est également clairement explicité dans ce chapitre de la présente PC/DPC de l'AC, ainsi que dans les conditions générales d'utilisation et/ou le contrat porteur. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du porteur ou du MC par l'AC avant d'entrer en relation contractuelle.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	La clé privée associée au certificat permet de créer des signatures électroniques qualifiées. Dans le cas 2 (QSCD à distance), Datasure vérifie que le certificat est valide avant utilisation de la clé privée [SIG-6.3.1-08] et s'assure qu'elle n'est utilisée que dans des
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	

	processus où le consentement à signer ait été obtenu au préalable [SIG-6.3.1-09]
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	La clé privée associée au certificat permet de créer des signatures électroniques avancées s'appuyant sur des certificats qualifiées.
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	La clé privée associée au certificat permet de créer des cachets électroniques qualifiés. Datasure vérifie que le certificat est valide avant utilisation de la clé privée[SIG-6.3.1-08] et s'assure qu'elle n'est utilisée que dans des processus où le consentement à sceller ait été obtenu au préalable [SIG-6.3.1-09]
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	La clé privée associée au certificat permet de créer des cachets électroniques qualifiés.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	La clé privée associée au certificat permet de créer des cachets électroniques avancés s'appuyant sur un certificat qualifié
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	La clé privée associée au certificat permet à l'AH de créer des jetons d'horodatage.
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	La clé privée associée au certificat permet de créer des signatures électroniques avancées. Datasure vérifie que le certificat est valide avant utilisation de la clé privée[SIG-6.3.1-08] et s'assure qu'elle n'est utilisée que dans des processus où le consentement à signer ait été obtenu au préalable [SIG-6.3.1-09]
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	La clé privée associée au certificat permet à une application de s'authentifier.
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	La clé privée associée au certificat permet de créer des signatures électroniques avancées. Datasure vérifie que le certificat est valide avant utilisation de la clé privée[SIG-6.3.1-08] et s'assure qu'elle n'est utilisée que dans des processus où le consentement à signer ait été obtenu au préalable [SIG-6.3.1-09]
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	La clé privée associée au certificat permet de créer des cachets électroniques avancés.
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	La clé privée associée au certificat permet de créer des signatures avancées. Datasure vérifie que le certificat est valide avant utilisation de la clé privée[SIG-6.3.1-08] et s'assure qu'elle n'est utilisée que

	dans des processus où le consentement à signer ait été obtenu au préalable [SIG-6.3.1-09]
Certificat d'OCSP	La clé privée associée au certificat permet de signer des jetons OCSP.
Certificat d'AC	La clé privée associée au certificat permet de signer les certificats des utilisateurs finaux, des OCSP et les CRL.
Certificat de l'AC Racine	La clé privée associée au certificat permet de signer les certificats d'AC, le certificat Racine et les ARL.

4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	La clé publique du certificat permet de vérifier la signature électronique ou le cachet électronique.
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	La clé publique du certificat permet d'authentifier le client.
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Voir cas Q1
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	
Certificat d'OCSP	La clé publique associée au certificat permet de vérifier les jetons OCSP

Certificat d'AC	La clé publique associée au certificat permet de de vérifier les certificats des utilisateurs finaux, des OCSP et les CRL
Certificat de l'AC Racine	La clé publique associée au certificat permet de vérifier les certificats d'AC et les ARL

4.6 Renouvellement d'un certificat

Conformément au [RFC3647], la notion de "renouvellement de certificat" correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique du porteur).
Dans la cadre de la présente PC/DPC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. L'AC Darasure garantit qu'un certificat correspondant à une bi-clé existante ne peut pas être renouvelé au sens du [RFC3647].

4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat au porteur liée à la génération d'une nouvelle bi-clé.

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés sont périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi, les bi-clés des porteurs, et les certificats correspondants, seront renouvelés minimum à une fréquence conforme RGS.
Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du porteur.

4.7.2 Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat est à l'initiative du porteur.

4.7.3 Procédure de traitement d'une demande d'un nouveau certificat

Les modalités de renouvellement sont identiques aux modalités de demande initiale [REG-6.2.3-01]. Voir chapitre 4.3.1.

4.7.4 Notification au porteur de l'établissement du nouveau certificat

Voir chapitre 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

Voir chapitre 4.4.1.

4.7.6 Publication du nouveau certificat

Voir chapitre 4.4.2.

4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Voir chapitre 4.4.3.

4.8 Modification du certificat

La modification de certificat n'est pas possible dans le cadre de cette PC/DPC.

4.9 Révocation et suspension des certificats

La présente section documente les procédures de révocation de certificats de porteur et d'AC [REV-6.2.4-01]. Datasure révoque sans délai tout certificat suite à une demande authentifiée et validée [REV-6.3.9-01]. Il est à noter que Datasure ne permet à l'utilisateur de révoquer son certificat si celui-ci est un certificat éphémère [REV-6.3.9-15/REV-6.3.9-16].
Les certificats pour lesquels la révocation n'est pas possible sont les suivants :

Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	La révocation n'est pas disponible
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	

Pour les certificats éphémères ne pouvant être révoqués, le signataire, ou tout utilisateur peut, en cas de problème avec le certificat, réaliser une réclamation en contactant Datasure au point de contact indiqué dans la présente PC/DPC, et demander des informations sur les conditions d'émissions de certificats [REV-6.3.9-17]/[REV-6.3.9-19]. Datasure enregistrera et conservera toute les réclamations et éléments associés [REV-6.3.9-18] jusqu'à la fin de vie de l'AC. Datasure diligentera une enquête interne pour établir l'éventuelle réalité d'une fraude. L'ensemble des éléments, y compris la demande, seront horodatés avec un horodatage qualifié afin d'assurer l'intégrité des données et de constituer une éventuelle preuve en justice.

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats de porteurs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur :

- le porteur ou une entité autorisée (représentant légal de l'entité ou MC par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur et/ou de son support) [REV-6.3.9-01];
- en cas de modification majeur de la présente PC/DPC, entraînant une non-conformité du certificat avec les exigences de la PC/DPC [REV-6.3.9-02]
- si l'AC apprend des faits qui entraînent l'invalidité du certificat tel que [REV-6.3.9-02] :

- le décès du porteur ou la cessation d'activité de l'entité du porteur ;
- les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple changement du nom de famille suite à un mariage), ceci avant l'expiration normale du certificat ;
- le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le porteur et/ou, le cas échéant, le MC / l'entité n'ont pas respecté leurs obligations découlant de la présent PC/DPC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ;
- la clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné est révoqué

4.9.1.2 Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats, de LCR et/ou de réponses OCSP) :

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant la composante.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats de porteurs

Les personnes / entités qui peuvent demander la révocation d'un certificat de porteur sont les suivantes.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	le porteur au nom duquel le certificat a été émis ; l'AC émettrice du certificat ou l'une de ses composantes (AE) Dans le cas du rattachement à une personne morale, le responsable légal et le cas échéant le MC, peut également demander la révocation.
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Le responsable de certificat Le responsable légal L'AC émettrice du certificat ou l'une de ses composantes (AE)
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	

Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Le responsable de certificat Le responsable de l'AH L'AC émettrice du certificat ou l'une de ses composantes (AE)
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Voir cas Q4
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Voir cas Q4
Certificat d'OCSP	Voir section suivante
Certificat d'AC	Voir section suivante

Le porteur est informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat dans les CGUs.

4.9.2.2 Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.
La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat de porteur

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre 3.4.

Datasure ne propose pas de mécanisme de révocation à une date programmée dans le future [REV-6.2.4-05A].

Les informations suivantes figurent dans la demande de révocation de certificat :

- l'identité du porteur du certificat utilisée dans le certificat (nom, prénom, ...) ;
- le nom du demandeur de la révocation ;
- toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série,...) ;
- optionnellement, la cause de révocation (celle-ci n'est pas publiée dans la CRL).

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.
L'information de révocation est diffusée selon les solutions suivantes [CSS-6.3.10-03] :

- via une LCR signée par l'AC elle-même;
- via un service OCSP dont la réponse est signée par un certificat de répondeur OCSP lui-même signé par l'AC ayant émis le certificat à révoquer (cf. chapitre 4.9.9).

Les deux services sont disponibles sur Internet [CSS-6.3.10-10].
Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du certificat [REV-6.3.9-03]. Le processus de révocation est définitif [REV-6.3.9-04]
L'opération est enregistrée dans les journaux d'évènements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat.

Le délai maximum entre une demande de révocation et la révocation effective du certificat est de 24h [REV-6.2.4-03A]. Si la confirmation de la demande (voir 3.4) n'est pas réalisée dans les 24h, le statut de révocation restera inchangé [REV-6.2.4-03B]. Cependant, Datasure propose des mécanismes permettant de révoquer dans un délai plus rapide (voir 3.4) [REV-6.2.4-06A] et permettant de traiter les demandes de révocation dès leur dépôt [REV-6.2.4-08].

Datasure mettant en œuvre l'OSCP et la CRL, il est possible qu'un statut différent soit temporairement renvoyé par les deux méthodes [REV-6.2.4-03C].
Les composantes du services de révocation sont synchronisées avec le temps UTC, comme l'ensemble des services en ligne [REV-6.2.4-07]

Le statut de révocation est systématiquement conservé, même en cas d'expiration du certificat [CSS-6.3.10-04].

4.9.3.2 Révocation d'un certificat d'une composante de l'IGC

L'AC Datasure précise dans sa DPC confidentielle les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.
En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides.
L'ANSSI est immédiatement informée en cas de révocation d'un des certificats de la chaîne de certification.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Dès que le porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

4.9.5 Délai de traitement par l'AC d'une demande de révocation

4.9.5.1 Révocation d'un certificat de porteur

Par nature, une demande de révocation doit être traitée en urgence.

4.9.5.2 Disponibilité du système de traitement des demandes de révocation

La fonction de gestion des révocations doit être disponible 24h/24 et 7J/7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) d'une heure.
Cette fonction a une durée maximale totale d'indisponibilité par mois de 4h.

Toute demande de révocation d'un certificat porteur est traitée dans un délai inférieur à 24h. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

4.9.5.3 Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.
La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR ou de réponses OCSP) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Pour cela, Data sure met à disposition une CRL et un répondeur OCSP [CSS—12-01]. La méthode utilisée (LCR ou OCSP) est laissée à l'appréciation de l'utilisateur.

4.9.7 Fréquence d'établissement et durée de validité des LCR

Lorsque l'information sur l'état de la révocation d'un certificat est assurée au travers de la mise en place d'un service de LCR la fréquence minimale de leur publication est de 24h [CSS-6.3.9-05]. Les LCR dont directement signées par l'AC [CSS-6.3.9-08]
Afin d'assurer une continuité du service dans le cas où un incident sur la publication des LCR survient, la durée de validité des LCR est de 48h [CSS-6.3.9-07]. Les LAR émises par l'AC racine ont une durée de vie d'un an. [CSS-6.3.9-12] La fréquence de publication de nouvelles LAR est cohérente avec la durée de ces LAR et est fixée à 2 par an, ce qui correspond à une publication tous les 6 mois [CSS-6.3.9-12].

4.9.8 Délai maximum de publication d'une LCR

Lorsque l'information sur l'état de la révocation d'un certificat est assurée au travers de la mise en place d'un service de publication de LCR, celles-ci sont publiées et disponibles pour le téléchargement au maximum dans les 30 minutes suivant leur génération.
Le délai entre 2 publications de LAR ne peut dépasser 8 mois. En cas de révocation d'une AC, la publication est immédiate [CSS-6.3.9-13].

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Les dispositifs de vérification de l'état des certificats (CRL et OCSP] sont disponibles 24h/24 et 7J/7 et sont chacun encadrées par un SLA de 99,5% mensuels [CSS-6.3.10-02].

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

L'intégrité et l'authenticité du statut est permise par la signature du jeton OCSP et de la CRL [CSS-6.3.10-03].

4.9.11 Autres moyens disponibles d'information sur les révocations

Non applicable.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de porteur, les entités autorisées à effectuer une demande de révocation sont tenues de le faire sans délais après avoir eu connaissance de la compromission de la clé privée.
Pour les certificats d'AC, outre les exigences du chapitre 4.9.3.2 ci-dessus, la révocation suite à une compromission de la clé privée fait l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).
L'AC impose, au travers des CGUs, au porteur ou au MC qu'en cas de compromission de la clé privée du porteur ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le porteur s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

4.9.13 Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC/DPC.

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

L'AC fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine), c'est-à-dire de vérifier également les signatures des

certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR ou des jetons OCSP et l'état du certificat de l'AC Racine
La fonction d'information sur l'état des certificats est mis à la disposition des utilisateurs de certificats au travers de LCR et OCSP.
Le service de LCR / LAR proposé est au format V2.
Le service OCSP s'appuie sur les données de révocation incluses en base de données et non sur la dernière CRL publiée, de ce fait, le délai entre la révocation effective et le changement de statut du jeton OCSP est quasi immédiat, permettant d'obtenir le statut d'un certificat en temps réel. De ce fait, un statut différent peut être renvoyé temporairement par l'OCSP et la CRL jusqu'à la publication de la prochaine CRL. Cet état temporaire peut-être de 24h au maximum [CSS-6.3.10-9A]

4.10.2 Disponibilité de la fonction d'information sur l'état des certificats

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7.
Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h.
Cette fonction doit avoir une durée maximale totale d'indisponibilité par mois de 8 heures.
Lors de la vérification en ligne du statut d'un certificat (OCSP), le temps de réponse du serveur à la requête reçue est au maximum de 10 secondes.

4.10.3 Dispositifs optionnels

Non applicable.

4.11 Fin de la relation entre le porteur et l'AC

En cas de fin de relation contractuelle entre l'AC et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

4.12 Séquestre de clé et recouvrement

Il n'est pas réalisé de séquestre de clé.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

Datasure met en œuvre des mesures de sécurité physique afin de protéger ces services de confiance [OVR-6.4.2-07], en particulier les services de génération de certificats et de révocation [OVR-6.4.2-02].

L'AC Racine est opérée dans un environnement spécifique présentant le plus haut niveau de sécurité [OVR-6.4.2-11].

5.1.1 Situation géographique et construction des sites

La construction des sites doit respecter les règlements et normes en vigueur

5.1.2 Accès physique

Datasure contrôle les accès physiques aux composants de l'AC dont la sécurité est critique pour la fourniture du service afin de minimiser les risques liés à la sécurité physique [REQ-7.6-01]. En particulier, un périmètre clair est défini autour des services sensibles, en particuliers les services de génération et révocation de certificats [OVR-6.4.2-05]. Ce périmètre ne peut pas être partagé avec d'autres organisations [OVR-6.4.2-06]

L'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée (entrée et sortie) [REQ-7.6-02/OVR-6.4.2-04]. Les personnels non-autorisés sont accompagnés en permanence par des personnels autorisés [OVR-6.4.2-03]

En dehors des heures ouvrables, la sécurité est renforcée par la mise en oeuvre de moyens de détection d'intrusion physique et logique.
Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines [REQ-7.6-03]. Pour cela, les composantes concernées de l'IGC définissent un périmètre de sécurité physique où sont installées ces machines. La mise en oeuvre de ce périmètre permet de respecter la séparation des rôles de confiance telle que prévue dans la présente PC/DPC. Notamment, tout local utilisé en commun avec d'autres fonctions que les fonctions rendues par la composante concernée soit en dehors du périmètre de sécurité.
Les composants critiques pour l'opération sécurisée du service de confiance sont localisés dans un environnement de sécurité muni d'une protection physique contre les intrusions et de mécanismes d'alarme [REQ-7.6-05]
Des mesures sont mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services de l'AC soient sortis du site sans autorisation [REQ-7.6-04].

Des contrôles d'accès sont appliqués aux d'AC pour remplir les exigences de sécurité attendues. Les contraintes sur l'environnement d'exploitation, identifiées dans la documentation liée à la certification du module (Profil de Protection, cible de sécurité), sont remplies.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs. Elles permettent également de respecter les exigences des PC Type RGS, des exigences de l'ETSI EN319401 ainsi que les engagements pris par l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4 Exposition aux dégâts des eaux

Datasure s'assure que les moyens de protection contre les dégâts des eaux permettent de respecter les exigences des PC Type RGS, des exigences de l'ETSI EN319401 ainsi que les engagements pris par l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5 Prévention et protection incendie

Datasure s'assure que les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences des PC Type RGS, des exigences de l'ETSI EN319401 ainsi que les engagements pris par l'AC dans la présente PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.6 Conservation des supports

Datasure assure un niveau de protection des biens approprié. Cela inclut les biens matériels mais également les biens immatériels et informations [REQ-7.3.1-01]
Les différentes informations intervenant dans les activités de l'IGC sont identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité) en ligne avec les résultats de l'analyse de risque. L'AC maintient un inventaire de ces informations [REQ-7.3.1-02]. L'AC met en place des mesures pour éviter la compromission et le vol de ces informations [. En particulier, tous les supports sont gérés de façon sécurisée en ligne avec les exigences de classification de l'information [
Les supports (papier, disque dur, supports amovibles, etc.) correspondant à ces informations sont gérées selon des procédures conformes à ces besoins de sécurité REQ-7.3.2-01]

En particulier, ils doivent être manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.
Des procédures de gestion protègent ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent [REQ-7.3.2-02].

5.1.7 Mise hors service des supports

En fin de vie, les supports devront être, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes [REQ-7.3.2-01]
Les procédures et moyens de destruction et de réinitialisation sont conformes à ce niveau de confidentialité visé.

Ces mesures de fin de vie permettent de protéger les données sensibles contre le risque de divulgation lors de la ré-utilisation de leur support [REQ-7.4-10/OVR-6.4.2-09]

5.1.8 Sauvegarde hors site

En complément de sauvegardes sur sites, les composantes de l'IGC mettent en oeuvre des sauvegardes hors sites de leurs applications et de leurs informations.

Ces sauvegardes sont organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conforme aux exigences des PC Type RGS, des normes ETSI EN 319401, 319411-1 et 319411-2 ainsi qu'aux engagements de l'AC dans la présent PC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats (cf. chapitres 4.9.5.1 et 4.10.2).
Les informations sauvegardées hors site respectent les exigences de Les informations sauvegardées hors site doivent respecter les exigences de la présente PC Type en matière de protection en confidentialité et en intégrité de ces informations.

En particulier, les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, mettent en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.).
Les fonctions de sauvegarde et de restauration sont effectuées par les rôles de confiance appropriés et conformément aux mesures de sécurité procédurales.

5.2 Mesures de sécurité procédurales

Datasure s'assure que ces employés et sous-traitant participent pleinement à la sécurité des opérations [REQ-7.2-01].

5.2.1 Rôles de confiance

Les rôles de sécurité et les responsabilités sont documentés dans des descriptions de poste. Les rôles de confiance, sur lesquels la sécurité du fonctionnement de l'Autorité de certification repose, sont clairement identifiés au travers de fiches de poste mise à disposition des personnels [REQ-7.2-06/ REQ-7.2-07] [119431-1/ OVR-6.5.1-01]
Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes [REQ-7.2-15] :

- les officiers/responsables chargés de la sécurité : responsabilité complète d'administrer la mise en œuvre des pratiques de sécurité ; Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité d'une ou plusieurs composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux d'évènements. Il est responsable des opérations de génération et de révocation des certificats.

- les administrateurs système : autorisés à installer, configurer et maintenir les modules de l'Autorité de certification ; Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante
- les opérateurs système : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation au quotidien des applications pour les fonctions mises en œuvre par la composante. L'opérateur système est responsable du fonctionnement les modules de l'Autorité de certification de manière quotidienne. Il est autorisé pour effectuer les opérations de sauvegarde et des secours ;
- Opérateur d'enregistrement (comprenant le rôle de spécialiste de la validation) et de révocation [OVR-6.4.4-02]: il sont responsable de la vérification des demandes de certificats et de révocation.
- Porteur de secret : les porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés
- les auditeurs de système/contrôleur : autorisés à consulter les archives et les fichiers d'audit des modules de l'autorité de certification. Personne autorisée à accéder et en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

Le personnel de l'Autorité de certification doit être formellement nommé aux rôles de confiance par la direction responsable de la sécurité [REQ-7.2-16A]. La personne nommée en rôle de confiance accepte également formellement son rôle et ses responsabilités [REQ-7.2-16B].
Des procédures sont établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de services de certification [REQ-7.7-08].
Les rôles sont décrits et définis dans la description des postes propre à chaque entité opérant une des composantes de l'IGC sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles déterminent la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés [REQ-7.2-10].

De plus, les opérations de sécurité de l'AC doivent être séparées des opérations normales [REQ-7.2-11].
Les responsabilités des opérations de sécurité incluent :

- les procédures et responsabilités opérationnelles ;
- la planification et la validation des systèmes sécurisés ;
- la protection contre les logiciels malicieux ;
- l'entretien ;
- la gestion de réseaux ;
- la surveillance active des journaux d'audit, l'analyse des évènements et les suites ;
- la manipulation et la sécurité des supports ;
- l'échange de données et de logiciels.

5.2.2 Nombre de personnes requises par tâche

La DPC confidentielle de l'AC précise quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter.

5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC vérifie l'identité et les autorisations de tous membres de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

Ces contrôles sont décrits dans la DPC Confidentielle de l'AC et sont conformes à la politique de sécurité de la composante.
Chaque attribution d'un rôle à un membre du personnel de l'IGC est notifiée par écrit. Ce rôle est clairement mentionné et décrit dans sa fiche de poste.

5.2.4 Rôles exigeant une séparation des attributions

Des descriptions de fonctions sont définies pour le personnel de l'Autorité de Certification (aussi bien provisoire que permanent) du point de vue de la séparation des responsabilités et du principe du privilège minimum, selon la sensibilité de la fonction sur la base des responsabilités et des niveaux d'accès.
Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre
En particulier, les rôles pouvant présenter des conflits d'intérêts ainsi que les aires de responsabilité doivent faire l'objet, chaque fois que cela est possible, d'une séparation des rôles pour réduire les opportunités d'atteinte, volontaire ou non, à l'intégrité du SI ou d'une mauvaise utilisation des biens [REQ-7.1.2-01/ REQ-7.2-14].

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur / contrôleur ;
- ingénieur système, opérateur et contrôleur.

5.3 Mesures de sécurité vis à vis du personnel

5.3.1 Qualifications, compétences, et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité vis-à-vis de leur employeur.

Chaque entité opérant une composante de l'IGC s'assure que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

L'autorité de certification emploie un personnel qui possède l'expertise, la formation, l'expérience et les qualifications nécessaires pour les services offerts, tels que l'exige la fonction. En particulier, le personnel a réalisé des formations sur la sécurité informatique et la protection des données à caractère personnel en ligne avec la spécificité d'un service d'autorité de certification et les fonctions occupées au sein de ce service.
Le personnel est en nombre suffisant pour assurer le volume de travail nécessaire pour la fourniture du service [REQ-7.2-02].
L'expertise des employés est acquise au travers de l'expérience, de formations spécifiques ou d'une combinaison des deux [REQ-7.2-03].

Le personnel de gestion employé doit posséder :

- la connaissance de la technologie de PKI et ;
- la connaissance de technologie de la signature numérique et ;
- pour le personnel avec des responsabilités de sécurité, une bonne connaissance des procédures de sécurité, et ;
- l'expérience avec la sécurité de l'information et l'évaluation des risques.

Le personnel d'encadrement possède également, au travers de son expérience ou d'une formation relative au service de confiance eIDAS, en particulier aux services d'émission de certificat, une familiarité avec les procédures de sécurité applicable à son personnel. Il doit également être familier des procédures de sécurité ainsi que des notions relatives aux responsabilités en matière de sécurité et disposer d'une expérience en sécurité de l'information et en analyse de risque suffisante pour être en mesure d'assurer la fonction d'encadrement [REQ-7.2-12/REQ-7.2-13].

L'AC informe toute personne intervenant dans des rôles de confiance de l'IGC :

- de ses responsabilités relatives aux services de l'IGC,
- des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

En particulier, les personnes intervenant dans des rôles de confiance doivent y être formellement affectées par l'encadrement supérieur chargé de la sécurité.

5.3.2 Procédures de vérification des antécédents

L'AC Datasure met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté de ses personnels.
L'AC Datasure ne nomme pas aux rôles de confiance ou de gestion toute personne connue pour avoir une condamnation pour un crime sérieux ou une autre infraction au bulletin n°3 du casier judiciaire qui

affecte son adéquation avec la position. Le personnel n'a pas accès aux fonctions de confiance avant que les contrôles nécessaires ne soient achevés [REQ-7.2-17]
Le contrôle inclut une vérification de l'extrait de casier judiciaire (bulletin n°3).
Datasure peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions.
Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

5.3.3 Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.
L'AC Datasure s'assure que les personnels ont la connaissance nécessaire et comprennent les implications des opérations dont ils ont la responsabilité.

5.3.4 Exigences en matière de formation continue et fréquences des formations

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation ou tout autre domaine pertinent en fonction de la nature de ces évolutions
La formation continue des employés inclut une mise à niveau, a minima annuelle, de la connaissance des nouvelles menaces et pratiques de sécurité [REQ-7.2-04].

5.3.5 Fréquence et séquence de rotations entre différentes attributions

Sans objet

5.3.6 Sanctions en cas d'actions non autorisées

Des sanctions disciplinaires sont prévues en cas de non-respect des consignes énoncées dans la présente PC/DPC, la DPC confidentielle ou dans la PSSI [REQ-7.2-05].

5.3.7 Exigences vis à vis du personnel des prestataires externes

Les exigences vis-à-vis du personnel des prestataires externes sont similaire à celle des employés de Datasure. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8 Documentation fournie au personnel

Chaque personnel dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, il doit lui être remis la ou les politique(s) de sécurité l'impactant.

5.4 Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer de façon manuelle ou automatique. Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.
Datasure conserve et garde accessible, pour une période appropriée, y compris en cas de cessation d'activité, toutes les données pertinentes créées et reçues par le service, en particulier à des fins de preuve légales mais également afin d'assurer la continuité du service [REQ-7.10-01].
Datasure étant soumis au RGPD, la constitution des données d'audit est conforme à la Réglementation Française et Européenne en matière de gestion des données à caractère personnel [119431-2/ OVR-7.10-05]

5.4.1 Type d'événement à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en oeuvre dans le cadre de l'IGC, chaque entité opérant une composante de l'IGC journalise les évènements tels que décrits ci-dessous, sous forme électronique. La journalisation est automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements sont recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration des systèmes ;
- les changements apportés au personnel ;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment :
réception d'une demande de certificat (initiale et renouvellement) ;

- validation / rejet d'une demande de certificat ;
- évènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des 20 clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;

- le cas échéant, génération des éléments secrets du porteur (bi-clé, codes d'activation,…) ;
- génération des certificats des porteurs ;
- transmission des certificats aux porteurs et, selon les cas, acceptations / rejets explicites par les porteurs ;
- le cas échéant, remise de son dispositif de protection des éléments secrets au porteur ;
- publication et mise à jour des informations liées à l'AC (PC/DPC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- réception d'une demande de révocation ;
- validation / rejet d'une demande de révocation ;
- génération puis publication des LCR ou des, requêtes / réponses OCSP.

Chaque enregistrement d'un évènement dans un journal doit contenir au minimum les champs suivants [119431-2/ OVR-7.10-06] :

- type de l'évènement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC ou du service de signature concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) [119431-2/ OVR-7.10-03/ OVR-6.4.5-05]. ;
- résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'évènement ;
- toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Concernant les fonctions de signature à distance,

- les opérations relatives à la création de signature font l'objet d'un enregistrement et sont liés aux données d'identification ou d'authentification du signataire ou du service apposant le cachet [119431-2/ OVR-7.10-02]. En particulier [119431-1/ OVR-6.4.5-03] :
  - les événements de signature d'un utilisateur
  - l'authentification dans le cadre du protocole du QSCD
  - les événements relatifs à la gestion des SAD
- La durée de présentation du document au signataire personne physique [119431-2/ ASI-8.1-11].

- La date de téléchargement du document par le signataire, si celui-ci est téléchargé [119431-2/ ASI-8.1-12].
- Tout changement important de l'environnement du QSCD [119431-1/ OVR-6.4.5-03]

Les opérations de journalisation sont effectuées au cours du processus.
En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'évènement.
Les évènements et données spécifiques à journaliser sont documentés par l'AC.

En cas d'incapacité à générer des traces, *a minima* une alerte est levée/ [119431-1/ OVR-6.4.5-04] :

5.4.2 Fréquence de traitement des journaux d'événements

Cf. chapitre §5.4.8 ci-dessous

5.4.3 Période de conservation des journaux d'événements

Les journaux d'événements sont conservés pour une durée appropriées afin de permettre la fourniture, le cas échéant, d'éléments de preuve juridique. La durée de conservation est notifiée dans les CGUs.
Les journaux d'évènements sont conservés pour la durée prévues aux CGU [119431-2/ OVR-7.10-04]. .

5.4.4 Protection des journaux d'événements

Datasure assure la confidentialité et l'intégrité des données d'audit concernant les opérations du service [REQ-7.10-02] Cette intégrité doit pouvoir être vérifiée [119431-1/ OVR-6.4.5-03]
Les événements sont générés de façon à ce qu'ils ne puissent pas être altérés ou générés facilement durant leur période de conservation [REQ-7.10-08]

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements [RGS]. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux [RGS]. Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).
Le système de datation des évènements doit respecter les exigences du chapitre 6.8.
La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.5 Procédure de sauvegarde des journaux d'événements

Chaque entité opérant une composante de l'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée,

conformément aux exigences des PC Type RGS, des normes ETSI EN 319401, ETSI EN 319411-1 et ETSI EN 319411-2.

5.4.6 Système de collecte des journaux d'événements

5.4.7 Notification de l'enregistrement d'un événement au responsable de l'événement

Sans objet

5.4.8 Evaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC doit être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

5.5 Archivage des données

La présente section précise les données archivées [119431-2/OVR-7.10-04].
Datasure étant soumis au RGPD, la constitution des données d'audit est conforme à la Réglementation Française et Européenne en matière de gestion des données à caractère personnel [119431-2/ OVR-7.10-05]

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage doivent également être prises par l'AC. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.
Les journaux concernant les opérations sont archivés de façon complète et confidentielle conformément aux disposition de la politique d'archivage [REQ-7.10-03]

Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.
Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les conditions générales d'utilisation ;
- les accords contractuels avec d'autres AC ;
- les certificats, LCR ou réponses OCSP tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les engagements signés des MC ;
- les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement ;
- les journaux d'évènements des différentes entités de l'IGC et du service de signature, en particulier :

- les dossiers d'enregistrement de l'AC
- les dossiers de preuve du service de signature et de gestion du QSCD

5.5.2 Période de conservation des archives

5.5.2.1 Dossier d'enregistrement

Tout dossier de demande de certificat accepté doit être archivé aussi longtemps que nécessaire, et pendant au moins sept (7) ans après l'expiration du certificat, pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.
La durée de conservation des dossiers d'enregistrement est portée à la connaissance du porteur ou du MC au travers de CGUs [REQ-7.10-07].
Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat sera présenté par l'AC lors de toute sollicitation par les autorités habilitées.
Ce dossier, complété par les mentions consignées par l'AE ou le MC, permet de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

5.5.2.2 Dossier de preuve

Le dossier de preuve est conservé dans des conditions similaires au dossier d'enregistrement

5.5.2.3 Certificats, LCR et réponses OCSP émis par l'AC

Les certificats de clés de porteurs et d'AC, ainsi que les LCR / LAR produites, sont archivés pendant au moins sept (7) années après leur expiration[4].
Les réponses OCSP produites sont archivées pendant au moins trois mois après leur expiration

5.5.2.4 Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 sont archivés pendant sept (7) années après leur génération. Les moyens mis en oeuvre par l'AC pour leur archivage offre le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être assurée tout au long de leur cycle de vie

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, sont :

- protégées en intégrité ;
- accessibles aux personnes autorisées ;
- lisibles et exploitables.

[4] 5 au titre du RGS.

L'AC précise dans sa DPC confidentielle les moyens mis en oeuvre pour archiver les pièces en toute sécurité.

5.5.4 Procédure de sauvegarde des archives

Afin d'assurer leur disponibilité, Datasure met en place des procédures de redondances de ces archives. Ces mesures sont décrites en détail dans la DPC confidentielle.
Le niveau de protection des sauvegardes est au moins équivalent au niveau de protection des archives.

5.5.5 Exigences d'horodatage des données

L'heure précise des événements, en particulier relatif à l'environnement du service, de la gestion des clés et de la synchronisation des horloges sont enregistrés [REQ-7.10-05] [119431-1/ OVR-6.4.5-07]
Cf. chapitre 5.4.4 pour la datation des journaux d'évènements.
Le chapitre 6.8 précise les exigences en matière de datation / horodatage

5.5.6 Système de collecte des archives

Le système de collecte des archives respecte les exigences de protection des archives

5.5.7 Procédures de récupération et de vérification des archives

Les enregistrements concernant les opérations du services seront rendu disponible en cas de besoin de fournir des éléments de preuve leur bonne mise en œuvre, en particulier en cas de besoin juridique [REQ-7.10-04]

Les archives (papier et électroniques) peuvent être récupérées dans un délai inférieur à deux (2) jours ouvrés [RGS].

5.6 Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC est supérieure à celle des certificats qu'elle signe.

Au regard de la date de fin de validité de ce certificat, son renouvellement est demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.
Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.
Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 Reprise suite à compromission et sinistre

5.7.1 Capacités de continuité d'activité suite à un sinistre

Datasure a défini un plan de continuité d'activité et de reprise d'activité en cas de sinistre [REQ-7.11-01]

Les différentes composantes de l'IGC et du service de signature/gestion du QSCD à distance disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences des exigences de l'ETSI 319401, 319411-1 et 319411-2, 119432-1 et 119432-2 [119431-2/ OVR-7.11-01] ainsi que de la présente PC/DPC.
En particulier, afin d'assurer la disponibilité du service, les accès réseaux sont redondés afin de permettre la disponibilité du service en cas de panne [REQ-7.8-12]. De même, le service de gestion du QSCD s'appuie sur a minima deux sites distants [119431-2/ OVR-7.11-02]. Le niveau de disponibilité contractuel du service de signature précisé dans les CGUs tient compte de l'architecture sous-jacente, mais également des dépendances des autres services, en particulier de la disponibilité de l'AC, des services de vérification d'identité et de l'AH [119432-2/OVR-7.11-03].

5.7.2 Procédures de remontée et de traitement des incidents et des compromissions

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

5.7.2.1 Surveillance du système, alerte et incidents

L'activité des différents systèmes mis en œuvre fait l'objet d'une surveillance, en particulier, l'utilisation et les requêtes vers les services sont surveillées [REQ-7.9-01].
Les activités de surveillance prennent en compte la sensitivité des données collectées et analysés [REQ-7.9-02].
La surveillance a pour but la détection de toute activité jugée anormale et indiquant un potentiel incident de sécurité, y compris une intrusion réseau. En cas de détection, une alarme est levée [REQ-7.9-03].
Les éléments suivants font l'objet d'une surveillance [REQ-7.9-04] :

- Le démarrage ou la désactivation des fonctions de génération des traces d'audit,
- La disponibilité et l'utilisation du service, en particulier le réseau.

La surveillance doit inclure la surveillance des traces d'audit ou leur revue régulière afin d'identifier l'existence d'activité malicieuses en mettant en œuvre des mécanismes automatique d'analyse des traces et de génération d'alertes en cas d'événements de sécurité critique [REQ-7.9-09]. Les mécanismes de revue sont réalisés sur une base journalière (vérification continue) [119431-2/OVR-7.10-04].

En cas d'incident, Datasure réagit sans délai et de façon coordonnée afin de mettre en œuvre une réponse rapide à l'incident et à limiter l'impact d'une éventuelle faille de sécurité [REQ-7.9-05]
Le suivi des alertes relatives aux potentiels événements de sécurité critiques est pris en charge par des personnels en rôle de confiance. Ces personnels s'assure que les incidents associés sont biens traités conformément aux procédures [REQ-7.9-06].

Les mesures de remontées et de réponse aux incidents sont mises en œuvre de façon à limiter les impacts et dysfonctionnements [REQ-7.9-12].

5.7.2.2 Incident majeur

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur est impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …).

En particulier, Datasure a établi une procédure de gestion des incidents majeurs qui inclut une notification de l'ANSSI dans les 24h en cas de d'incident de sécurité ou de perte d'intégrité ayant un impact significatif sur le service fourni. En cas d'incident relatif aux données à caractère personnel, une notification à la CNIL sera réalisée [REQ-7.9-07]. Si l'incident impacte un porteur de certificat, personne physique ou morale, elle sera également notifiée sans délai [REQ-7.9-08]
En cas de désastre majeur, incluant la compromission d'une clé de signature ou de moyen d'authentification du service, les opérations seront restaurées dans le délai fixé dans le plan de continuité et de reprise d'activité, après avoir, le cas échéant, résolu la cause du désastre par des mesures de correction appropriées [REQ-7.11-01]

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors l'AC doit :

- informer tous les porteurs et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou a d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- révoquer tout certificat concerné

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

Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant des PC Type RGS, des exigences de l'ETSI 319401, 319411-1 et 319411-2 ainsi que de la présente PC/DPC, notamment en ce qui concerne les fonctions liées à la publication et liées à la révocation des certificats.
Ce plan est testé a minima une fois par an.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante en tant que sinistre Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué : cf. chapitre §4.9
En outre, l'AC respecte les engagements suivants :

- informer les entités suivantes de la compromission : tous les porteurs, MC et les autres entités avec lesquelles l'AC a passé des accords ou a d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information doit être mise à disposition des autres tiers utilisateurs ;
- indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

En cas de compromission de l'AC, une liste des numéros de série des certificats révoquées sera dressée et publiées sur le site officiel de l'AC. L'origine et l'intégrité de cette liste sera assurée par un cachet électronique de Datasure dont le certificat est émis par une autre AC que celle compromise [CSS-6.3.10-12].

5.8 Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses. La présente section présente les dispositions relatives à la fin de vie [REQ-6.1-11].
L'AC et le service de signature/gestion de QSCD à distance dispose d'un plan de fin de vie à jour [REQ-7.12-02]/[119231-2/ OVR-7.12-01].

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite. [REQ-7.12-03]. Cette exigence est également applicable à la gestion du QSCD.
Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.
La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

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

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC, ainsi que le service de signature et de gestion de QSCD s'assure de :

- Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats, archivage des fichiers de preuve).
- Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication de l'état des certificat), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC/DPC.

L'AC Datasure et son service de signature/gestion de QSCD à distance s'engagent les éléments suivants :

- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats Datasure avise ces derniers aussitôt que nécessaire et, au moins, sous le délai d'un (1) mois.
- Datasure communique à l'ANSSI les principes du plan d'action qui met en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle présente notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC/DPC. Datasure communique à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. Datasure mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats.
- Datasure tiendra informée l'ANSSI de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus.

5.8.2 Cessation d'activité affectant l'AC et le service de gestion de QSCD à distance

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité sera mise en œuvre de façon progressive de telle sorte que seules les obligations ci-dessous soient à exécuter par Datasure, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.
Dans l'hypothèse d'une cessation d'activité totale, Datasure ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans la présente PC/DPC.

Datasure doit stipuler dans sa DPC confidentielle les dispositions prises en cas de cessation de service. Elles incluent:

- la notification des entités affectées ;
- le transfert de ses obligations à d'autres parties ;
- la gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés
- la destruction des clés associés à des certificats permanents hébergées sur le QSCD à distance

En particulier en cas de fin de vie, concernant le statut de révocation [CSS-6.3.10-12] :

- la responsabilité de l'activité de publication sera reprise par le Groupe Certisure, maison mère de Datasure.
- En cas d'arrêt du groupe, Datasure a créé une entité indépendante chargée d'assurer la continuité de la publication, en particulier des dernières CRL produites. Cette entité dispose des ressources nécessaires pour assurer cette publication pour la durée légale de 7 ans.

Dans tous les cas, les éléments publiés seront également transmis à l'ANSSI.
Lors de l'arrêt du service, Datasure :

- s'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;

- prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- révoque son certificat ;
- révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- détruit toutes les clés associées aux certificats permanents hébergées sur le QSCD et prend toutes les mesures nécessaires pour empêcher toute restauration.
- informer(par exemple par récépissé) tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre 3.2.3).

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

La génération des clés de signature d'AC doit être effectuée dans un environnement sécurisé (cf. chapitre V).
Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences de qualification au niveau renforcé de l'ANSSI.
La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre 5.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies se déroulent suivant des scripts préalablement définis.
Selon le cas, l'initialisation de l'IGC et/ou la génération des clés de signature d'AC s'accompagne la génération de parts de secrets d'IGC.

Suite à leur génération, les parts de secrets sont remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne détient plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets est mise en œuvre par son porteur. Ce dernier peut le cas échéant, en accord avec le responsable de l'IGC, notamment en cas d'indisponibilité au moment ou la cérémonie ce clé doit être opérée, transférer temporairement ou définitivement cette part de secret à un personnel désigné.

Les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins deux sont externes à l'AC et sont impartiaux [GEN-6.4.3-02]. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. L'un des témoins est un huissier de justice (désormais Commissaire de justice).

6.1.1.2 Clés porteurs générées par l'AC

Lorsque l'AC Datasure génère les clés des porteurs, elle le fait en toute sécurité [GEN-6.3.3-03]. Cette modalité s'applique aux cas d'usage suivantes.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	La clé est générée par l'opérateur sur un dispositif QSCD carte à puce dans des conditions sécurisées décrites dans la DPC confidentielle.
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	

6.1.1.3 Clés porteurs générées par le porteur

Dans la pratique deux cas d'usage se présentent :

- Le cas où la clé est générée par le porteur
- La cas où la clé est générée par le service de signature Datasure, à la demande du porteur.

Nous décrivons ci-dessous les différents cas.

Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	L'AC Datasure ne génère pas stricto sensu la clé privée du signataire, cependant, celle-ci est générée dans le QSCD à distance opérée par le service de signature ou de cachet Datasure [119431-1/ GEN-6.2.1-01] avec des paramètre appropriés [119431-1/ GEN-6.2.1-03]. La clé ne peut être utilisée hors du QSCD [119431-1/ GEN-6.2.1-02]. La préparation du QSCD à distance est réalisé sous « dual control » [119431-1/ GEN-6.2.1-05]. Les clés des porteurs ne sont pas pré-générées mais Datasure s'autorise ce processus [119431-1/ GEN-6.2.1-07].
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Le certificat est généré par le porteur et Datasure n'est jamais en possession de la clé privée.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	La clé est générée par l'AH datasure.

6.1.2 Transmission de la clé privée à son propriétaire

6.1.2.1 Clés d'AC

Non applicable, la clé privée est générée par l'AC.

6.1.2.2 Clés porteurs générées par l'AC

La clé privée est transmise au porteur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Cette transmission se fait directement dans le dispositif de protection des éléments secrets du porteur. Plus particulièrement :

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Le QSCD carte-à-puce est transmis par courrier recommandé.
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	

6.1.2.3 Clés porteurs non-générées par l'AC

Non applicable

6.1.3 Transmission de la clé publique à l'AC

6.1.3.1 Clés d'AC

La clé publique est transmise, sous forme de CSR, de façon sécurisée sous la supervision d'au moins deux personnes en rôle de confiance et devant témoin lors d'une cérémonie de clé.

6.1.3.2 Clés porteurs générées par l'AC

Non applicable.

6.1.3.3 Clés porteurs non-générées par l'AC

Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	Le service de signature de Datasure se charge de générer une CSR au format PKCS#10 qui est transmise de façon sécurisée à l'AC de façon a protéger son origine et son intégrité.
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	

Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	La clé publique est transmis au format PKCS#10 par un canal sécurisé.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	La procédure est interne

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

Les clés publiques de vérification de signature de l'AC sont diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine. Pour cela, le dispositif suivant est mis en place :

- Le certificat de l'AC est publié sur le site de publication (§2.2)
- Le certificat de l'AC Racine est publié accompagné de son haché SHA512.
-

6.1.5 Taille de clé

Les tailles de clés suivantes sont utilisées :

Clés de l'AC et de l'AC Racine	RSA 4096 bit
Clés des porteurs	A minima RSA 3072 bit

En particulier, la taille de clé des porteurs concerne également les paires de clés générées dans le QSCD à distance [119 431-1/OVR-5.1-02/ GEN-6.2.1-04]

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

Les paramètres et les algorithmes utilisés sont documentés par l'AC et sont précisés dans les profils de certificats (chapitre §7) [OVR-5.2-04] [119 431-1/OVR-5.1-02]

6.1.7 Objectifs d'usage de la clé

6.1.7.1 Clés d'AC

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats d'utilisateur final, d'OCSP et de LCR / LAR [OVR-5.2-10].

6.1.7.2 Clés porteurs (cas général)

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la fonction de sécurité concernée (voir section 1.4).

6.1.7.3 Clés porteurs (cas du QSCD à distance)

Les clés des porteurs visent à générer des signatures avancées au sens du Règlement eIDAS au format PAdES-T[5] a minima (les formats PAdES-LT/LTA peuvent également être envisagées) [TS 119431-2/ OVR-6.1-04]. Les signatures sont créées avec les algorithmes de signature conforme aux recommandations de l'ETSI TS 119 312 et de l'ANSSI (recommandation SOG-IS) [TS 119431-2/ OVR-6.1-02]/ [TS 119431-1/GEN-6.2.1-06/SIG-6.3.1-10]. En particulier, l'algorithme RSA-PSS est utilisée avec un algorithme de hachage de SHA-256 *a minima*. En accord avec le format PAdES, le certificat du signataire et la chaîne complète de certificat est incluse dans la signature PAdES [TS 119431-2/ OVR-8.2-06 / OVR-B.1-03] .
Les clés ne peuvent être utilisées avant la génération du certificat [TS 119431-1/ LNK-6.2.3-02].
Les AC utilisées pour inclure des horodatages sont [TS 119431-2/ OVR-8.2-02] :

- L'AH qualifiée Datasure
- L'AH qualifiée Certigna (en cas de panne de l'AH Datasure)

[5] D'autres formats tels que CAdES ou XAdES pourront être envisagées dans le futur.

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

Des mesures de sécurité et de contrôle sont mises en place pour la gestion des clés cryptographiques et du matériel cryptographique associé au travers de leur cycle de vie [REQ-7.5-01].

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature des certificats des porteurs est un module cryptographique qualifié au niveau renforcé par l'ANSSI.

6.2.1.2 Dispositifs de protection des éléments secrets des porteurs

Les dispositifs de protection des éléments secrets des porteurs, pour la mise en œuvre de leurs clés privées respecte les exigences suivantes.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Le dispositif est certifié QSCD
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	Le dispositif est certifié QSCD à distance notifié à la commission Européenne.
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Sous la responsabilité du demandeur.
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Voir cas Q2
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Voir cas Q1.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Voir cas Q3.
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Le dispositif est un HSM conforme à la PH.
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	Voir cas Q2
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Voir cas Q3.
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Voir cas Q2
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Voir cas Q3.
Cas B1. Certificat Biométrie	Voir cas Q2.

1.3.6.1.4.1.58753.2.1.1.1.3.1.1	

Le dispositif est soit fourni directement par l'AC Datasure, soit fourni par le service de signature de Datasure. L'AC s'assure que:

- la préparation des dispositifs de protection des éléments secrets est contrôlée de façon sécurisée;
- les dispositifs de protection des éléments secrets sont stockés et distribués de façon sécurisée ;

Les désactivations des dispositifs de protection des éléments secrets ne sont pas mis en œuvre.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 2).

Concernant les clés de signature du QSCD, des mesures de ségrégation sont en place de façon à ce qu'un utilisateur ne puisse signer avec la clé d'un autre utilisateur [119431-1/ SIG-6.3.1-03].

6.2.3 Séquestre de la clé privée

Le séquestre de clé privé est interdit par la présente PC [SDP-6.3.12-03/SDP-6.3.12-04 / SDP-6.3.12-05/SDP-6.3.12-06 / SDP-6.3.12-07]

6.2.4 Copie de secours de la clé privée

6.2.4.1 Clés d'AC

Les clés privées d'AC font l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences décrites dans la présente PC , soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée.
Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.
Le contrôle des opérations de chiffrement / déchiffrement doit être conforme aux exigences du chapitre 6.2.2.

6.2.4.2 Clés porteurs

Aucune clé privée de porteur ne fait l'objet de copie de secours par l'AC.

Le service de signature de Datasure réalise des copies de secours des clés privés (certificats non-éphémère) des porteurs afin d'en assurer la disponibilité. Dans ce cas, les copies de secours bénéficient du même niveau de sécurité que les clés d'origine [SDP-6.3.12-01]. Le nombre de copie est limité au strict minimum pour assurer la continuité du service [SDP-6.3.12-02] [TS19231-1/ GEN-6.3.3-04/ GEN-6.3.3-01// GEN-6.3.3-02].
En dehors des mesures de redondances, tout restauration ne peut être réalisées que sous « dual contrôle » par du personnel autorisé [TS19231-1/ GEN-6.3.3-03]

6.2.5 Archivage de la clé privée

6.2.5.1 Clés d'AC

Les clés privées de l'AC ne sont pas archivées.

6.2.5.2 Clés porteurs

Les clés privées des porteurs ne sont pas archivées.

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

6.2.6.1 Clés d'AC

Pour les clés privées d'AC, tout transfert doit se faire sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.6.2 Clés porteurs

Pour les clés générées au format PKCS#12, le transfert se fait sous forme chiffré, conformément au chapitre 6.2.4.

6.2.7 Stockage de la clé privée dans un module cryptographique

Voir 6.2.1.1.
Les copies de secours des clés d'AC sont réalisées hors du module cryptographique conformément au 6.2.4.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés d'AC

L'activation des clés privées d'AC dans un module cryptographique est contrôlée via des données d'activation (cf. chapitre 6.4) et fait intervenir au moins deux personnes dans des rôles de confiance.

6.2.8.2 Clés privées des porteurs

La méthode d'activation de la clé privée du porteur dépend du dispositif utilisé.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Le moyen d'activation est le code PIN de la carte à puce
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	L'activation de la clé privée ne peut se faire qu'à la suite du processus de vérification de l'identité (certificat éphémère) [119431-1/SIG-6.3.1-01]. Cela implique donc que la clé privée est sous le contrôle exclusif du signataire [OVR-6.3.5-04/ OVR-6.3.5-05] et est lié avec le certificat du signataire au travers de la clé publique [119431-1/ LNK-6.2.3-01]. Datasure s'assure de l'intégrité du lien entre la clé et le certificat associé [119431-1/ LNK-6.2.3-03]. Le protocole de signature est conçu pour éviter les attaques « man-in-the-middle », les rejeu et plus généralement les méthodes d'attaques s'appuyant sur l'utilisation des moyens d'identification / authentification de tiers [119431-1/ SIG-6.3.1-02] Cela est en particulier assuré par l'utilisation de certificats éphémères et de données d'activations liées aux données à signer (SAD), permettant de s'assurer que les données liées à un utilisateurs ne peuvent être signées que par la clé privée e cet utilisateur [119431-1/ SIG-6.3.1-04/ SIG-6.3.1-05] La clé du porteur ne peut être utilisée sans vérification préalable du SAD. [119431-1/ SIG-6.3.1-07]
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Le moyen d'activation est le sous le contrôle du demandeur, la clé n'était pas générée dans le périmètre Datasure.
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	L'activation de la clé privée ne peut se faire qu'à la suite d'une authentification de la personne morale ou d'un représentant autorisé, assurant ainsi le contrôle sur la clé. [OVR-6.3.5-04/ OVR-6.3.5-05].
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les modalités sont similaires au cas Q1.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Les modalités sont similaires au cas Q3.
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	L'activation de la clé privée s'appuie sur les mécanisme du HSM protégeant la clé de l'unité d'horodatage (voir PH).
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	S'agissant également de l'usage du QSCD à distance, similaire au cas Q2.
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Les modalités sont similaires au cas Q3.

Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Similaire au cas Q2.
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Les modalités sont similaires au cas 3.
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Similaire au cas 2.

Pour les cas impliquant le QSCD à distance, Datasure s'appuie sur un dispositif conforme à la norme ETSI TS 119 431-1 [OVR-6.3.5-06].

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés d'AC

La désactivation des clés privées d'AC dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

6.2.9.2 Clés privées des porteurs

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	La clé privée peut-être désactivée en retirant le support carte-à-puce du lecteur (ou en déconnectant la clé USB du token). De plus, 3 erreurs PIN désactivent définitivement la clé.
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	Non applicable, la clé privée est détruite après chaque session de signature.
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Non applicable, le moyen d'activation est le sous le contrôle du demandeur, la clé n'était pas générée dans le périmètre Datasure.
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les données d'activation sont à usage unique, la clé privée est donc désactivée automatiquement par le QSCD. De plus, l'administrateur du QSCD peut à tout moment suspendre le processus de création de données d'activation.
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les modalités sont similaires au cas Q1.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Les modalités sont similaires au cas Q3.

Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	La clé privée peut être désactivée en arrêtant le HSM ou en désactivant les accès au HSM.
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	S'agissant également de l'usage du QSCD à distance, similaire au cas 2.
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Les modalités sont similaires au cas Q3.
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Similaire au cas Q2.
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Les modalités sont similaires au cas Q3.
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Similaire au cas Q2.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés d'AC

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé doit est systématiquement détruite au moyen des fonctions d'effacement du HSM, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.10.2 Clés privées des porteurs

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	La clé privée peut être définitivement détruite en détruisant le support.
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	La clé privée est éphémère : elle est automatiquement détruite après l'opération unique de signature [TS 119231-1 / DEL-6.3.2-02/ DEL-6.3.2-01/ DEL-6.3.2-03].
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Non applicable, le moyen de signature étant sous le contrôle du signataire. Pour le cas d'un certificat logiciel, le porteur

	peut effacer le fichier contenant la clé privée, ainsi que toutes les éventuelles copies de secours.
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Une fonction du QSCD permet d'effacer définitivement une clé privée, en particulier à la demande du responsable de certificat dans le cas d'une révocation [TS 119231-1 / DEL-6.3.2-02/]. Cela inclut tout copie redondé des clés et sauvegardes associées [TS 119231-1 /DEL-6.3.2-04]
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les modalités sont similaires au cas Q1.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Les modalités sont similaires au cas Q3.
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Une fonction du HSM permet d'effacer la clé privée de façon sécurisée, ainsi que les éventuelles copies de secours.
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	S'agissant également de l'usage du QSCD à distance, similaire au cas Q2.
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Les modalités sont similaires au cas Q3.
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Similaire au cas Q2.
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Les modalités sont similaires au cas Q3.
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Similaire au cas Q2.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de protection des éléments secrets

6.2.11.1 HSM de l'AC

Voir 6.2.1.

6.2.11.2 QSCD Carte-à-puce

En cas de modification du statut du QSCD sur la liste de confiance, Datasure réaliserait les actions suivantes en cas de retrait du QSCD [SDP-6.5.1-07B] :

- Notification de l'ANSSI et des porteurs de certificats utilisant ce QSCD de l'impact
- Suspension immédiate de la production de nouvelles cartes
- Révocation des certificats en cours de validité sur QSCD

- Recherche d’un nouveau fournisseur avec un statut notifié
- Renouvellement des certificats sur le nouveau QSCD.

Dans la mesure du possible, si la modification du statut peut-être anticipée (par exemple, connaissance d’un non-renouvellement de certification ou changement du statut de qualification par l’ANSSI), il sera proposé aux utilisateurs un renouvellement par anticipation.

6.2.11.3 QSCD à distance

En cas de modification du statut du QSCD sur la liste de confiance, Datasure réaliserait les actions suivantes en cas de retrait du QSCD [SDP-6.5.1-07B] :

- Notification de l’ANSSI et des clients se reposant sur ce service
- Suspension du service de signature et des scellements qualifié
- Révocation des certificats de cachets qualifiés sur QSCD à distance.

Il est à noter que la modification de statut n’impacte que les Q4 et Q5 (signature qualifié et cachet qualifié à distance). Les autres cas d’usage à distance ne nécessitant pas un QSCD.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC et des porteurs sont archivées dans le cadre de l'archivage des certificats correspondants. La durée d’archivage est de 7 ans à compter de l’expiration du certificat.

6.3.2 Durées de vie des bi-clés et des certificats

Les durée de vie des bi-clés et des certificats sont indiquées dans les profils du chapitre 7.
La fin de validité d'un certificat d'AC est postérieure à la fin de vie des certificats porteurs qu'elle émet.
La durée d’utilisation de la clé privée est également à la durée de vie du certificat à l’exception des certificats d’unités d’horodatage, pour lesquels la durée est limitée à 3 ans.

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 d'un module cryptographique de l'IGC se fait lors de la phase d'initialisation et de personnalisation de ce module durant la cérémonie des clés. Les données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués.

6.4.1.2 Clés de porteurs

Le mécanisme diffère selon le type de certificat.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Le code PIN est généré de façon sécurisée par l'opérateur d'enregistrement Datasure
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	Les données d'activation sont générées dans un environnement sécurisé.
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Les données d'activation sont créées par le porteur.
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Voir cas Q2
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les modalités sont similaires au cas Q1.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Les modalités sont similaires au cas Q3.
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Les données d'activation sont créées lors d'une cérémonie des clés.
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	S'agissant également de l'usage du QSCD à distance, similaire au cas Q2.
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Les modalités sont similaires au cas Q3.
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Similaire au cas Q2.
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Les modalités sont similaires au cas Q3.
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Similaire au cas Q2.

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

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'IGC sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire durant la cérémonie des clés. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité. En particulier, les clés sont stockées dans des coffres individuels.

6.4.2.2 Protection des données d'activation correspondant aux clés privées des porteurs

Le mécanisme diffère selon le type de certificat.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Le code PIN des dispositifs de protection des éléments secrets des porteurs est généré par l'AC, il est protégé en intégrité et en confidentialité jusqu'à la remise aux porteurs.
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	La clé d'activation est conservée dans l'environnement sécurisé où elle a été générée.
Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Non applicable, le moyen de signature étant sous le contrôle du signataire.
CasQ 4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Voir cas Q2
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les modalités sont similaires au cas Q1.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Les modalités sont similaires au cas Q3.
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Les données d'activation sont conservées par des porteurs de secret .
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	S'agissant également de l'usage du QSCD à distance, similaire au cas Q2.
Cas C2. Certificat authentification NCP+ personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Les modalités sont similaires au cas Q3.
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Similaire au cas Q2.
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Les modalités sont similaires au cas Q3.
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Similaire au cas Q2.

6.4.3 Autres aspects liés aux données d'activation

Non applicable.

6.5 Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risque de l'AC.

Datasure a réalisé une analyse de risque afin d'identifier, analyser et évaluer les risques portant sur le service de confiance, incluant l'AC mais également le service de signature [119431-2/OVR-9-05]. En particulier, l'analyse de risque prend en compte les risques techniques mais également les risques métiers [REQ-5-01]. Datasure sélectionne les mesures de traitement du risque appropriés à partir des résultats de l'analyse de risque [REQ-5-02].
Datasure détermine l'ensemble des exigences de sécurité et procédures opérationnelles nécessaires à la mise en place des mesures de sécurité sélectionnées et documentées dans la PSSI et dans la présent PC/DPC [REQ-5-03]. Cette documentation est complétée d'une partie confidentielle de la PC/DPC ainsi que d'un corpus documentaire décrivant les politiques et procédures de l'AC [REQ-5-06]. Ces documents sont approuvés par le management de Datasure, mis à disposition et communiqué aux employés concernés, ainsi qu'aux personnels externes et sous-traitant lorsque cela est approprié [REQ-5-07]
L'analyse de risques est revue et révisée régulièrement, a minima annuellement et lors de chaque changement majeur [REQ-5-04].
L'analyse de risque fait l'objet d'une approbation formelle par l'organisme de gouvernance de Datasure qui accepte le risque résiduel. En particulier, Datasure met en place, conformément aux exigences de l'ANSSI, une procédure d'homologation [REQ-5-05].

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

6.5.1.1 PSSI

Datasure a défini une politique de sécurité du système d'information (PSSI). Cette politique présente l'approche mise en oeuvre pour la gestion de la sécurité et reprend, entre autre, les mesures de sécurité identifiées dans l'analyse de risque ainsi que les mesures issues du guide d'hygiène informatique de l'ANSSI, lorsque ces mesures sont applicable. La PSSI fait l'objet d'une approbation formelle par l'autorité de Gouvernance [REQ-6.3-01].
La PSSI est documentée, mis en œuvre et maintenue à jour. Celle-ci inclut, entre autres, les procédures de contrôle et les procédures opérationnelles pour les sites Datasure, les systèmes d'informations et les biens entrant en jeu dans la délivrance du service [REQ-6.3-03].
La PSSI est communiquée à l'ensemble des personnels et sous traitants concernés [REQ-6.3-04].
Toute modification de la PSSI fait l'objet d'une communication aux personnes concernées, éventuellement externe à Datasure [REQ-6.3-02]
La PSSI, ainsi que les différents inventaires des biens, font l'objet de revues régulières, ou sont systématiquement revues en cas de changement majeurs [REQ-6.3-07].

Les exigences relatives à la PSSI couvre le périmètre de l'AC mais également le périmètre du service de signature et de gestion du QSCD [TS119431-2/OVR-6.3-01]

6.5.1.2 Niveau de sécurité des systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est décrite dans la DPC confidentielle de l'AC ainsi que dans sa PSSI
Il répond au moins répondre aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique),
- gestion des droits des utilisateurs (permettant de mettre en oeuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels [REQ-7.7-05],
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- protection du réseau contre toute intrusion d'une personne non autorisée,
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- fonctions d'audits (non-répudiation et nature des actions effectuées),

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle font l'objet de mesures particulières découlant de l'analyse de risque.
Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont mis en place.

6.5.1.3 Gestion des accès

L'accès aux différent composants du service est limité aux personnels autorisés [REQ-7.4-01].
Datasure administre les accès des administrateurs, opérateurs et auditeurs sur le principe du moindre privilège [REQ-7.4-04A]. Cette tâche inclut la gestion des utilisateurs et la désactivation/modification des accès sans délai en cas de besoin [REQ-7.4-05]. Les droits sont appliqués conformément à la politique de contrôle d'accès [REQ-7.4-06].

Les composants de l'AC fournissent des mécanismes de contrôle permettant de séparer les différents rôles de confiance identifiés, en particulier en séparant les niveaux administrateurs et opérateurs [REQ-7.4-07].

Le personnel travaillant sur l'AC est identifié et authentifié avant d'accèder à n'importe quel élément critique de l'infrastructure [REQ-7.4-08]. Les actions des personnels sont tracés (voir 5.4) [REQ-7.4-09]

6.5.1.4 Veille technique et vulnérabilité

Datasure met en place des procédures de veille technique. En particulier, ces mesures permettent de s'assurer que les mises à jour de sécurité sont appliqués dans une délai raisonnable après leur mise à disposition. Les mises à jour de sécurité sont appliquées seulement si elles n'introduisent pas de risques vulnérabilités ou d'instabilités qui surpasseraient les bénéfices de leur application. Lorsqu'une mise à jour de sécurité n'est pas appliquée, elle fait l'objet d'une documentation.[REQ-7.7-09]
Toutes vulnérabilités critiques doit être adressée dans les 48 heures suivant leur découverte [REQ-7.9-10].

Pour chaque vulnérabilité, prenant en compte l'impact potentiel, Datasure :

- Définira et mettra en œuvre un plan de correction ou de contournement de la vulnérabilité, ou
- Documentera de façon factuelle les raisons ne nécessitant pas de corriger la vulnérabilité (par exemple, vulnérabilité sur un interface réseau d'un dispositif hors ligne). [REQ-7.9-11].

6.5.1.5 Scan de vulnérabilité

Des scans de vulnérabilités réguliers sont mis en œuvre sur les IP publiques et privées du service.
Datasure garde les éléments de preuve permettant de démontrer que les scans de vulnérabilités ont été réalisés par du personnel ou une organisation ayant les compétences, les outils, un code d'éthique et l'indépendance nécessaire pour fournir un rapport d'audit fiable [REQ-7.8-13].
Le scan de vulnérabilités est réalisé au moins une fois par trimestre [REQ-7.8-13].

6.5.1.6 Test de pénétration.

Datasure réalise un test de pénétration avant l'ouverture de son service et après chaque modification majeur de celui-ci [REQ-7.8-14].
Ce test est réalisé sur une base annuelle [REQ-7.8-14A].
Datasure garde les éléments de preuve permettant de démontrer que les tests de pénétration ont été réalisés par du personnel ou une organisation ayant les compétences, les outils, un code d'éthique et l'indépendance nécessaire pour fournir un rapport d'audit fiable [REQ-7.8-15].

6.5.2 Niveau de qualification des systèmes informatiques

Voir 6.2.1

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques satisfont aux objectifs de sécurité découlant de l'analyse de risque de l'AC.

6.6.1 Mesures de sécurité liées au développement des systèmes

Une analyse des besoins de sécurité est réalisée en phase amont des développements au travers d'une étapes de spécification des exigences de sécurité du système à développer [REQ-7.7-02]

6.6.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC est signalée à l'AC pour validation par l'autorité de Gouvernance [REQ-6.3-08]. Elle est documentée et apparaît dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

Des procédures de gestion des changements sont mis en place afin d'encadre les livraisons, modifications et mise à jour d'urgence des briques logicielles des différents composants de la plate-

forme et de leur configuration [REQ-7.7-03]. Ces procédures incluent la documentation des changements [REQ-7.7-04]

La configuration des différents composants de l'AC font l'objet de vérification régulières, afin d'identifier des changements qui seraient en contradiction avec les règles de la présente PC/DPC ou de la PSSI [REQ-6.3-09] La fréquence des vérifications est précisée dans la DPC confidentielle. Elle est a minima annuelle [REQ-6.3-10].

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

Non applicable

6.7 Mesures de sécurité réseau

Datasure met en œuvre des mesures de sécurité contre les attaques réseau [REQ-7.8-01]

6.7.1 Segmentation réseau

En particulier, Datasure segmente son Système d'information en zones réseau distinctes en s'appuyant sur l'analyse de risque réalisée. En particulier, les séparations au niveau fonctionnel, logique et physique sont pris en compte [REQ-7.8-02]
Datasure applique des mesures de sécurité similaires à l'ensemble des systèmes d'une même zone réseau [REQ-7.8-03].
L'ensemble des systèmes les plus sensibles sont gérés dans les zones réseaux les plus sécurisées. En particulier, l'AC Racine est opérée hors ligne [REQ-7.8-07].
Les réseaux dédiés aux opérations et à l'administration font l'objet d'une séparation [REQ-7.8-08] Les systèmes dédiés à l'administration ne peuvent être utilisés pour d'autres usages [REQ-7.8-09]

6.7.2 Filtrage des flux et interconnexions

Les communications et accès entre les différentes zones sont restreintes aux seules nécessaire pour les opérations du service [REQ-7.8-04]. Ces restrictions sont permises par des mesures de contrôles réseaux (tel que la mise en place de pare-feu) permettant de prémunir le service contre les accès non autorisés, y compris les accès des utilisateurs et des abonnés [REQ-7.8-16].
Toutes les communications et services non nécessaires sont explicitement interdits ou désactivés [REQ-7.8-05]. En particulier, les pare-feu sont configurés de manière à ne laisse passer que les flux réseaux strictement nécessaire aux opérations du service [REQ-7.8-17]

En particulier, l'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.
L'AC garantit que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC [REQ-7.8-06].

6.7.3 Communication entre composants

Les communications entre les différents composants sont sécurisés par des canaux permettant leur isolation. Cette isolation s'appuie sur des mécanismes logiques, cryptographiques ou physiques permettant leur isolation des autres canaux de communications. En particulier, il permettant d'assurer la confidentialité et l'intégrité des échanges [REQ-7.8-11].

Datasure utilise une connexion sécurisée entre l'application de création de signature et le QSCD.[119431-2/ ASI-8.1-02] ainsi qu'entre l'application de signature et les utilisateurs. Cette connexion permet de garantir l'intégrité et la confidentialité des informations reçues [119431-2/ OVR-8.2-01].

6.7.4 Séparation des plates-formes de production et de test.

Les plates-formes de production et les plates-formes hors production (test, pre-production) font l'objet d'une séparation stricte [REQ-7.8-10]

6.8 Horodatage / Système de datation

Les horloges de l'ensemble des systèmes sont synchronisés avec une source de temps UTC a minima toutes les 24h [REQ-7.10-06].

7 Profil des certificats, CRL et des OCSP

7.1 Profil du certificat de l'AC Racine (Datasure Root CA)

7.1.1 Champs de base

Champ	Valeur
Version	V3
Serial Number	1120c36f6bf2f65adb2acf724a6dd6dad657
Signature	SHA-256 RSA 4096
Subject Public Key Info	RSA 4096 bits
Validity	20 years

Issuer DN	CN = DATASURE Root CA OU = 0002 90466620300016 OI (oid:2.5.4.97) = NTRFR-90466620300016 O = DATASURE C = FR
Subject DN	CN = DATASURE Root CA OU = 0002 90466620300016 OI (oid:2.5.4.97) = NTRFR-90466620300016 O = DATASURE C = FR

7.1.2 Extension de certificat

Extension	Critique	Description
Subject key identifier	non	Identifiant de la clé publique de l'autorité Racine
Authority key identifier	non	Identifiant de la clé publique de l'autorité Racine
Basic constraint	oui	CA = TRUE
Key Usage	oui	Signature de certificat Signature de CRL

7.2 Profil du certificat de l'AC Opérationnelle (Datasure Global CA)

7.2.1 Champs de base

Champ	Valeur
Version	V3
Serial Number	11207823e390ce0265358d4798fa8ce59d39
Signature	SHA-256 RSA 4096
Subject Public Key Info	RSA 4096 bits
Validity	10 ans
Issuer DN	CN = DATASURE Root CA OU = 0002 90466620300016 OI (oid:2.5.4.97) = NTRFR-90466620300016 O = DATASURE C = FR
Subject DN	CN = DATASURE Global CA OU = 0002 90466620300016

	OI (oid:2.5.4.97) = NTRFR-90466620300016 O = DATASURE C = FR

7.2.2 Extension de certificat

Extension	Critique	Description
Subject key identifier	non	Identifiant de la clé publique de l'autorité Global CA
Authority key identifier	non	Identifiant de la clé publique de l'autorité Root CA
Certificate Policies	non	**OID=**any policy **CPS=** https://www.datasure.net/download/pc-root.pdf
Authority Information Access	non	caIssuers= http://pki-p.datasure.net/datasure/cacert/DATASURE_Root_CA.cer
CRL Distribution Points	non	URL= http://pki-p.datasure.net/datasure/arl/DATASURE_Root_CA.crl
Basic constraint	oui	CA = TRUE PathLengthConstraint = 0
Key Usage	oui	Signature de certificat Signature de CRL

7.3 Profil du certificat final – certificat de signature qualifiée sur QSCD carte à puce

7.3.1 Champs de base

Champ	Valeur	
Version	V3	
Serial Number	Généré par l'AC	
Signature	SHA-256 RSA 3072-4096	
Subject Public Key Info	RSA 3072-4096 bits	
Validity	1 à 3 ans	
Issuer DN	CN = DATASURE Global CA OU = 0002 90466620300016 OI (oid:2.5.4.97) = NTRFR-90466620300016 O = DATASURE C = FR	
Subject DN	CN=	<Prénom> <Nom>

	GN=	<Prénom>
	SN=	<Nom>
	OI=	[conditionnel si champ O présent] Identifiant de la personne morale à laquelle la personne physique est attachée
	O=	[optionnel] nom de la personne morale
	C=	<Code Pays>
	SERIALNUMBER	Aléa permettant l'unicité du DN

7.3.2 Extension de certificat

Extension	Critique	Description
Subject key identifier	non	Identifiant de la clé publique du certificat
Authority key identifier	non	Identifiant de la clé publique de l'autorité qualifiée
Certificate Policies	non	OID=1.3.6.1.4.1.58753.2.1.1.1.1.1.1 CPS= https://www.datasure.net/download/pc-global.pdf
Authority Information Access	non	caIssuers= http://pki-p.datasure.net/datasure/cacert/DATASURE_Global_CA.cer ocsp= http://ocsp-p.datasure.net/DATASURE_Global_CA
CRL Distribution Points	non	URL= http://pki-p.datasure.net/datasure/crl/DATASURE_Global_CA.crl
Basic constraint	oui	CA = FALSE
Key Usage	oui	Digital Signature Non repudiation
Extended Key Usage	non	Client Auth Email Protection
QCstatement	non	QcCompliance
		QcQSCD
		QcEuPDS https://www.datasure.net/download/pds-global.pdf
		QcType eSignature

7.4 Profil du certificat final – certificat de signature qualifiée sur QSCD à distance

7.4.1 Champs de base

Champs identiques au 7.3.1 à l'exception des champs mentionnés ci-dessous

Champ	Valeur
Validity	24 heures (certificat éphémère)

7.4.2 Extension de certificat

Champs identiques au 7.3.2 à l'exception des champs mentionnés ci-dessous

Extension	Critique	Description
Certificate Policies	non	OID=1.3.6.1.4.1.58753.2.1.1.1.1.1.3 CPS= https://www.datasure.net/download/pc-global.pdf
validity assured extension	non	-

Les cas d'usage étendus ne sont ajoutés.

7.5 Profil du certificat final – certificat de signature qualifiée logiciel

7.5.1 Champs de base

Champs identiques au 7.3.1

7.5.2 Extension de certificat

Champs identiques au 7.3.2 à l'exception des champs mentionnés ci-dessous

Extension	Critique	Description
Certificate Policies	non	OID=1.3.6.1.4.1.58753.2.1.1.1.1.1.2 CPS= https://www.datasure.net/download/pc-global.pdf
QCstatement	non	QcCompliance
		QcEuPDS https://www.datasure.net/download/pds-global.pdf
		QcType eSignature

7.6 Profil du certificat final – certificat de cachet qualifiée sur QSCD à distance ou carte à puce

7.6.1 Champs de base

Champ	Valeur	
Version	V3	
Serial Number	Généré par l'AC	
Signature	SHA-256 RSA 3072-4096	
Subject Public Key Info	RSA 3072-4096 bits	
Validity	1 à 3 ans	
Issuer DN	CN = DATASURE Global CA OU = 0002 90466620300016 OI (oid:2.5.4.97) = NTRFR-90466620300016 O = DATASURE C = FR	
Subject DN	CN=	<Société> <Nom du service>
	OI=	Identifiant de la personne morale à laquelle la personne physique est attachée
	O=	Nom de la personne morale
	C=	<Code Pays>
	OU=	[optionnel] Service / sous diection

7.6.2 Extension de certificat

Extension	Critique	Description
Subject key identifier	non	Identifiant de la clé publique du certificat
Authority key identifier	non	Identifiant de la clé publique de l'autorité qualifiée
Certificate Policies	non	**OID=**1.3.6.1.4.1.58753.2.1.1.1.1.2.1 CPS= https://www.datasure.net/download/pc-global.pdf
Authority Information Access	non	calssuers= http://pki-p.datasure.net/datasure/cacert/DATASURE_Global_CA.cer ocsp= http://ocsp-p.datasure.net/DATASURE_Global_CA

CRL Distribution Points	non	URL= http://pki-p.datasure.net/datasure/crl/DATASURE_Global_CA.crl
Basic constraint	oui	CA = FALSE
Key Usage	oui	Digital Signature
QCstatement	non	QcCompliance
		QcQSCD
		QcEuPDS https://www.datasure.net/download/pds-global.pdf
		QcType eSeal

7.7 Profil du certificat final – certificat de cachet qualifiée sur QSCD logiciel

7.7.1 Champs de base

Les champs sont identiques au profil précédant

7.7.2 Extension de certificat

Les champs sont identiques au profil précédant à l'exception des extensions suivantes

Extension	Critique	Description
Certificate Policies	non	**OID=**1.3.6.1.4.1.58753.2.1.1.1.1.2.2 CPS= https://www.datasure.net/download/pc-global.pdf
QCstatement	non	QcCompliance
		QcEuPDS https://www.datasure.net/download/pds-global.pdf
		QcType eSeal

7.8 Profil du certificat final – certificat d'unité d'horodatage (QCP-l)

7.8.1 Champs de base

Champ	Valeur	
Version	V3	
Serial Number	Généré par l'AC	
Signature	SHA-256 RSA 3072-4096	
Subject Public Key Info	RSA 3072-4096 bits	
Validity	5 ans maximum	
Issuer DN	CN = DATASURE Global CA OU = 0002 90466620300016 OI (oid:2.5.4.97) = NTRFR-90466620300016 O = DATASURE C = FR	
Subject DN	CN=	DATASURE – DATASURE TSA<NN>
	OI=	NTRFR-90466620300016
	O=	DATASURE
	C=	FR

7.8.2 Extension de certificat

Extension	Critique	Description
Subject key identifier	non	Identifiant de la clé publique du certificat
Authority key identifier	non	Identifiant de la clé publique de l'autorité qualifiée
Certificate Policies	non	**OID=**1.3.6.1.4.1.58753.2.1.1.1.1.2.2 **CPS=** https://www.datasure.net/download/pc-global.pdf
Authority Information Access	non	calssuers= http://pki-p.datasure.net/datasure/cacert/DATASURE_Global_CA.cer ocsp= http://ocsp-p.datasure.net/DATASURE_Global_CA
CRL Distribution Points	non	URL= http://pki-p.datasure.net/datasure/crl/DATASURE_Global_CA.crl
Basic constraint	oui	CA = FALSE

Key Usage	oui	Digital Signature
Extended key usage	oui	id-kp-timeStamping
QCstatement	non	QcCompliance
		QcEuPDS https://www.datasure.net/download/pds-global.pdf
		QcType eSeal

7.9 Profil du certificat final – certificat de signature NCP+ à distance

7.9.1 Champs de base

Champ	**Valeur**	
Version	V3	
Serial Number	Généré par l'AC	
Signature	SHA-256 RSA 3072-4096	
Subject Public Key Info	RSA 3072-4096 bits	
Validity	24 heures	
Issuer DN	CN = DATASURE Global CA OU = 0002 90466620300016 OI (oid:2.5.4.97) = NTRFR-90466620300016 O = DATASURE C = FR	
Subject DN	CN=	<Prénom> <Nom>
	GN=	<Prénom>
	SN=	<Nom>
	OI=	[conditionnel si champ O présent] Identifiant de la personne morale à laquelle la personne physique est attachée
	O=	[optionnel] nom de la personne morale
	C=	<Code Pays>
	SERIALNUMBER	Aléa permettant l'unicité du DN

7.9.2 Extension de certificat

Extension	**Critique**	**Description**

Subject key identifier	non	Identifiant de la clé publique du certificat
Authority key identifier	non	Identifiant de la clé publique de l'autorité qualifiée
Certificate Policies	non	**OID=**1.3.6.1.4.1.58753.2.1.1.1.1.2.1.1 **CPS=** https://www.datasure.net/download/pc-global.pdf
Authority Information Access	non	caIssuers= http://pki-p.datasure.net/datasure/cacert/DATASURE_Global_CA.cer ocsp= http://ocsp-p.datasure.net/DATASURE_Global_CA
CRL Distribution Points	non	URL= http://pki-p.datasure.net/datasure/crl/DATASURE_Global_CA.crl
Basic constraint	oui	CA = FALSE
Key Usage	oui	Digital Signature Non repudiation
validity assured extension	non	-

7.10 Profil du certificat final – certificat de cachet NCP (authentification)

7.10.1 Champs de base

Identique au §7.6.1

7.10.2 Extension de certificat

Extension	Critique	Description
Subject key identifier	non	Identifiant de la clé publique du certificat
Authority key identifier	non	Identifiant de la clé publique de l'autorité qualifiée
Certificate Policies	non	**OID=**1.3.6.1.4.1.58753.2.1.1.1.1.2.2.1 **CPS=** https://www.datasure.net/download/pc-global.pdf
Authority Information Access	non	caIssuers= http://pki-p.datasure.net/datasure/cacert/DATASURE_Global_CA.cer ocsp= http://ocsp-p.datasure.net/DATASURE_Global_CA
CRL Distribution Points	non	URL= http://pki-p.datasure.net/datasure/crl/DATASURE_Global_CA.crl
Basic constraint	oui	CA = FALSE
Key Usage	oui	Digital Signature
Extended key usage	non	ClientAuthentication

7.11 Profil du certificat final – certificat de signature LCP à distance

7.11.1 Champs de base

Les champs de base sont similaires au 7.8.1

7.11.2 Extension de certificat

Les champs d'extension sont similaires au 7.8.2.

Extension	Critique	Description
Certificate Policies	non	**OID=**1.3.6.1.4.1.58753.2.1.1.1.2.1.2 **CPS=** https://www.datasure.net/download/pc-global.pdf
validity assured extension	non	-

7.12 Profil du certificat final – certificat de LCP

7.12.1 Champs de base

Les champs sont identiques au profil 7.6.1.

7.12.2 Extension de certificat

Extension	Critique	Description
Subject key identifier	non	Identifiant de la clé publique du certificat
Authority key identifier	non	Identifiant de la clé publique de l'autorité qualifiée
Certificate Policies	non	**OID=**1.3.6.1.4.1.58753.2.1.1.1.2.2.2 CPS= https://www.datasure.net/download/pc-global.pdf
Authority Information Access	non	caIssuers= http://pki-p.datasure.net/datasure/cacert/DATASURE_Global_CA.cer ocsp= http://ocsp-p.datasure.net/DATASURE_Global_CA
CRL Distribution Points	non	URL= http://pki-p.datasure.net/datasure/crl/DATASURE_Global_CA.crl

Basic constraint	oui	CA = FALSE
Key Usage	oui	Digital Signature

7.13 Profil du certificat final – certificat de Biométrie

7.13.1 Champs de base

Les champs de base sont similaires au 7.8.1

7.13.2 Extension de certificat

Les champs d'extension sont similaires au 7.8.2 à l'exception du champ suivant

Extension	Critique	Description
Certificate Policies	non	OID=1.3.6.1.4.1.58753.2.1.1.1.3.1.1 CPS= https://www.datasure.net/download/pc-global.pdf
validity assured extension	non	-

7.14 Profil de l'ARL

7.14.1 Champs de base

Champ	Valeur
Version	V1
Issuer DN	CN = DATASURE Root CA OU = 0002 90466620300016 OI (oid:2.5.4.97) = NTRFR-90466620300016 O = DATASURE C = FR
Durée de validité	12 mois

Les ARL sont produites avec 2 mois de recouvrement.

7.14.2 Extensions

Champ	Valeur
Authority key identifier	Valeur de l'AC Racine
CRL Number	Généré de façon incrémentale par l'AC

7.15 Profil de la CRL

7.15.1 Champs de base

Champ	Valeur
Version	V1
Issuer DN	CN = DATASURE Global CA OU = 0002 90466620300016 OI (oid:2.5.4.97) = NTRFR-90466620300016 O = DATASURE C = FR
Durée de validité	7 jours

7.15.2 Extensions

Champ	Valeur
Authority key identifier	Valeur de l'AC fille
CRL Number	Généré de façon incrémentale par l'AC
ExpiredCertsOnCRL	présent

7.16 Profil de l'OCSP

Le profil OCSP est conforme à la RFC 6960 avec les particularisme suivants :

- Le certificat est produit par l'AC
- L'extension « archive cutoff » est présente
- Le statut de révocation est maintenu après expiration

8 Audit de conformité et autre évaluations

Les audits et les évaluations concernent,

- d'une part, ceux réalisés en vue de la délivrance d'une évaluation et/ou d'une certification de conformité aux normes ETSI 319411-1, 319411-2 et du processus de qualification eIDAS ;
- d'autre part, les audits dit « internes » que réalise l'AC afin de s'assurer que l'ensemble de l'IGC est conforme aux exigences énoncées dans la présente PC/DPC.

8.1 Fréquences et circonstances des évaluations.

Suite à toute modification significative d'une composante de l'IGC, Datasure procède à une analyse de sécurité et fait évoluer en conséquence, le cas échéant, les mesures techniques et organisationnelles permettant de maintenir ou d'améliorer le niveau de sécurité attendu.
Datasure procède également régulièrement à un contrôle interne de conformité de l'IGC, en tout ou partie. La fréquence de ce contrôle est biannuel en alternance avec l'audit de l'organisme d'évaluation de la conformité.
Datasure fait en effet évaluer, dans le cadre de la certification et qualification de ses services, son IGC conformément à la règlement en vigueur par un organisme d'évaluation accrédité ou autorisé.

8.2 Identités / qualifications des évaluateurs

Concernant l'audit interne, Datasure choisit et assigne une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité contrôlée.
Dans le cadre de la certification et qualification de ses services, Datasure fait appel à un organisme accrédité.

8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit est choisie de façon à assurer une indépendance et une impartialité de l'audit.

8.4 Sujets couverts par les évaluations

L'audit interne couvre l'ensemble des sujets de la présente PC.

8.5 Actions prises suite aux conclusions des évaluations

En cas d'écart ou d'anomalie suite à un audit, qu'il soit un audit interne de conformité ou un audit d'évaluation, un plan de correction sera établi et appliqué

8.6 Communication des résultats

Les résultats des audits internes conformité sont tenus à la disposition de l'organisme d'évaluation.

9 Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

La tarification de la prestation de fourniture de certificat est hors du périmètre de la présente PC/DPC.

9.1.2 Tarifs pour accéder aux certificats

La tarification de la prestation d'accès aux certificats générés est hors du périmètre de la présente PC/DPC.

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

L'accès au LCR, LAR et OCSP est libre et gratuit. En revanche tout abus de sollicitation des serveurs peut faire l'objet d'une limitation technique aux fins de préservation des ressources.

9.1.4 Tarifs pour d'autres services

Non applicable

9.1.5 Politique de remboursement

Non applicable.

9.2 Responsabilité financière

Conformément à ses obligations, l'AC prend les dispositions nécessaires pour couvrir, ses responsabilités liées à ses opérations et/ou activités.

9.2.1 Couverture par les assurances

Datasure déclare avoir les ressources nécessaires pour opérer ses services en toute sécurité et conformité avec la présente PC/DPC et a souscrit une assurance spécifique informatique pour couvrir ses activités [REQ-7.1.1-04/ REQ-7.1.1-05].

9.2.2 Autres ressources

Non applicable

9.2.3 Couverture et garantie concernant les entités utilisatrices

Non applicable

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- la partie non-publique de la DPC de l'AC,
- les clés privées de l'AC, des composantes et des porteurs de certificats,
- les données d'activation associées aux clés privées d'AC et des porteurs,
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les dossiers d'enregistrement des porteurs,
- les causes de révocations, sauf accord explicite du porteur.

9.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'AC appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.
De plus, lorsque ces données sont échangées, l'AC garantit l'intégrité.
L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle met à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales. Elle donne donner l'accès à ces informations au porteur et au MC.

9.4 Protection des données à caractère personnel

9.4.1 Politique de protection des données à caractère personnel

Datasure respecte la réglementation en vigueur, et en particulier le règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit « Règlement Général sur la Protection des Données [RGPD].

9.4.2 Données à caractère personnel

Dans le cadre de l'émission de certificats, les données considérées comme personnelles sont les suivantes :

- les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur) ;
- le dossier d'enregistrement du porteur.

Dans le cadre du processus de signature, les données signées et documents soumis à signature sont des données à caractère personnel [119231-2/ OVR-7.13-02]. Elles ne sont conservées par Datasure que si la conservation est nécessaire [119231-2/ OVR-7.13-03], dans un cadre contractuel par exemple.

9.4.3 Données à caractère non personnel

Sans objet

9.4.4 Responsabilité en termes de protection des données à caractère personnel

La législation en vigueur sur le territoire Français est applicable. Datasure s'assure en cas de sous-traitance que le sous-traitant met en place des mesures appropriées conformément au [119231-2/ OVR-7.13-02/ OVR-7.13-04].

Notification et consentement d'utilisation des données à caractère personnel

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne doivent ni être divulguées ni transférées à un tiers sauf

dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

La législation en vigueur sur le territoire Français est applicable.

9.5 Droits de propriété intellectuelle

La législation en vigueur sur le territoire Français est applicable.

9.6 Interprétations contractuelles et garanties

La présente PC/DPC détermine des différentes obligations des composantes de l'IGC et des différentes parties prenantes. Les obligations des éventuels différents sous-traitants sont décrits dans la partie confidentielle de la DPC [REQ-6.1-04] [119231-2/OVR-6.1-06]
Les obligations communes aux composantes de l'IGC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la présente PC/DPC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC confidentielle leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre 8) et l'organisme d'évaluation,
- respecter les accords ou contrats qui les lient entre elles ou aux porteurs,
  documenter leurs procédures internes de fonctionnement,
- mettre en oeuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1 Autorités de Certification

L'AC a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences du chapitre 4.4 ci-dessus.
- Garantir et maintenir la cohérence de sa DPC confidentielle avec la présente PC/DPC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant de 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'IGC. La relation entre un porteur et l'AC est formalisée par un lien contractuel précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC est responsable de la conformité de la présente Politique de Certification avec les exigences des normes ETSI 319411-1, ETSI EN 319411-2 et des procédures de qualification de l'ANSSI. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC/DPC, par elle-même ou l'une de ses composantes. Elle prend les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et activités et possède la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente PC/DPC.

9.6.2 Service d'enregistrement

9.6.2.1 AE Datasure

l'AE doit :

- conserver et protéger en intégrité et confidentialité, les informations qui lui sont confiées ;
- assurer que les processus de gestion des demandes et révocations de certificats sont conformes aux règles énoncées dans la présente PC.

9.6.2.2 Mandataire de certification

Le MC doit :

- effectuer correctement et de façon indépendante les contrôles d'identité des futurs porteurs de l'entité pour laquelle il est MC,
- respecter les parties de la présente PC/DPC qui lui incombent,
- signaler à l'AC, si possible préalablement mais au moins sans délai, son départ, ou la fin de sa mission de MC.

9.6.3 Porteurs de certificats

Le porteur a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- informer l'AC de toute modification concernant les informations contenues dans son certificat ;
- faire, sans délai, une demande de révocation de son certificat auprès de l'AE, du MC de son entreprise ou de l'AC en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activation).

Des obligations complémentaires sont applicables pour certains types de certificats.

Cas Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	protéger sa clé privée par des moyens appropriés à son environnement, typiquement en conservant de façon sécurisée sa carte-à-puce contenant la clé privée ; protéger ses données d'activation, en particulier ne pas partager le code PIN;
Cas Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	Pas d'exigences supplémentaires

Cas Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	protéger sa clé privée par des moyens appropriés à son environnement, particulièrement, en assurant, le cas échéant, un contrôle d'accès sur son fichier PKCS#12 de signature (installation sur un poste personnel…) et en le protégeant par un mot de passe personnel à l'état de l'art. Le porteur doit également, lorsqu'il crée sa CSR, respecter l'état de l'art en matière cryptographiques et en particulier les recommandations relatives aux caractéristiques des clés de la norme ETSI TS 119 312 [OVR-6.3.5-01].
Cas Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Voir cas Q2
Cas Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les modalités sont similaires au cas Q1.
Cas Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Les modalités sont similaires au cas Q3.
Cas Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Obligation pour le porteur de respecter la norme ETSI EN 319421 ainsi que les exigences de qualification pour l'horodatage.
Cas C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	S'agissant également de l'usage du QSCD à distance, similaire au cas Q2.
Cas C2. Certificat authentification NCP personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	Les modalités sont similaires au cas Q3.
Cas C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	Similaire au cas Q2.
Cas C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Les modalités sont similaires au cas Q3.
Cas B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Similaire au cas Q2.

La relation entre le porteur et l'AC ou ses composantes est formalisée par un engagement du porteur visant à certifier l'exactitude des renseignements et des documents fournis
Ces informations s'appliquent également aux MC.

9.6.4 Utilisateurs de certificats

Les utilisateurs de certificat doivent

- vérifier et respecter l'usage pour lequel un certificat a été émis ;

- pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC/DPC.

9.6.5 Autres participants

9.6.5.1 Service de signature à distance.

Les obligations suivantes s'appliquent au service de signature Datasure [**OVR-6.1-06]**

Cas 2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3 **Cas 4.** QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1 **Cas C1**. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1 **Cas C3.** Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2 **Cas B1s**. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Le service de signature et de gestion de QSCD à distance de Datasure est utilisé pour générer les clés des porteurs et produire les signatures Ce service a pour obligation de respecter les exigences des normes ETSI TS 119431-1 et TS 119431-2 qui lui sont applicables : - De ne créer les clés de signatures qu'à l'intérieur d'un QSCD qualifié et notifié. - De n'utiliser les clés que dans un QSCD qualifié et notifié. - Dans le cas de la signature éphémère, procéder à l'effacement des clés dès la fin du processus de signature et au plus tard à la date d'expiration du certificat. - De ne créer des signatures ou des cachets que dans le cadre d'un processus de signature ou de scellement incluant le consentement et la vérification de l'identité du signataire (ou l'authentification du porteur de cachet) conformément au procédure de l'AC.

9.7 Limite de garantie

Tout certificat commandé doit faire l'objet d'une acceptation par le porteur. Avant la génération du certificat, le RC ou le Porteur doit vérifier que les informations énoncées dans la demande de certificat sont exactes. Après génération, aucune modification des informations ne peut être effectuée par l'AC. Il est donc de la responsabilité du RC ou du Porteur de bien vérifier l'exactitude de ses informations la première fois que cela lui est demandé. A défaut, le RC ou le Porteur devra faire une nouvelle demande de certificat et le certificat généré ne donnera lieu à aucun remboursement, sauf en cas d'erreur dont la responsabilité serait imputé à Datasure.

Sauf dans les cas où Datasure opère le QSCD pour le compte du porteur ou lorsque Datasure délivre un certificat sur support carte-à-puce, l'installation du certificat délivré est sous la responsabilité du porteur.

9.8 Limite de responsabilité

Sous réserve des dispositions d'ordre public applicables, Datasure ne pourra pas être tenue responsable d'une utilisation non autorisée ou non conforme des Certificats, des données d'activation, des LCR ainsi que de tout autre équipement ou logiciel mis à disposition.
Datasure décline en particulier sa responsabilité pour tout dommage résultant :
- d'un emploi des clés et des certificats pour un usage autre que ceux prévus;
- de l'usage de certificats expirés ;
- d'un cas de force majeure

Datasure décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les Certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées.
En aucun cas, Datasure n'intervient, de quelque façon que ce soit, dans les relations contractuelles qui peuvent se nouer entre le Porteur de certificat et le commanditaire de la signature, client de Datasure, notamment quant au contenu des documents soumis à signature ou cachet via le Service de signature électronique Datasure.

9.9 Indemnités

Sans objet

9.10 Durée et fin anticipée de validité de la PC/DPC

9.10.1 Durée de validité

La présent PC/DPC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC/DPC

9.10.2 Fin anticipée de validité

La publication d'une nouvelle version des documents cités au chapitre 1.1 peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC/DPC correspondante. Dans ce cas, cette mise en conformité n'imposera pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité. Enfin, la validité de la PC peut arriver à terme prématurément en cas de cessation d'activité de l'AC.

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 majeur de toute nature intervenant dans la composition de l'IGC, l'AC s'engage à
- A valider en amont ce changement et en identifier les éventuels impacts
- En informer en amont, l'organisme de qualification ainsi que l'organisme d'évaluation

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

Tout amendement de la PC/DPC doit faire l'objet d'une procédure d'approbation et de publication (§1.2.4) [TS 119 431-1/OVR-9-06].

9.12.2 Mécanisme et période d'information sur les amendements

Lorsqu'un amendement de la présente PC/DPC affecterait l'acceptation du service par le porteur de certificat, l'abonné ou l'utilisateur, Datasure notifie le changement au préalable 15 jours avant la publication de la nouvelle PC/DPC. Les changements mineurs, tels que les corrections de coquilles ou précisions ne nécessitent pas une notification préalable [REQ-6.1-09A][TS 119 431-1/OVR-5.2-01] [TS 119 431-2/OVR-9-09].

9.12.3 Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC/DPC étant inscrit dans les certificats finaux qu'elle émet, toute évolution de cette PC.DPC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) se traduit par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences [OVR-5.3-01], [TS 119 431-1/OVR-5.2-01].
En particulier, l'OID de la présente PC/DPC évolue dès lors qu'un changement majeur intervient dans les exigences de la présente PC/DPC.

9.13 Dispositions concernant la résolution de conflits

L'AC Datasure en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles elle fournit des services électroniques de confiance ou d'autres points qui y sont liés [REQ-7.1.1-06]
En particulier, toute réclamation peut être soumis au point de contact indiqué en 1.2.2.

9.14 Juridictions compétentes

La loi applicable est le droit français. En cas de litige entre les parties découlant de l'interprétation, l'application et/ou l'exécution du contrat et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée au tribunal de commerce de Béziers

9.15 Conformité aux législations et réglementations

Datasure se conformes aux lois et règlements en vigueur. En particulier, les pratiques de l'AC sont non-discriminatoires [REQ-7.1.1-02]
De façon générale, Datasure essaye, dans la mesure du possible, de mettre en place des procédures permettant de rendre accessible ses services à l'ensemble des demandeurs et utilisateurs, et prendre en compte les personnes en situation de handicap [REQ-7.1.1-03].

9.16 Dispositions diverses

9.16.1 Accord global

Le présent document contient l'intégralité des clauses régissant l'IGC.

9.16.2 Transfert d'activités

Voir 5.8.

9.16.3 Conséquences d'une clause non valide

En cas d'une clause non valide, les autres clauses ne sont pas remises en question.

9.16.4 Application et renonciation

Aucune renonciation à se prévaloir de l'un de ses droits ne saurait intervenir tacitement. Pour être opposable à l'AC une renonciation doit avoir été formulée par écrit. Une telle renonciation ne saurait constituer une renonciation pour l'avenir aux dits droits

9.16.5 Force majeure

Datasure ne pourra être tenue pour responsable de tout retard ou manquement dans l'exécution de l'une quelconque de ses obligations au titre de la présente PC/DPC, si ledit retard ou manquement est dû à la survenance d'un cas de force majeure habituellement reconnu par la jurisprudence des Cours et tribunaux français.

9.17 Autres dispositions

Sans objet