Conditions Générales d'Utilisation du service de signature, de cachet et d'émission de certificats

V 1.3

Niveau de confidentialité : public

Datasure

L'historique du document est dans le tableau suivant :

version	Date	Commentaire	Auteur
1.0	09/07/2024	Version initiale du document	Datasure
1.1	07/09/2024	Inclusion du périmètre signature suite atelier cadrage périmètre avec auditeur	F. de Vaulx
1.2	14/10/2024	Prise en compte des remarques de l'auditeur. Intégration d'exigences des normes de signatures	DataSure
1.3	10/11/2024	Prise en compte des remarques de l'auditeur	Datasure

1 Intégralité du présent accord

Le présent accord ne représente pas l'intégralité de l'accord entre l'AC et les porteurs de certificats (la notion de porteur et d'abonnée est confondue), signataires et utilisateurs de certificats.
L'intégralité des obligations et engagement de l'AC et, le cas échéant du service de signature Datasure sont décrits dans sa Politique de Certification / Déclaration des pratiques de certification publiques.
Les présentes CGU complètent la Politique de certification de l'AC, les CGV et CGU du site Datasure.

2 Objet

Le présent document décrit les Conditions Générales d'Utilisation à destination des abonnés, porteurs de certificats, signataires et utilisateurs souhaitant

- utiliser l'AC Datasure et le service de signature et de gestion de QSCD de Datasure. et
- vérifier les certificats émis par Datasure.

Avant toute utilisation du Service, l'Utilisateur reconnaît :

- Avoir pris connaissance des présentes CGU ;
- Disposer de la capacité juridique et des habilitations pour s'engager au titre des présentes CGU
- Accepter sans réserve les présentes CGU.

L'acceptation est matérialisée en cliquant sur la case à cocher lors de la création d'un compte d'Utilisateur, d'une signature électronique, ou de la signature d'un devis/contrat comportant les CGUs en Annexe.

Les CGU sont mises à sa disposition par l'AC Datasure sur son site de publication. Elles peuvent être téléchargées au format PDF.

3 Informations 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

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

4 Service d'émission de certificats

Le Service d'émission de certificat permet d'obtenir un certificat électronique pour diverses finalités après des vérifications effectuées par l'autorité d'enregistrement.

4.1 Accès au service

L'accès au Service nécessite de disposer d'équipements logiciels et matériels adaptés pour accéder au Service ; Ces équipements diffèrent selon le type de certificats

4.1.1 Accès au service par API

Offre Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1 1.3.6.1.4.1.58753.4.1.1.1.1.2.1	L'utilisation du Service au moyen de l'API nécessite la configuration du système d'information de l'abonné selon les prescriptions de la Documentation API.

4.1.2 Accès au service par le navigateur

Les autres offres nécessitent d'avoir un navigateur internet récent (Edge, Safari, Chrome ou Firefox par exemple). Certain moyens d'identification à distance peuvent nécessiter des équipements supplémentaires (téléphone portable muni d'une caméra, connexion 4G…) décrit dans les conditions générales du service.

4.2 Moyen d'identification proposés

Offre Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	Les moyens d'identification proposés sont : - Procédure d'identification PVID
Offre Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3 1.3.6.1.4.1.58753.4.1.1.1.1.1.3	Les moyens d'identification proposés sont : - Procédure d'identification PVID
Offre Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	Les moyens d'identification proposés sont : - Procédure d'identification PVID
Offre Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1 1.3.6.1.4.1.58753.4.1.1.1.1.2.1	Les moyens d'identification du demandeur représentant la personne morale sont : - Procédure d'identification PVID
Offre Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	Les moyens d'identification du demandeur représentant la personne morale sont : - Procédure d'identification PVID
Offre Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Les moyens d'identification du demandeur représentant la personne morale sont : - Procédure d'identification PVID
Offre Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Les moyens d'identification du demandeur représentant la personne morale sont : Procédure d'identification PVID
Offre C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1 1.3.6.1.4.1.58753.4.1.1.1.2.1.1	Les moyens d'identification proposés sont : - Procédure d'identification à distance automatisée impliquant une vérification de la pièce d'identité présentée, une correspondance biométrique des visages entre la photo de la pièce d'identité et une prise de vue du porteurs ainsi qu'une analyse du caractère vivant de ce dernier
Offre C2. Certificat authentification NCP personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	Les moyens d'identification proposés au demandeur représentant la personne morale sont : - Procédure d'identification à distance automatisée impliquant une vérification de la pièce d'identité présentée, une correspondance biométrique des visages entre la photo de la pièce d'identité et une prise de vue du porteurs ainsi qu'une analyse du caractère vivant de ce dernier
Offre C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2 1.3.6.1.4.1.58753.4.1.1.1.2.1.2	Les moyens d'identification proposés sont : - La soumission d'une copie de la pièce d'identité
Offre C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Les moyens d'identification du demandeur représentant la personne morale proposés sont : - La soumission d'une copie de la pièce d'identité
Offre B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1 1.3.6.1.4.1.58753.4.1.1.1.3.1.1	Le porteur est authentifié par tous moyens permettant d'avoir un faisceau d'indices sur son identité (par exemple SMS, signature manuscrite, etc.)

4.3 Acceptation du certificat

L'acceptation du certificat est réalisée de façon explicite.

Offre 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 bouton « accepter ». Le porteur dispose de 15 jours pour accepter son certificat après la vérification effective de son identité.
Offre Q2. QCP-n-QSCD (à distance) 1.3.6.1.4.1.58753.2.1.1.1.1.1.3 1.3.6.1.4.1.58753.4.1.1.1.1.1.3	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.
Offre Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	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'un bouton « accepter ». Le porteur dispose de 15 jours pour accepter son certificat après la vérification effective de son identité.
Offre Q4. QCP-l-QSCD (à distance) 1.3.6.1.4.1.58753.2.1.1.1.1.2.1 1.3.6.1.4.1.58753.4.1.1.1.1.2.1	L'acceptation du certificat est réalisée avant l'installation de celui-ci sur le dispositif de gestion de création de cachet qualifié à distance de Datasure. Les données contenues dans le certificat généré sont présentées au porteur qui accepte celui-ci à l'aide d'un bouton « accepter ». L'acceptation du certificat doit se faire au maximum une heure après la fin du processus PVID.
Offre Q5. QCP-l-QSCD (sur carte à puce) 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	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'un bouton « accepter ». Le porteur dispose de 15 jours pour accepter son certificat après la vérification effective de son identité.
Offre Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	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'un bouton « accepter ». Le porteur dispose de 15 jours pour accepter son certificat après la vérification effective de son identité. .

Offre 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 nécessairement implicite. Le responsable de certificat vérifie son contenu avant installation sur la TSU.
Offre C1. NCP+ personne physique (à distance) 1.3.6.1.4.1.58753.2.1.1.1.2.1.1 1.3.6.1.4.1.58753.4.1.1.1.2.1.1	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 de vérification d'identité..
Offre C2. Certificat authentification NCP personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	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'un bouton « accepter ». Le porteur dispose de 15 jours pour accepter son certificat après la vérification effective de son identité.
Offre C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2 1.3.6.1.4.1.58753.4.1.1.1.2.1.2	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 de vérification d'identité.
Offre C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	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'un bouton « accepter ». Le porteur dispose de 15 jours pour accepter son certificat après la vérification effective de son identité.
Offre B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1 1.3.6.1.4.1.58753.4.1.1.1.3.1.1	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.

5 Service de signature et de cachet

Datasure, pour certaines de ses offres, opère pour le compte du porteur le service de signature ou de cachet électronique à distance en mettant en œuvre la clé privée de ce dernier. Ce service concerne exclusivement les offres suivantes :

Offre Q2. QCP-n-QSCD signature à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3 1.3.6.1.4.1.58753.4.1.1.1.1.1.3

Offre Q4. QCP-l-QSCD cachet à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1 1.3.6.1.4.1.58753.4.1.1.1.1.2.1
Offre C1. NCP+ personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.1 1.3.6.1.4.1.58753.4.1.1.1.2.1.1
Offre C3. LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2 1.3.6.1.4.1.58753.4.1.1.1.2.1.2
Offre B1 . Biométrie – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.3.1.1 1.3.6.1.4.1.58753.4.1.1.1.3.1.1

Ces services ne peuvent être souscrit sans souscription conjointe au service de signature ou de cachet correspondant.

5.1 Opérations réalisées par le service de création de signature ou de cachet à distance pour le compte du Client

Datasure réalise, pour le compte du signataire, les opérations suivantes :

- Génération de la biclé dans un dispositif QSCD à distance ;
- Génération de la demande de certificat (CSR) au nom du signataire depuis le QSCD et soumission à l'AC avec les données d'identification ;
- Récupération du certificat et installation du certificat sur le dispositif de création de signature ou de cachet à distance ;
- Création d'une signature électronique ou d'un cachet électronique à l'aide de la clé privée et du certificat à la demande du signataire et après identification ou authentification de celui-ci.

5.2 Accès au service

5.2.1 Accès au service par API (certificats de cachet à distance)

Offre Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1 1.3.6.1.4.1.58753.4.1.1.1.1.2.1	Le porteur adresse au Service le document à sceller ou l'empreinte de la donnée à signer, par le biais de l'API, conformément à la Documentation. Le Service adresse en réponse à la requête du porteur le document signé (PAdES) ou directement la signature (hash signing).

	Le porteur est préalablement authentifié à l'aide du moyen d'authentification associé à sa clé privé. Ce moyen d'authentification permet de conserver la clé sous le contrôle du porteur.

5.2.2 Accès au service au travers de l'interface de signature

Offre Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3 1.3.6.1.4.1.58753.4.1.1.1.1.1.3	L'utilisation du service de signature se fait de façon conjointe au processus d'émission de certificat. Le document à signer est présenté au signataire qui peut le consulter et donne explicitement son consentement à signer au moyen d'une case à cocher. Il confirme l'opération par un envoi de code unique reçu sur un dispositif sous son contrôle. Le signataire réalise alors la procédure d'enregistrement afin d'obtenir son certificat. Immédiatement après la validation de l'identité et l'émission du certificat, la signature électronique est créée. La Signature est au format PAdES-T a minima. Il n'y a pas de paramètre spécifiques relatifs à la signature. Les augmentations LT et LTA peuvent être mises en œuvre. Dans le cadre de la signature, il n'est pas possible de fournir uniquement le haché.
Offre C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1 1.3.6.1.4.1.58753.4.1.1.1.2.1.1	
Offre C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2 1.3.6.1.4.1.58753.4.1.1.1.2.1.2	
Offre B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1 1.3.6.1.4.1.58753.4.1.1.1.3.1.1	

.

5.3 Disponibilité

Datasure propose un niveau de 99,5% mensuel dans le cadre des presentes CGUs.

5.4 Limite du service

Seul le service de signature Datasure et le QSCD managé associé peuvent être utilisés dans le cadre de ce service. Seul la signature PAdES est supporté par le service. Le cachet est limité aux formats PAdES et aux signatures cryptographiques.

6 Type de certificats et usages

Le service d'émission de certificat est opéré conformément aux normes suivantes :

Offre Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	ETSI 319411-2 niveau QCP-n-QSCD Procédure du qualification ANSSI
Offre Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.1.3	ETSI 319411-2 niveau QCP-n-QSCD Procédure du qualification ANSSI
Offre Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.1.2	ETSI 319411-2 niveau QCP-n Procédure du qualification ANSSI
Offre Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	ETSI 319411-2 niveau QCP-l-QSCD Procédure du qualification ANSSI
Offre Q5. QCP-l-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.2.1	ETSI 319411-2 niveau QCP-l-QSCD Procédure du qualification ANSSI
Offre Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	ETSI 319411-2 niveau QCP-l Procédure du qualification ANSSI
Offre Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	ETSI 319411-2 niveau QCP-l Procédure du qualification ANSSI
Offre C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1	ETSI 319411-1 niveau NCP+
Offre C2. Certificat authentification NCP personne morale (certificat logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.1	ETSI 319411-1 niveau NCP
Offre C3 Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2	ETSI 319411-1 niveau LCP
Offre C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	ETSI 319411-1 niveau LCP
Offre B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1	Non applicable

7 Limites d'utilisation

Les événements relatifs à l'émission d'un certificats sont conservés pendant une période de 7 ans après l'expiration du certificat, conformément aux exigences de l'ANSSI.

Datasure ne vérifie pas l'adéquation du service fourni avec la réglementions applicable au porteur. En particulier, Datasure n'est pas habilité à traiter des données de santé ou des données relevant de la diffusion restreinte ou du confidentiel défense. A ce titre, Datasure décline toute responsabilité en cas d'utilisation non adéquate de son service.

8 Obligations du porteur relatives au service d'émission de certificat

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'Autorité d'enregistrement (AE), du Mandataire de certification (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.

Offre Q1. QCP-n-QSCD sur carte à puce 1.3.6.1.4.1.58753.2.1.1.1.1.1.1	• utiliser exclusivement la carte-à-puce QSCD ; • 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.
Offre Q2. QCP-n-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.3 1.3.6.1.4.1.58753.4.1.1.1.1.3	L'exigence de révocation n'est pas applicable (certificat éphémère)
Offre Q3. QCP-n (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2	• 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 et conforme aux préconisations de l'ANSSI. • 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
Offre Q4. QCP-l-QSCD à distance 1.3.6.1.4.1.58753.2.1.1.1.1.2.1 1.3.6.1.4.1.58753.4.1.1.1.1.2.1	Pas d'exigences supplémentaires.
Offre 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 à l'offre Q1.

Offre Q6. QCP-l (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.1.2.2	Les modalités sont identiques à l'offre Q3.
Offre Q7. QCP-l (horodatage) 1.3.6.1.4.1.58753.2.1.1.1.1.2.3	Obligation pour le responsable de certificat de respecter la norme ETSI EN 319421 ainsi que les exigences de qualification pour l'horodatage.
Offre C1. Certificat signature NCP+ personne physique 1.3.6.1.4.1.58753.2.1.1.1.2.1.1 1.3.6.1.4.1.58753.4.1.1.1.2.1.1	L'exigence de révocation n'est pas applicable (certificat éphémère)
Offre 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 identiques à l'offre Q3.
Offre C3. Certificat LCP personne physique – signature à distance 1.3.6.1.4.1.58753.2.1.1.1.2.1.2 1.3.6.1.4.1.58753.4.1.1.1.2.1.2	L'exigence de révocation n'est pas applicable (certificat éphémère)
Offre C4. Certificat LCP personne morale (logiciel) 1.3.6.1.4.1.58753.2.1.1.1.2.2.2	Les modalités sont identiques à l'offre Q3.
Offre B1. Certificat Biométrie 1.3.6.1.4.1.58753.2.1.1.1.3.1.1 1.3.6.1.4.1.58753.4.1.1.1.3.1.1	L'exigence de révocation n'est pas applicable (certificat éphémère)

En souscrivant au service, le porteur accepte également :

- l'ensemble des obligations suscitées, y compris l'obligation d'utiliser un QSCD pour les offres où celui-ci est nécessaire ;
- que Datasure conserve son dossier d'enregistrement et les traces de sa délivrance de certificat, et le cas échéant, les traces de cycle de vie des clés du QSCD, pour la durée légale indiquée dans les présentes CGUs, ainsi que les traces liées au processus de révocation, le cas échéant ;
- Qu'en cas d'arrêt d'activité, ces éléments puissent être transmis à un tiers en assurant sa conservation.

Datasure ne réalise pas de publication de certificats.

9 Obligations relatives à la vérification des certificats

Il est recommandé à l'utilisateur, en plus de la validation de la signature électronique, de vérifier le certificat de signature électronique ou de cachet électronique apposé. Les informations permettant de vérifier ces certificats sont disponibles sur le site de Datasure.

Le Service mis à la disposition de l'utilisateur par l'AC permet :

- D'obtenir l'ensemble des certificats de la chaîne de certification jusqu'à l'AC Racine ;
- D'obtenir les listes de certificats révoqués (LCR). Les LCR sont conformes à la norme IETF RFC 5280.

Le service est disponible, en fonctionnement normal, 24h/24 et 7J/7 selon les conditions prévues par la Politique de Certification de l'AC. Datasure met également à disposition un service de répondeur OCSP.

L'utilisateur souhaitant utiliser un certificat électronique émis par l'AC Datasure est tenu de s'assurer de l'utilisation appropriée des informations contenues dans le certificat, notamment en :

- 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 PC/DPC.

Ces vérifications peuvent être réalisées de façon automatique par des outils standards du marché tels que Acrobat Reader™ ou les bibliothèques Open-Source SD-DSS (fournies par la Commission européenne) et OpenSSL.

Conformément à la PC, cas de fin de vie, concernant le statut de révocation :

- 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.

10 Rétention des traces

L'ensemble des traces relatives aux services de confiance sont conservées pendant une période de 7 ans après expiration du certificat conformément aux exigences de l'ANSSI**.**

11 Limites de responsabilité.

La responsabilité de Datasure ne pourra être engagée en cas de non-respect par le porteur ou l'utilisateur des présentes conditions contractuelles.

En particulier, la responsabilité de Datasure ne pourra être engagée en cas d'inadéquation entre le niveau offert par le service, tel que décrit dans les présentes conditions et dans la politique du service, et les besoins de sécurité attendu par le client ou l'utilisateur.

Le service d'émission de certificat de Datasure se limite à la mise à disposition d'un dispositif technique aux porteurs et utilisateurs. La responsabilité de Datasure ne pourra être engagée en cas d'usage du service par le porteur ou l'utilisateur à des fins illégales ou non-conformes à la réglementation.

De même, Datasure ne pourra être tenu responsable des dommages, directs ou indirects causés par la divulgation des moyens de connexion fournis pour accéder au service.

Datasure ne pourra être tenu responsable d'aucun dommage indirect découlant de l'utilisation du service et en tout état de cause, la responsabilité sera limitée à hauteur du montant versé à Datasure pour l'obtention du certificat de signature électronique et le cas échéant, pour la réalisation d'un processus de signature.

Les informations nécessaires à la mise en œuvre de la procédure de vérification des
des signatures et certificats sont disponibles sur le Site de publication de Datasure.

En cas d'évènement affectant la sécurité du Service et qui pourraient entraîner une conséquence sur les certificats, les signatures ou les cachets, une information appropriée sera mise à la disposition des Utilisateurs via le Site de publication de Datasure.

12 Politiques applicables

Les politiques applicables pour chacune des offres sont précisées dans le tableau suivant.

Offre Q1. QCP-n-QSCD sur carte à puce	Certification : 1.3.6.1.4.1.58753.2.1.1.1.1.1.1
Offre Q2. QCP-n-QSCD à distance	Certification : 1.3.6.1.4.1.58753.2.1.1.1.1.1.3 Signature : 1.3.6.1.4.1.58753.4.1.1.1.1.1.3
Offre Q3. QCP-n (logiciel)	Certification : 1.3.6.1.4.1.58753.2.1.1.1.1.1.2
Offre Q4. QCP-l-QSCD à distance	Certification : 1.3.6.1.4.1.58753.2.1.1.1.1.2.1 Signature : 1.3.6.1.4.1.58753.4.1.1.1.1.2.1
Offre Q5. QCP-l-QSCD sur carte à puce	Certification : 1.3.6.1.4.1.58753.2.1.1.1.1.2.1
Offre Q6. QCP-l (logiciel)	Certification : 1.3.6.1.4.1.58753.2.1.1.1.1.2.2
Offre Q7. QCP-l (horodatage)	Certification : 1.3.6.1.4.1.58753.2.1.1.1.1.2.3
Offre C1. Certificat signature NCP+ personne physique	Certification : 1.3.6.1.4.1.58753.2.1.1.1.2.1.1 Signature : 1.3.6.1.4.1.58753.4.1.1.1.2.1.1
Offre C2. Certificat authentification NCP personne morale (certificat logiciel)	Certification : 1.3.6.1.4.1.58753.2.1.1.1.2.1.1
Offre C3. Certificat LCP personne physique – signature à distance	Certification : 1.3.6.1.4.1.58753.2.1.1.1.2.1.2 Signature : 1.3.6.1.4.1.58753.4.1.1.1.2.1.2
Offre C4. Certificat LCP personne morale (logiciel)	Certification : 1.3.6.1.4.1.58753.2.1.1.1.2.2.2
Offre B1. Certificat Biométrie	Certification : 1.3.6.1.4.1.58753.2.1.1.1.3.1.1 Signature : 1.3.6.1.4.1.58753.4.1.1.1.3.1.1

13 Politique de protection des données à caractère personnel

La politique générale de protection de données à caractère personnel de Datasure est applicable.

En particulier :

- Datasure ne réalise aucune analyse du contenu sémantique des documents fournis. Un haché est calculé sur le document à des fins de création de la signature électronique
- Datasure n'utilise les données à caractères fournies, en particulier les données d'enregistrement, que dans la stricte finalité de la gestion de certificats et des signatures.

14 Politique de remboursement

Il n'est pas prévu de remboursement.

15 Disponibilité

L'engagement de disponibilité du service d'émission de certificat fourni est 99.5% mensuel.
L'engagement de disponibilité du service de gestion de dispositif de création de signature ou cachet à distance est 99,5% mensuel.

16 Loi applicable

La loi applicable est la loi française.
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, la compétence exclusive est attribuée au Tribunal de commerce de Béziers et en tout état de cause aux juridictions de la Cour d'appel de Montpellier.

17 Procédure en cas de litige

En cas de litige, les parties chercheront un accord à l'amiable. A ce titre, Datasure pourra être contacté au point de contact mentionné dans la politique de certification et rappelé dans les présentes.

18 Conformité et audit

Le comité de Direction de Datasure procède à la validation de la conformité du service par rapport à ses engagements inscrits dans la PC.

Un contrôle de conformité est réalisé lors de la mise en service au travers d'une homologation de sécurité du service. De plus, un audit interne sera réalisé au moins tous les deux ans, en alternance avec l'audit biannuel d'évaluation de la conformité.

Dans le cadre d'obtention de la qualification eIDAS de ces services de confiance, l'audit d'évaluation de la conformité est réalisé par une société externe dûment accréditée ou autorisée, et la qualification est demandée auprès de l'organe de contrôle national, l'ANSSI.

Pour les certificats qualifiés, la procédure de qualification de l'organe de contrôle national induit la conformité :

- Aux normes ETSI EN 319401, ETSI EN 319411-1 et ETSI EN 319411-2 ;
- Aux exigences complémentaires énoncées dans ladite procédure de qualification, en particulier les exigences relatives aux dispositifs cryptographiques.