POLITIQUE de gestion de QSCD à distance
Fourniture d'un Service d'Application de Signature Serveur (SSASP)

EMETTEUR	DESTINATAIRES	COPIES
CERTINOMIS	PUBLIC	

Certinomis

Docaposte Certinomis SAS au capital de 40 156 euros.

Siège social : 45-47, Boulevard Paul Vaillant-Couturier

94200 Ivry sur Seine – France. RCS Créteil B 433 998 903

Historique des versions

DATE	VERSION	EVOLUTION	AUTEUR
30/09/2025	0.1	Création du document	Y. THOMASSIER
23/12/2025	1.0	Document initial	Y. THOMASSIER

Table des matières

AVERTISSEMENT

1 INTRODUCTION

1.1 PRESENTATION GENERALE

1.1.1 Service SEQ Certinomis

Le Service SEQ (Signature Electronique Qualifiée) de Docaposte Certinomis est utilisé par des applications de création de signature (SCA) afin de produire le calcul de la signature électronique qualifiée du condensat d'un document.

Pour ce faire, le Service génère et assure le cycle de vie de la clé privée de signature d'un particulier ou d'un professionnel (Signataire).

Le Service SEQ est en relation avec le Service d'émission de certificat de signature qualifié d'une AC, pour lequel il assure la gestion des clés privées associées aux clés publiques que ce dernier a certifiés.

1.1.2 Objet du document

Le document décrit la Politique du Service d'Application de Signature Serveur appliquée au Service SEQ fourni par Docaposte Certinomis.

La Politique couvre la gestion de la bi-clé de signature au nom d'un Signataire, associée au certificat de signature délivré par l'AC Certinomis, au sein d'un dispositif cryptographique à distance (HSM) de niveau QSCD.

La Politique couvre également l'usage exclusif de la clé privée de signature par le Signataire, pour le calcul le de la valeur cryptographique de signatures électroniques de condensats (hash) de documents électroniques.

La Politique est conforme à l'annexe A du standard de l'[ETSI 119 431-1].

1.2 IDENTIFICATION DU DOCUMENT

La désignation du numéro d'identification d'objet (OID) du présent document est : 1.2.250.1.86.7.1.1.1

Ce document couvre une seule Politique d'Application de Serveur de Signature, pour laquelle un OID a été attribué.

La Politique ETSI adoptée comme base est précisée dans le tableau ci-dessous.

OID	*Usage*	*Conformité ETSI / RGS*
1.2.250.1.86.7.1.1.1	Politique qualifiée de Gestion de QSCD à distance de production	EUSPv2 : 0.4.0.19431.1.1.4

1.3 ENTITES INTERVENANT DANS LE SERVICE

1.3.1 Fournisseur de Service d'Application de Signature Serveur

La société Docaposte Certinomis est le Fournisseur de Service d'Application de Signature Serveur (SSASP).

La société Docaposte Agility lui fournit le Service d'identification et d'authentification du Signataire d'une clé privée de signature. L'identification et l'authentification sont réalisées par différents moyens techniques, selon l'usage.

La société Docaposte Certinomis est également prestataire de Service de certification électronique qualifié (PSCE) au sens du RGS et du règlement eIDAS. Elle gère au travers de ce Service qualifié, les certificats de signature qualifiés des Signataires, associés aux bi-clés gérées dans le QSCD distant.

1.3.2 Les Souscripteurs du Service et les Signataires

Les entités clientes de Docaposte Certinomis (Souscripteurs) s'interfacent au travers d'API avec le Service et mettent en œuvre des applications de création de signature (SCA) au sens du standard [ETSI 119431-1] .

Les SCA interagissent avec le Service afin de lui demander :

- La création d'une bi-clé au sein du QSCD distant, pour un Signataire dûment identifié et authentifié par le Service;
- Le calcul cryptographique d'une signature électronique, pour un Signataire dûment authentifié, sur la base d'un condensat de document fourni (hash), en utilisant la clé privée du Signataire gérée au sein du QSCD distant.

Les Signataires sont des clients des Souscripteurs du Service. Celui-ci leur garantit l'accès exclusif à leur clé privée de signature associée à leur certificat de signature qualifié, stockée dans le QSCD distant,

1.4 USAGE DU SERVICE

Le Service est consommé par des applications de création de signature (SCA), en relation contractuelle avec Docaposte Certinomis et produit une signature qualifiée au sens du règlement eIDAS v2.

1.5 GESTION DE LA POLITIQUE

La présente Politique s'applique au Service SEQ de gestion de QSCD à distance de Docaposte Certinomis.

La présente Politique est revue et mise à jour annuellement.

1.5.1 Entité gérant la Politique

La présente Politique de Service du Service d'Application de Signature Serveur est sous la responsabilité de la société Docaposte Certinomis.

1.5.2 Point de contact

Le directeur général de Certinomis

45-47, Boulevard Paul Vaillant-Couturier

94200 Ivry sur Seine

Téléphone : 0810 184 956

Courrier électronique : ld-Politiquecertification@certinomis.fr

1.5.3 Entité déterminant la conformité d'une DPSSAS avec cette Politique

La Direction de Certinomis détermine la conformité de la Déclaration des Pratiques de Service du Service d'Application de Signature Serveur (DPSSAS) avec la Politique PSSAS, soit directement soit indirectement en faisant appel à des experts indépendants spécialisés dans le domaine de la sécurité et des Services de confiance.

La Direction de Docaposte Certinomis a désigné parmi les collaborateurs de l'entreprise, un responsable de la conformité, en charge entre autres d'effectuer une veille régulière de l'évolution des exigences du règlement eIDAS et des standards de l'ETSI référencés par les actes d'exécution de ce règlement.

1.5.4 Procédures d'approbation de la conformité de la DPSSAS

Docaposte Certinomis est garante de l'application de la DPSSAS avec la Politique PSSAS.

Docaposte Certinomis est responsable de la gestion (mise à jour, révisions) de la DPSSAS. Toute demande de mise à jour de la DPSSAS suit le processus d'approbation mis en place.

Une instance de l'Autorité de Gestion des Politiques (AGP) peut demander l'examen de la DPSSAS conformément aux procédures en vigueur.

1.6 DEFINITIONS ET ACRONYMES

1.6.1 Acronymes

Les acronymes utilisés dans la présente Politique sont les suivants :

- AC Autorité de Certification
- AE Autorité d'Enregistrement
- API Application Programming Interface
- AGP Autorité de Gestion des Politiques
- CC Common Criteria
- DPSSAS Déclaration des Pratiques du Service d'Application de Signature Serveur (SSAS)
- ECDSA Elliptic Curve Digital Signature Algorithm
- ETSI European Telecommunications Standards Institute
- IDP IDentity Provider
- OID Object Identifier
- PKI Public Key Infrastructure
- PSSAS Politique du Service d'Application de Signature Serveur (SSAS)
- PSCE Prestataire de Services de Certification Electronique
- PVID Prestataire de vérification de l'Identité à Distance
- QSCD Qualified Signature Creation Device
- RSA Rivest Shamir Adelman
- SAD Signature Activation Data
- SAP Signature Activation Protocol
- SCA Signature Creation Application
- SAM Signature Activation Module
- SSI Sécurité des Systèmes d'Information
- SSAS Service du Service d'Application de Signature Serveur (SSAS)
- URL Uniform Resource Locator

1.6.2 Définitions

Autorité de Certification (AC) :

Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une Politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette Politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre 1.1 et le terme d'AC est le seul utilisé. Il désigne Docaposte Certinomis chargée de l'application de la Politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

Autorité de Gestion de la Politique (AGP) :

L'Autorité de Gestion de la Politique, pour les usages qui la concerne, établit les besoins et les exigences en termes de sécurité dans l'ensemble du processus de certification et d'utilisation des certificats. Elle établit des lignes directrices, qui peuvent prendre la forme d'un canevas de Politique que doivent respecter toutes les

Autorités de Certification qu'elle accrédite. Elle valide et suit toute évolution des Politiques de certification des Autorités de Certification qu'elle accrédite.

Son rôle est celui d'une autorité morale qui indique par l'accréditation la confiance que l'on peut accorder à une Autorité de Certification.

Certificat :

Attestation électronique liant les données afférentes au chiffrement ou à la vérification de signature, des échanges, messages et documents électroniques à un sujet, afin d'en assurer la confidentialité ou d'en assurer l'authentification et l'intégrité.

Signataire

Personne physique, identifiée conformément à la PC du Certificat, et authentifiée par le fournisseur d'identité (IDP), qui possède une paire de clés de signature générée par le SERVICE et qu'il utilise, sous son contrôle exclusif, pour effectuer la signature électronique de document.

Souscripteur

Personne morale qui contracte Docaposte Certinomis l'usage du Service d'Application de Signature Serveur, afin de l'interfacer au travers d'API, avec son application de création de signature (SCA).

Politique :

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

Déclaration des Pratiques d'Application de Serveur de Signature (DPSSAS) :

Une DPSSAS identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que le SERVICE applique dans le cadre de la fourniture de ses Services d'Application de Serveur de Signature aux usagers et en conformité avec la ou les Politiques d'Application de Serveur de Signature qu'elle s'est engagée à respecter.

Prestataire de Services de certification électronique (PSCE) :

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

Service :

Désigne le Service d'Application de Serveur de Signature, au sens du standard ETSI 119 431-1, opéré par Docaposte Certinomis.

Docaposte Certinomis SAS au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1 ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

Les informations sont mises à disposition par Docaposte Certinomis , au travers de son site internet https://www.certinomis.com.

2.2 INFORMATIONS DEVANT ETRE PUBLIEES

Docaposte Certinomis a pour obligation de publier au minimum les informations suivantes à destination des utilisateurs de son Service :

- La présente Politique
-

2.3 DELAIS ET FREQUENCES DE PUBLICATION

Les informations liées au Service doivent être publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs du prestataire de Service.

En particulier, toute nouvelle version doit être communiquée aux Souscripteurs (SCA clientes du Service) avec un préavis raisonnable avant sa publication. Les systèmes publiant ces informations doivent au moins être disponibles les jours et heures ouvrés.

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées est libre d'accès en lecture.

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de Docaposte Certinomis, au moins au travers d'un contrôle d'accès de type mots de passe longs basé sur une Politique de gestion stricte des mots de passe.

3 INITIALISATION DE LA CLE DE SIGNATURE

3.1 GENERATION DE LA CLE DE SIGNATURE

Les clés privées de signature des Signataires doivent être générées dans un dispositif matériel de niveau QSCD (certifié conforme à la norme EN 419 241-5).

Les clés privées de signature ainsi générées doivent demeurer dans le dispositif matériel. Un protocole sécurisé, partie intégrante de la cible de sécurité du dispositif matériel, doit permettre la synchronisation des clés entre tous les dispositifs matériels composant le Service.

Les modules des bi-clés de signature doivent être calculés selon l'algorithme RSA ou ECDSA, et doivent être d'une longueur de 3072 ou 4096 bits pour RSA et a minima P-256 pour ECDSA.

La paire de clés de signature d'un Signataire est générée par le Service et concomitamment, le certificat de signature correspondant doit être signé par l'AC du PSCE.

Dans le cas des certificats éphémères (durée de vie de 30 minutes), la paire de clés de signature du Signataire doit être générée et utilisée au cours de la même et unique session de signature.

3.2 MOYEN D'IDENTIFICATION

Le Signataire doit être identifié par l'AC conformément à la PC du Certificat (par exemple au travers d'un Service d'identification fourni par un PVID qualifié, d'un MIE de niveau élevé, ou lors d'une vérification d'identité en face à face). Il devra accepter les CGU de l'AC avant de se voir délivrer son certificat de signature.

Le Signataire doit être authentifié avant de signer soit :

- à l'aide de l'application de l'Identité Numérique de LA POSTE (INLP) (identité numérique notifiée au niveau substantiel)
- à l'aide d'un OTP / SMS transmis sur son téléphone mobile et renseigné au sein d'une même session fonctionnelle
- à l'aide d'un OTP / SMS transmis sur son téléphone mobile et renseigné sous le contrôle d'un Notaire.

Ces moyens d'authentification nécessitent l'enrôlement préalable par l'AC de l'identifiant de l'INLP ou du téléphone mobile du Signataire.

L'authentification peut être déléguée à un IDP externe et doit dans tous les cas aboutir à un jeton d'accès contenant un identifiant unique pour le Signataire.

L'IDP doit assurer la correspondance entre l'identification portée par le moyen d'authentification utilisé par le Signataire et l'identité associée à son certificat de signature.

Dans le cas où l'authentification du Signataire est déléguée à un IDP externe, l'authentification auprès du module SAM du QSCD doit être réalisée au moyen d'un jeton, dérivé du jeton d'identification délivré par l'IDP et signé par une clé de signature résidant dans un HSM.

Le cas échéant, Docaposte Certinomis doit s'assurer de la couverture des exigences qui incombent à l'IDP externe.

Dans le cas des certificats éphémères, l'identification, la génération de la clé et l'authentification du Signataire doivent être réalisées au sein d'une même session fonctionnelle

3.3 LIEN AVEC LE CERTIFICAT DE SIGNATURE

Le certificat de signature du Signataire et sa clé privée de signature doivent être associés dans le QSCD du Service.

La signature électronique réalisée par le Signataire au moyen de sa clé privée, doit être produite après l'émission de son certificat de signature par l'AC.

La PKI de l'AC ainsi que le module SAM du QSCD doivent assurer l'intégrité de la clé de signature et du certificat correspondant.

3.4 FOURNITURE DU MOYEN D'IDENTIFICATION

Sans Objet, Docaposte Certinomis ne fournit pas de moyen d'identification aux Signataires.

4 CYCLE DE VIE DE LA CLE DE SIGNATURE

4.1 ACTIVATION DE LA SIGNATURE

L'activation de la clé privée de signature du Signataire doit être réalisée sous le contrôle exclusif de celui-ci.

L'activation de la clé privée nécessite une authentification du Signataire réussie. L'activation de la signature doit faire suite nécessairement à une action explicite du Signataire, dans le but de procéder à la signature électronique de documents.

Les données d'activation (SAD) doivent être envoyées directement au module SAM du QSCD. Un SAD peut contenir les références de plusieurs documents qui seront signés au cours de la même session.

Le protocole d'activation (SAP) doit garantir que la signature sera produite sur la base de données envoyées par le Signataire, associées à sa clé privée de signature.

Le jeton d'accès à la clé privée doit contenir l'identifiant unique du Signataire ainsi que la référence de son émetteur.

La demande de signature doit provenir d'une SCA avec laquelle Docaposte Certinomis est en relation contractuelle. Le consentement du Signataire de la clé privée, au travers des CGU de la SCA, encadre l'usage pour la signature électronique.

Les algorithmes retenus doivent être réputés fiables pour la signature électronique. Les clés RSA dont la longueur du module est strictement supérieure à 2048 bits ainsi que les clés ECDSA dont l'algorithme est a minima P-256 sont réputés fiables, ainsi que les algorithmes de condensat (hash) de la famille SHA-2.

4.2 EFFACEMENT DES CLES DE SIGNATURE

La bi-clé de signature doit être supprimée du QSCD à la suite de l'expiration ou de la révocation du certificat de signature associé.

4.3 SAUVEGARDE ET RESTAURATION DES CLES DE SIGNATURE

Les bi-clés de signature générées par le Service doivent demeurer dans les QSCD.

Les contenus des QSCD composant le Service doivent être synchronisé entre eux.

5 MESURES DE SECURITE NON TECHNIQUES

5.1 MESURES DE SECURITE PHYSIQUE

Les locaux techniques, qui accueillent les dispositifs matériels qui composent le Service, doivent être fortement protégés contre les intrusions.

Le niveau de protection des locaux techniques est essentiel dans la garantie de la sécurité des moyens techniques du Service et de leur exploitation.

5.1.1 Situation géographique et construction des sites

La présente Politique ne formule pas d'exigence spécifique concernant la localisation géographique des sites.

La construction des sites doit respecter les règlements et normes en vigueur et le cas échéant, des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques...).

5.1.2 Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources du SERVICE et l'interruption des Services de Docaposte Certinomis, les accès aux locaux des différentes composantes du SERVICE doivent être contrôlés.

L'accès doit être strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines doit être limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

Nota - On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisé pour la mise en œuvre de ces fonctions.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation doivent permettre de respecter les conditions d'usage des équipements du Service telles que fixées par leurs fournisseurs.

Elles doivent également permettre de respecter les exigences de la présente Politique, ainsi que les engagements pris par Docaposte Certinomis dans sa DPSSAS, en matière de disponibilité de ses fonctions.

5.1.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux doivent permettre de respecter les exigences de la présente Politique, ainsi que les engagements pris par Docaposte Certinomis dans sa DPSSAS, en matière de disponibilité de ses fonctions.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies doivent permettre de respecter les exigences de la présente Politique, ainsi que les engagements pris par Docaposte Certinomis dans sa DPSSAS, en matière de disponibilité de ses fonctions.

5.1.6 Conservation des supports

Dans le cadre de l'analyse de risque, les différentes informations intervenant dans les activités du SERVICE doivent être identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

Docaposte Certinomis doit maintenir un inventaire de ces informations. Docaposte Certinomis doit mettre en place des mesures pour éviter la compromission et le vol de ces informations.

Les supports (papier, disque dur, clé USB, DVD / CD, etc.) correspondant à ces informations doivent être gérés selon des procédures conformes à ces besoins de sécurité. 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 doivent protéger ces supports contre l'obsolescence et la détérioration pendant la période durant laquelle Docaposte Certinomis s'engage à conserver les informations qu'ils contiennent.

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.

Les procédures et moyens de destruction et de réinitialisation doivent être conformes à ce niveau de confidentialité.

5.1.8 Sauvegardes

Les composantes du Service, à l'exception des QSCD, doivent mettre en œuvre des sauvegardes déportées permettant une reprise rapide de ces fonctions à la suite de 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 informations sauvegardées doivent respecter les mêmes exigences de la présente Politique en matière de protection en confidentialité et en intégrité de ces informations.

5.2 MESURES DE SECURITE PROCEDURALES

5.2.1 Rôles de confiance

Chaque composante du Service distingue au moins les sept rôles fonctionnels de confiance suivants :

Responsable de sécurité - Le responsable de sécurité est chargé de la mise en œuvre de la Politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

Responsable d'application - Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la Politique et de la déclaration des pratiques du SERVICE au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

Ingénieur système - 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.

Opérateur - Un opérateur au sein d'une composante du Service réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.

Contrôleur - Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux Politiques de certification, aux déclarations des pratiques de certification du Service et aux Politiques de sécurité de la composante.

En plus de ces rôles de confiance au sein de chaque composante du Service, Docaposte Certinomis distingue également en tant que rôle de confiance, les rôles de porteur de parts de secrets du Service.

Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiées.

5.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, les fonctions sensibles sont réparties sur plusieurs personnes. La présente Politique définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques du Service.

5.2.3 Identification et authentification pour chaque rôle

Tous les membres du personnel de Docaposte Certinomis doivent faire vérifier leur identité et leurs autorisations avant :

- que leur nom soit ajouté à la liste d'accès aux locaux de Docaposte Certinomis ; ou
- que leur nom soit ajouté à la liste des personnes autorisées à accéder physiquement au système de Docaposte Certinomis.

Tous les intervenants sur le système de Docaposte Certinomis, ou d'une autre composante du SERVICE, doivent faire vérifier leur identité et leur autorisation avant :

- qu'un certificat leur soit délivré pour accomplir le rôle qui leur est dévolu ; ou
- qu'un compte soit ouvert en leur nom dans le système.

Chacun de ces certificats et comptes (à l'exception des certificats de signatures de Docaposte Certinomis) :

- est attribué directement à une personne ;
- ne doit pas être partagé ;
- doit être utilisé seulement pour les tâches autorisées pour le rôle assigné ; un mécanisme de contrôle est mis en place.

Les opérateurs distants intervenant sur le système de Docaposte Certinomis doivent être identifiés au moyen de mécanismes cryptographiques forts.

Docaposte Certinomis et les composantes du Service s'assurent que tout processus de vérification qu'elles utilisent permet de superviser toutes les activités des personnes qui en leur sein détiennent des rôles privilégiés.

5.2.4 Rôles exigeant une séparation des attributions

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.

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

- responsable de sécurité et ingénieur système / opérateur
- contrôleur et tout autre rôle
- ingénieur système et opérateur

5.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

5.3.1 Qualifications, compétences et habilitations requises

Le responsable de Docaposte Certinomis doit s'assurer que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation du Service:

- sont nommés à un poste faisant l'objet d'une description détaillée par écrit ;
- sont liés par contrat ou par la loi aux postes qu'ils occupent ;
- ont reçu toute la formation nécessaire pour accomplir leurs tâches ;
- sont tenus par contrat ou par la loi de ne pas divulguer de renseignements ayant trait à la sécurité de Docaposte Certinomis, aux clients ou aux Signataires ; une clause de confidentialité est expressément inscrite dans les contrats de travail des membres du personnel de Docaposte Certinomis ;

5.3.2 Procédures de vérification des antécédents

Chaque entité opérant une composante du Service doit mettre en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.

A ce titre, l'employeur peut demander à ces personnels la communication d'une copie du bulletin n°3 de leur casier judiciaire.

L'employeur peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions du personnel, de lui retirer ces attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications doivent être 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 doit être 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.

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné doit recevoir une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Les sanctions doivent être précisées dans la DPSSAS.

Docaposte Certinomis SAS au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes du Service doit également respecter les exigences du présent chapitre 5.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8 Documentation fournie au personnel

Chaque personnel doit disposer au minimum 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 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier ou électronique, rendent possibles la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'évènements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre du Service, chaque entité opérant une composante du Service doit au minimum journaliser les évènements tels que décrits ci- dessous, sous forme électronique. La journalisation doit être 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 à la suite d'une défaillance de la fonction de journalisation ;
- Évènements liés au changement des paramètres d'audit;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements doivent aussi être 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.

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions du Service, des évènements spécifiques aux différentes fonctions du Service doivent également être journalisés, notamment :

- évènements liés aux bi-clés de signature (génération et destruction) ;
- évènements liés aux signatures électroniques réalisées;
- évènements liés à l'authentification du Signataire et à la gestion des données de signature ;

Chaque enregistrement d'un évènement dans un journal doit contenir au minimum les champs suivants :

- 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 Docaposte Certinomis concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) ;
- 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).

Les opérations de journalisation doivent être effectuées au cours du processus.
En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

Les évènements et données spécifiques à journaliser doivent être documentés par Docaposte Certinomis.

5.4.2 Fréquence de traitement des journaux d'évènements

Cf. chapitre 5.4.8.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements doivent être conservés sur site pendant au moins un (1) mois. Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard sous un (1) mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

5.4.4 Protection des journaux d'évènements

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements doivent être 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 6.2.

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'évènements

Docaposte Certinomis SAS au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Chaque entité opérant une composante du Service doit mettre en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC.

5.4.6 Système de collecte des journaux d'évènements

Les journaux d'évènements doivent être remontés dans des puits de logs afin de faciliter leur exploitation.

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

Sans objet.

5.4.8 Évaluation des vulnérabilités

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

Les journaux d'évènements doivent être contrôlés une (1) fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux doivent être analysés dans leur totalité au minimum une fois toutes les deux semaines et dès la détection d'une anomalie.

Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles doit être effectué au moins une fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

5.5 ARCHIVAGE DES DONNEES

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage doivent également être prises par Docaposte Certinomis. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes du Service.

Il doit également permettre la conservation des documents papier liées aux opérations techniques.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les Politiques ;
- les DPSSAS ;
- les accords contractuels avec les AC ;
- les journaux d'évènements des différentes entités du Service

5.5.2 Période de conservation des archives

5.5.2.1 Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 doivent être archivés pendant dix (10) années après leur génération. Les moyens mis en œuvre par Docaposte Certinomis pour leur archivage doivent offrir le même niveau

de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements doit 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, doivent :

- être protégées en intégrité ;
- être accessibles aux personnes autorisées ;
- pouvoir être relues et exploitées.

Docaposte Certinomis précisera dans sa DPSSAS les moyens mis en œuvre pour archiver les pièces en toute sécurité.

Une copie de tout le matériel informatique archivé ou sauvegardé est protégée soit par des mesures de sécurité physique seulement, soit par une combinaison de mesures physiques et cryptographiques. Le site d'archivage protège adéquatement le matériel contre les dangers naturels, par exemple les excès de température, d'humidité et de magnétisme.

Docaposte Certinomis vérifiera l'intégrité de ses archives au moins tous les six (6) mois.

De plus, les informations conservées ou sauvegardées par Docaposte Certinomis peuvent être assujetties aux lois et règlements en vigueur et applicables à l'archivage et la conservation.

5.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

5.5.5 Exigences d'horodatage des données

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, qu'il soit interne ou externe, doit respecter les exigences de protection des archives concernées.

5.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à deux (2) jours ouvrés, sachant que seule Docaposte Certinomis peut accéder à toutes les archives (par opposition à une entité opérant une composante du Service qui ne peut récupérer et consulter que les archives de la composante considérée).

5.6 REPRISE SUITE A COMPROMISSION ET SINISTRE

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

Chaque entité opérant une composante du Service doit mettre 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.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de Docaposte Certinomis, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement Docaposte Certinomis. Le cas de l'incident majeur doit être 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 …). Docaposte Certinomis doit également prévenir directement et sans délai, le point de contact identifié sur le site https://cyber.gouv.fr.

Toute pratique non-conforme avec la Politique ou la DPSSAS en vigueur doit être considérée comme un incident. Une non-conformité majeure dans le cadre d'un audit de certification doit également être considérée comme un incident.

Tout incident doit faire l'objet d'un rapport d'incident et doit être communiqué à qui de droit.

La procédure de traitement des incidents doit être précisée dans la DPSSAS.

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

- informer tous les clients (SCA) avec lesquels Docaposte Certinomis a passé des accords.

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

Chaque composante du Service doit disposer d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions du Service, des engagements de Docaposte Certinomis dans sa propre Politique.

Ce plan doit être testé au minimum une fois tous les deux ans.

5.6.3 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes du Service doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente Politique.

5.7 FIN DE VIE DU SERVICE

Une ou plusieurs composantes du Service peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

Docaposte Certinomis doit prendre les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où Docaposte Certinomis 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.

Le transfert d'activité est défini comme la fin d'activité d'une composante du Service ne comportant pas d'incidence sur la validité des bi-clés de signature produites antérieurement au transfert considéré et la reprise de cette activité organisée par Docaposte Certinomis en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante du Service comportant une incidence sur la validité des bi-clés de signature produites antérieurement à la cessation concernée.

5.7.1 Transfert d'activité ou cessation d'activité affectant une composante du Service

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, Docaposte Certinomis doit entre autres obligations :

- Mettre en place des procédures dont l'objectif est d'assurer un Service constant en particulier en matière d'archivage;
- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des Signataires de bi-clés de signature, Docaposte Certinomis les en avise aussitôt que nécessaire sous un délai de trois mois;
- Docaposte Certinomis doit communiquer au point de contact identifié sur le site https://cyber.gouv.fr/, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa Politique. Docaposte Certinomis devra communiquer à l'ANSSI, selon les différentes composantes du SERVICE concernées, les modalités des changements survenus. Docaposte Certinomis 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 ;
- Docaposte Certinomis doit tenir informée l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

5.7.2 Cessation d'activité affectant Docaposte Certinomis

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 est progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par Docaposte Certinomis, ou une entité tierce qui reprennent les activités.

Dans l'hypothèse d'une cessation d'activité totale, Docaposte Certinomis ou, en cas d'impossibilité, toute entité qui lui serait substituée de part 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.

Docaposte Certinomis doit stipuler dans ses pratiques les dispositions prises en cas de cessation de Service. Elles doivent inclure :

- La notification des entités affectées ;
- Le transfert de ses obligations à d'autres parties ;
- La suppression des bi-clés de signature des Titulaires.

6 MESURES DE SECURITE TECHNIQUES

6.1 GESTION DES SYSTEMES ET DE LA SECURITE

Le Service supporte des rôles à privilèges représentés par différents rôles de confiance, définis au chapitre 5.3.1.

Les règles énoncées au chapitre 5.2.4 de cette politique doivent être respectées pour l'affectation des rôles de confiance.

Les utilisateurs qui disposent des privilèges système doivent être identifiés de manière nominative et formés en rapport aux activités qu'ils vont accomplir sur le système. Seuls ces utilisateurs doivent avoir accès au QSCD du Service. Ils doivent disposer de privilèges étendus pour administrer le QSCD au travers d'une interface dédiée.

Le Service supporte également des rôles sans privilège :

- Le Signataire est autorisé a accédé au Service au travers du SAD en utilisant le protocole SAP, à demander la signature électronique de données ;
- La SCA (Souscripteur) est autorisée à envoyer les données à signer par le Signataire au Service ;
- La PKI (de l'AC du PSCE) est autorisée à fournir le certificat de signature de signature du Signataire au Service.

Aucun utilisateur ne doit disposer à la fois d'un rôle de confiance et d'un rôle sans privilège.

6.2 SYSTEMES ET OPERATIONS

Le Service et ses composants techniques doivent être documentés (DAT et DEX) afin d'être exploités de manière sécurisée, déployés en minimisant les risques de panne et en étant protégés contre les virus et malwares.

Les horloges des composants du Service doivent être synchronisées sur une source de temps fiable, avec pour référence le temps UTC.

6.3 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

6.3.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques du SERVICE doit être défini dans la DPSSAS internes de Docaposte Certinomis. Il doit 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 œuvre la Politique de contrôle d'accès définie par Docaposte Certinomis, 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,
- 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),
- éventuellement, gestion des reprises sur erreur.

Les applications utilisant les Services des composantes peuvent requérir des besoins de sécurité complémentaires.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle (cf. chapitre 1.4.1.2) doit faire l'objet de mesures particulières, qui peuvent découler 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) doivent être mis en place.

Docaposte Certinomis. doit mettre en conformité ses pratiques avec les documents de l'ANSSI relatifs à la protection du poste de l'application de l'AE et du poste de Docaposte Certinomis.

En particulier, Docaposte Certinomis doit appliquer l'ensemble des règles définies dans le guide d'hygiène informatique publié par l'ANSSI pour le niveau « standard ».

6.3.2 Niveau d'évaluation sécurité des systèmes informatiques

Cf. Annexe 2 pour les exigences concernant le composant QSCD du Service.

6.4 MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

6.4.1 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes du SERVICE doit être documentée et doit respecter dans la mesure du possible des normes de modélisation et d'implémentation. La configuration du système des composantes du SERVICE ainsi que toute modification et mise à niveau doivent être documentées et contrôlées.

Docaposte Certinomis doit :

- garantir que les objectifs de sécurité sont définis lors des phases de spécification et de conception,
- utiliser des systèmes et des produits fiables qui sont protégés contre toute modification.

6.4.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante du SERVICE doit être signalée à Docaposte Certinomis pour validation. Elle doit être documentée et doit apparaître 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.

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

Sans objet.

6.5 MESURES DE SECURITE RESEAU

L'interconnexion vers des réseaux publics doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein du Service.

Docaposte Certinomis doit garantir 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 Docaposte Certinomis.

De plus, les échanges entre composantes au sein du Service peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

7 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Le présent chapitre ne concerne que les audits et évaluations de la responsabilité de Docaposte Certinomis afin de s'assurer du bon fonctionnement de son Service.

7.1 FREQUENCES ET/OU CIRCONSTANCES DES EVALUATIONS

Avant la première mise en Service d'une composante de son Service ou à la suite de toute modification significative au sein d'une composante, Docaposte Certinomis doit procéder à un contrôle de conformité de cette composante.

Docaposte Certinomis doit également procéder à un contrôle biennal de conformité de l'ensemble de son Service.

7.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

Le contrôle d'une composante doit être assigné par Docaposte Certinomis à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

7.3 RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

L'équipe d'audit ne peut pas appartenir à l'entité opérant la composante du Service contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

7.4 SUJETS COUVERTS PAR LES EVALUATIONS

Les contrôles de conformité portent sur une composante du Service (contrôles ponctuels) ou sur l'ensemble de l'architecture du Service (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définis dans la présente Politique et dans la DPSSAS qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

7.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à Docaposte Certinomis, un avis parmi les suivants :

- "réussite",
- "échec",
- "à confirmer".

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à Docaposte Certinomis qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par Docaposte Certinomis et doit respecter ses Politiques de sécurité internes.
- En cas de résultat "À confirmer", Docaposte Certinomis remet à la composante un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, Docaposte Certinomis confirme à la composante contrôlée la conformité aux exigences de la présente Politique et la DPSSAS associée.

7.6 COMMUNICATION DES RESULTATS

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification en charge de la qualification de Docaposte Certinomis.

Si le rapport d'audit contient des informations touchant la sécurité de Docaposte Certinomis ou des informations qu'elles considèrent confidentielles, la publication n'est pas effectuée. Il est possible d'obtenir, sur demande expresse, un résumé ou des extraits du rapport sous forme électronique.

Les attestations d'audits de conformité sont tenues à la disposition du public. Il est possible d'obtenir, sur demande expresse, une copie sous forme électronique.

8 AUTRES PROBLEMATIQUES METIERS ET LEGALES

8.1 RESPONSABILITE FINANCIERE

8.1.1 Couverture par les assurances

La garantie associée à la signature électronique calculée par le Service est limitée au montant prévu au contrat. Pour toute transaction commerciale, ou échange électronique, dont les conséquences financières directes ou indirectes sont d'un montant supérieur au montant prévu, la responsabilité des acteurs du Service ne peut être engagée vis-à-vis des clients, bénéficiaires et tiers utilisateurs.

8.1.2 Autres ressources

Aucune exigence particulière.

8.1.3 Couverture et garantie concernant les entités utilisatrices

Les signatures électroniques garanties par la présente Politique comportent un niveau d'assurance garanti, précisé par contrat et accessible à la partie utilisatrice.

8.2 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

8.2.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- les clés privées des Signataires ,
- les données d'activation associées aux clés privées des Signataires,
- tous les secrets du Service,
- les journaux d'évènements des composantes du Service,
- les procédures et Politiques internes de Certinomis.

8.2.2 Informations hors du périmètre des informations confidentielles

Sans objet.

8.2.3 Responsabilités en termes de protection des informations confidentielles

Docaposte Certinomis est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 8.2.1 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, Docaposte Certinomis doit en garantir l'intégrité.

Docaposte Certinomis est tenue de respecter la législation et la réglementation en vigueur sur le territoire français.

8.3 PROTECTION DES DONNEES PERSONNELLES

Docaposte Certinomis SAS au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

8.3.1 Politique de protection des données personnelles

Le Règlement Européen UE 2016/679 du 27 avril 2016 relatif à la protection des données personnelles ainsi que la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifié par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel s'applique à tous les documents détenus ou transmis par Docaposte Certinomis ou par une des composantes du Service (site de la CNIL http://www.cnil.fr).

En vertu des textes, les Souscripteurs et les Signataires disposent d'un droit d'accès, de rectification et d'opposition à la cession de toute information qui les concerne. Ce droit peut s'exercer par l'intermédiaire du Service agent, en particulier l'AE de l'AC du PSCE, ayant recueilli ces informations, à l'adresse figurant sur le site WEB de Docaposte Certinomis.

Docaposte Certinomis respecte rigoureusement toutes les prescriptions légales applicables et explique sur son site WEB, les modalités concrètes d'application de la loi, notamment dans les rubriques « mentions légales & gestion des données personnelles ».

La Politique respecte les principes fondamentaux en matière de protection des données à caractère personnel consacrés dans la loi, le RGPD et toute autre convention internationale entrée en vigueur.

8.3.2 Données à caractère personnel

Toutes les données collectées et détenues par Docaposte Certinomis sur une personne physique ou morale sont considérées comme confidentielles et ne peuvent pas être divulguées sans avoir obtenu le consentement préalable du Signataire.

Les renseignements concernant l'identification ou d'autres données à caractère personnel, du Signataire, apparaissant sur les certificats sont considérés comme étant confidentiels, sauf si le bénéficiaire a donné son consentement exprès et préalable à toute diffusion.

8.3.3 Données à caractère non personnel

Sans objet.

8.3.4 Responsabilité en termes de protection des données à caractère personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous)

8.3.5 Notification et consentement d'utilisation des données à caractère personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous)

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

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous)

8.3.7 Autres circonstances de divulgation de données personnelles

Le secret des correspondances émises par voie des télécommunications est garanti par la loi française. En cas d'atteinte, toute violation est punie par l'article 226-15 du code pénal pour celles commises par un particulier et par les articles 432-9 et 432-17 du code pénal pour celles commises par une personne dépositaire de l'autorité publique.

D'une façon générale, aucun salarié de Docaposte Certinomis et aucun collaborateur ou sous-traitant, dans le cadre de leur participation aux Services de certification, n'a le droit d'intercepter, d'ouvrir, de détourner, de divulguer, de rechercher ou d'utiliser les documents soumis à Docaposte Certinomis, sauf dans les cas prévus dans la présente Politique, ou dans le cadre du régime des interceptions ordonnées par l'autorité judiciaire ou des interceptions de sécurité en vertu de la loi n°91-646 du 10 juillet 1991.

8.4 DROITS SUR LA PROPRIETE INTELLECTUELLE

Tous les droits de propriété intellectuelle détenus par Certinomis sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de leur non-respect. Par exemple, conformément à la loi n°98-536 du 1er juillet 1998 (Journal officiel du 2 juillet 1998, p.10075) et à la directive européenne 96/6/CE du 11 mars 1996, les bases de données réalisées par Certinomis sont protégées. Le texte de la loi peut être consulté sur le site suivant : http://www.legifrance.gouv.fr.

8.5 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Ce chapitre contient des dispositions relatives aux obligations respectives de Docaposte Certinomis, du personnel de Docaposte Certinomis, des diverses entités composant le Service, des clients, et des Signataires. Elle contient aussi des dispositions juridiques, relatives notamment à la loi applicable et à la résolution des litiges.

Les obligations communes aux composantes du Service 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 Politique de Docaposte Certinomis et les documents qui en découlent,
- respecter et appliquer la partie de la DPSSAS 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 Docaposte Certinomis (cf. chapitre VIII) et l'organisme de qualification,
- respecter les accords ou contrats qui les lient entre elles ou aux RC,
- documenter leurs procédures internes de fonctionnement,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

8.5.1 Prestataire d'Application de Signature Serveur

Docaposte Certinomis a pour obligation de :

- garantir que les requêtes de signature proviennent d'utilisateurs authentifiés, en utilisant des méthodes d'authentification sécurisées.
- mettre en place des mécanismes de sécurité afin de garantir que les données signées ne peuvent pas être modifiées sans détection.
- empêcher tout accès non autorisé aux données.
- assurer la résilience du Service et la capacité de récupérer rapidement en cas de panne.

Docaposte Certinomis est responsable de la conformité de sa Politique, avec les exigences émises dans les référentiels applicables pour le niveau de sécurité considéré. Docaposte Certinomis assume toute conséquence dommageable résultant du non-respect de sa PC, par elle-même ou l'une de ses composantes. Elle doit prendre

les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente Politique.

De plus, Docaposte Certinomis reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des RC à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de Docaposte Certinomis.

Par ailleurs, Docaposte Certinomis reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses Services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de Docaposte Certinomis.

8.5.2 Signataires

Le Signataire doit se conformer à toutes les exigences de la présente Politique.

Il s'engage à respecter le contrat qui le lie à l'AC, qui a délégué au Service la gestion des bi-clés de signature des Titulaires de Certificats de Signature qu'elle émet.

S'il soupçonne la compromission d'une clé privée, il est tenu d'en aviser l'AC dans les plus brefs délais et selon les instructions données par celle-ci.

En aucun cas le Signataire n'acquiert la propriété de la bi-clé de signature émise par Docaposte Certinomis. Il n'en acquiert que le droit d'usage. Par conséquent, toutes les bi-clés de signature demeurent la propriété de Docaposte Certinomis qui les a émis.

8.6 LIMITE DE GARANTIE

La génération et la gestion d'une bi-clé de signature, conformément à la présente Politique, ne fait pas de Docaposte Certinomis, de l'une des composantes du Service, du responsable de Docaposte Certinomis et du personnel de Docaposte Certinomis et des composantes du Service un fiduciaire, un mandataire, un garant ou un autre représentant de quelque façon que ce soit du bénéficiaire, du client ou de toutes autres parties concernées. Chaque partie s'interdit de prendre un engagement au nom et pour le compte de l'autre partie à laquelle elle ne saurait en aucun cas se substituer.

En conséquence de quoi, les Signataires et les clients sont des personnes juridiquement et financièrement indépendantes et, à ce titre, ne disposent d'aucun pouvoir ni de représentation, ni d'engager Docaposte Certinomis ou l'une des composantes du Service, susceptible de créer des obligations juridiques, tant de façon expresse que tacite au nom de Docaposte Certinomis ou de l'une des composantes du Service. Les Services d'Application de Serveur de Signature ne constituent pas un partenariat ni ne créent une quelconque forme juridique d'association juridique qui imposerait une responsabilité basée sur les actions ou les carences de l'autre. Le contrat ne constitue ni une association, ni une société ou autre groupement, ni un mandat donné par l'une des parties à l'autre.

8.7 LIMITE DE RESPONSABILITE

Docaposte Certinomis le personnel de Docaposte Certinomis, les composantes du Service, les clients, les bénéficiaires, les tiers utilisateurs sont responsables pour tous dommages et intérêts découlant du non-respect de leurs obligations respectives telles que définies aux termes de la présente Politique et de la DPSSAS associée.

Docaposte Certinomis détaille le périmètre des limites de responsabilité dans sa DPSSAS.

8.8 INDEMNITES

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de l'une des parties envers l'autre, les dommages et intérêts et indemnités à sa charge, toutes causes confondues, ne sauraient en aucun cas dépasser les limites de responsabilité mentionnées dans le cadre du contrat conclu entre Docaposte Certinomis et son client.

8.9 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA POLITIQUE

8.9.1 Durée de validité

La présente Politique reste en application jusqu'à la fin de vie du dernier certificat émis sur la base d'une bi-clé générée par cette Politique.

8.9.2 Fin anticipée de validité

La publication d'une nouvelle version de la présente Politique peut entraîner, en fonction des évolutions apportées, la nécessité pour Docaposte Certinomis de faire évoluer sa DPSSAS correspondante.

En fonction de la nature et de l'importance des évolutions apportées à la Politique, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

8.9.3 Effets de la fin de validité et clauses restant applicables

Sans objet.

8.10 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

En cas de changement de toute nature intervenant dans la composition du SERVICE, Docaposte Certinomis devra :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de Docaposte Certinomis et de ses différentes composantes ;
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

8.11 AMENDEMENTS A LA POLITIQUE

Le présent chapitre définit les exigences en matière d'administration et de gestion de la présente Politique de certification.

8.11.1 Procédures d'amendements

Docaposte Certinomis devra contrôler que tout projet de modification de sa POLITIQUE reste conforme aux exigences des référentiels ETSI applicables et des éventuels documents complémentaires. En cas de changement important, Docaposte Certinomis fera appel à une expertise technique pour en contrôler l'impact.

8.11.2 Mécanisme et période d'information sur les amendements

Pas d'exigence particulière.

8.11.3 Circonstances selon lesquelles l'OID doit être changé

L'OID de la Politique de Docaposte Certinomis doit évoluer dès lors qu'un changement majeur intervient dans les exigences applicables au Service.

8.12 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

Docaposte Certinomis doit mettre 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.

8.13 JURIDICTIONS COMPETENTES

La présente Politique de certification est expressément élaborée, régie, appliquée et interprétée selon les lois et règlements français, bien que les activités qui découlent de la présente Politique puissent avoir des effets juridiques en dehors du territoire de la République française.

8.14 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

Les textes législatifs et réglementaires applicables à la présente Politique sont, notamment, ceux indiqués au chapitre 10 ci-dessous.

8.15 DISPOSITIONS DIVERSES

8.15.1 Accord global

Sans objet.

8.15.2 Transfert d'activités

Cf. chapitre 5.8.

8.15.3 Conséquences d'une clause non valide

Le caractère inapplicable dans un contexte donné d'une disposition de la Politique n'affecte en rien la validité des autres dispositions, ni de cette disposition hors du dit contexte. La Politique continue à s'appliquer en l'absence de la disposition inapplicable, et ce tout en respectant l'intention des parties.

Les intitulés portés en tête de chaque article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

8.15.4 Application et renonciation

Toute notification devant être donnée au titre de la présente Politique sera censée avoir été donnée si elle est envoyée par lettre recommandée avec avis de réception ou par télécopie adressée au domicile élu comme indiqué en entête du contrat de Service et sera censée avoir été reçue sept (7) jours après la date de cachet de la Poste

dans le cadre de la lettre recommandée avec avis de réception et un (1) jour après la date d'envoi dans le cadre de la télécopie.

8.15.5 Force majeure

Dans un premier temps, les cas de force majeure suspendront l'exécution du contrat. Si les cas de force majeure ont une durée supérieure à celle indiquée dans le contrat, le contrat est résilié automatiquement, sauf accord contraire entre les parties. L'exécution des obligations reprendra son cours normal dès que l'évènement constitutif de la force majeure aura cessé.

Docaposte Certinomis ne saurait être tenue responsable et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente Politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'article 1148 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des cours et tribunaux français, des clauses contractuelles contenues dans la Déclaration des Pratiques associée et toutes autres conventions liant les parties (par exemple le contrat) :

Grève totale ou partielle, lock-out, émeute, trouble civil, insurrection, guerre civile ou étrangère, risque nucléaire, embargo, confiscation, capture ou destruction par toute autorité publique, intempérie, épidémie, blocage des moyens de transport ou d'approvisionnement pour quelque raison que ce soit, tremblement de terre, incendie, tempête, inondation, dégâts des eaux, restrictions gouvernementales ou légales, modifications légales ou réglementaires des formes de commercialisation, panne d'ordinateur, blocage des communications électroniques, y compris des réseaux de télécommunications, toute découverte scientifique majeure remettant en cause en totalité ou en partie les principes de la cryptographie asymétrique, toute conséquence d'une évolution technologique, non prévisible par Docaposte Certinomis, remettant en cause les normes et standards de sa profession et tout autre cas indépendants de la volonté des parties empêchant l'exécution normale du présent contrat.

8.16 AUTRES DISPOSITIONS

En vertu des articles 323-1 à 323-7 du Code pénal, applicable lorsqu'une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc.

Les peines encourues varient de 2 à 5 ans d'emprisonnement et d'une amende allant de 30.000 à 375.000 euros pour les personnes morales.

La contrefaçon de marques de fabrique, de commerce et de Services, dessins et modèles, signes distinctifs, droits d'auteur (par exemple : logiciels, pages WEB, bases de données, textes originaux, ...) est sanctionnée par les articles L. 716-1 et suivants du Code de la propriété intellectuelle

9 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

9.1 REGLEMENTATION

Renvoi	Document
[CNIL]	*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004*
[EIDAS]	*RÈGLEMENT (UE) 2024/1183 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 11 avril 2024 modifiant le règlement (UE) no 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique*
[ETSI 119431-1]	*Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev*
[RGPD]	*Règlement Européen UE 2016/679 du 27 avril 2016 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, et abrogeant la directive 95/46/CE*

9.2 DOCUMENTS TECHNIQUES

Renvoi	Document
[X.509]	*Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version mars 2000 (complete par les correctifs techniques n° 1 d'octobre 2001, n° 2 d'avril 2002 et n° 3 d'avril 2004)*
[SOGIC-CRYPTO]	*SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms - Version en vigueur.*

10 ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DU SERVICE

10.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le dispositif cryptographique, utilisé par le Service pour générer et stocker et mettre en œuvre les bi-clés des Signataires doit répondre aux exigences de sécurité suivantes :

- garantir que la génération de la bi-clé est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- authentifier le Signataire et identifier sa clé privée de signature de manière sûre et fiable;
- générer un cachet ou une signature qui ne peut être falsifiée sans la connaissance de la clé privée.

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques doivent être mises en place afin de :

- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction des clés privées ;
- garantir la confidentialité et l'intégrité de la clé privée ;

10.2 EXIGENCES SUR LA QUALIFICATION

Le module cryptographique matériel utilisé pour la génération et la mise en œuvre des clés des Signataires doit être évalué selon les Critères Communs au niveau EAL 4 minimum [SOGIS-CRYPTO] et certifié QSCD conformément à l'article 3 du règlement [EIDAS], par une autorité compétente (cf. eIDAS Dashboard).