Goodflag Cachetage

Conditions Générales d'Utilisation du Service de Cachet Electronique Qualifié à Distance

Version 1.0

Date d'entrée en vigueur : 17/04/2026

OID du Service : 1.3.6.1.4.1.22542.100.3.2

9 Av Maréchal Leclerc – 10120 ST ANDRE LES VERGERS – FRANCE
Tél. : +33 (0)3 25 43 90 78 – www.goodflag.com
SAS au capital de 26 739 euros – R.C.S. Troyes 480 622 257 – Code APE 5829C – TVA FR01480622257

Table des matières

1. Introduction

1.1 Présentation générale

La société Lex Persona a adopté la marque commerciale Goodflag au début de l'année 2025. Dans les présentes Conditions Générales d'Utilisation (CGU), le nom Goodflag est utilisé en priorité dans la mesure où il s'agit de la marque principalement exposée aux utilisateurs du service ; Lex Persona demeure l'entité légale qui porte le service et, le cas échéant, les activités de prestataire de services de confiance qualifié au sens du règlement (UE) n° 910/2014.

Goodflag fournit un Service de Cachet Électronique Qualifié à Distance (SCEQAD) destiné aux personnes morales (ci-après les « Sujets ») qui souhaitent apposer des cachets électroniques qualifiés à distance sur des documents numériques, par l'intermédiaire d'une personne physique désignée comme « Responsable de la Clé Privée du Sujet » (RCPS), qui utilise le SCEQAD au moyen :

- D'un Certificat qualifié eIDAS, au nom du Sujet et fourni au RCPS, conforme au standard ETSI EN 319 411-2 au profil QCP-l-qscd, délivré par l'Autorité de Certification « Sunnystamp Legal Persons CA 1 », pour une durée maximale de trois (3) ans, et désigné « Certificat d'Entité » dans la suite du document ;
- D'un dispositif qualifié de création de cachet électronique (Qualified Signature Creation Device - QSCD) à distance, opéré dans un environnement contrôlé et sécurisé conformément aux normes ETSI applicables, notamment ETSI TS 119 431-1, qui héberge la Clé Privée associée à la Clé Publique du Certificat d'Entité précédemment délivré, et dont la mise en œuvre est contrôlée exclusivement par le RCPS.

Le contrôle exclusif de l'utilisation de la Clé Privée par le RCPS repose sur un mécanisme à deux niveaux :

- Un engagement initial formalisé, lors de la phase d'enregistrement du Certificat, par la signature des CGU relatives à la demande de Certificat et des présentes CGU, et matérialisé par la signature électronique qualifiée du formulaire de demande de Certificat ;
- L'utilisation d'un Module de Création de Cachet (MCC) fournit par Goodflag, qui impose :
    - L'authentification du RCPS au moyen d'un Certificat d'authentification ;
    - La fourniture des données d'activation de cachet (SAD) qui conditionnent l'accès à la Clé Privée du Sujet.

Le SCEQAD n'est pas un service de création de cachet générique couvrant plusieurs niveaux de cachets. Il est limité à la création de cachets électroniques qualifiés à distance pour des personnes morales, et ne couvre aucun autre usage cryptographique. Les présentes CGU ne régissent ni d'autres niveaux de cachet, ni les modules ou applications tiers permettant d'initier une demande de cachet, sauf mention expresse contraire.

1.2 Acceptation et opposabilité des CGU du SCEQAD

Les CGU du SCEQAD, s'entendent au sens de la norme ETSI EN 319 401 (paragraphe 6.2) et sont établies conformément aux exigences de la norme ETSI TS 119 431-1 (paragraphe 4.3.3).

Les présentes CGU définissent les conditions d'utilisation du SCEQAD par un RCPS. Elles sont mises à disposition du RCPS au format numérique, avant l'entrée dans la relation contractuelle relative à l'utilisation du service et avant tout acte de cachet, et acceptées par le RCPS lors de la signature électronique qualifiée du formulaire de demande de Certificat. La version applicable est celle en vigueur à la date de l'utilisation du SCEQAD concernée.

Cette acceptation vaut engagement contractuel, reconnaissance expresse de leur opposabilité et adhésion sans réserve à l'ensemble des dispositions qui y sont prévues.

Le RCPS reconnaît que l'utilisation du SCEQAD implique le respect strict des présentes CGU, des politiques applicables ainsi que des normes et réglementations en vigueur.

1.3 Identification du document

Le présent document constitue les CGU du SCEQAD opéré par Goodflag.

Il est rattaché à l'OID 1.3.6.1.4.1.22542.100.3.2.1, qui identifie la Politique et la Déclaration des Pratiques du SCEQAD (PSCEQUAD/DPSCEQAD). Toute évolution substantielle du présent document donne lieu à une nouvelle version et, le cas échéant, à une mise à jour des identifiants et références documentaires applicables.

2. Références normatives

Les présentes CGU s'inscrivent notamment dans le cadre des textes et normes suivants :

- Règlement (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement eIDAS), ainsi que ses textes d'application et d'évolution ;
- ETSI EN 319 401, General Policy Requirements for Trust Service Providers ;
- ETSI EN 319 411-2, Policy and security requirements for Trust Service Providers issuing EU qualified certificates ;
- ETSI TS 119 431-1, Policy and security requirements for trust service providers supporting server signing ;
- Le cas échéant, les référentiels applicables aux prestataires de services de confiance qualifiés et aux QSCD.

3. Politique applicable / documents de référence

Le SCEQAD est régi, en complément des présentes CGU, par les documents suivants, dans leur version en vigueur :

- La Politique de Service de Cachet Électronique Qualifiée à Distance et sa Déclaration des Pratiques de Service associée (PSCEQAD/DPSCEQAD) ;
- La Politique Générale des Services de Confiance de Goodflag / Lex Persona (PGSC), pour les exigences transverses qu'elle définit ;
- La Politique de Certification et la Déclaration des Pratiques de Certification de l'Autorité de Certification « Sunnystamp Legal Persons CA 1 » ;

- Les informations publiées dans le dépôt documentaire officiel de Goodflag / Lex Persona, y compris, le cas échéant, les Certificats d'AC, les informations de validation et les versions applicables des politiques.

En cas de contradiction entre les présentes CGU et les documents techniques ou contractuels applicables au service, l'interprétation se fait en cohérence avec le règlement eIDAS, les normes ETSI applicables et la PSCEQAD/DPSCEQAD, sous réserve des droits impératifs reconnus aux Signataires par la loi applicable.

Le dépôt officiel de Goodflag / Lex Persona est accessible à l'adresse *https://www.goodflag.com/services-de-confiance*.

4. Définitions

Autorité de Certification (AC) : entité qui, au sein d'un prestataire de services de confiance, émet et gère des Certificats. Dans le cadre du SCEQAD, l'AC utilisée pour l'émission des Certificats qualifiés de cachet est « Sunnystamp Legal Persons CA 1 ».

Autorité d'Enregistrement (AE) : entité chargée de l'identification des RCPS et du RL de la personne morale à laquelle le Sujet est rattaché et de la gestion des demandes de Certificats ou des données nécessaires à leur émission.

Bi-clé : combinaison d'une Clé Privée et d'une Clé Publique utilisée pour effectuer des opérations cryptographiques.

Certificat : ensemble d'informations garantissant l'association entre l'identité d'une personne physique ou morale et une Clé Publique, grâce à une signature électronique de ces données effectuée à l'aide de la Clé Privée de l'AC qui délivre le Certificat. Un Certificat contient des informations telles que : la Clé Publique et l'identité de son propriétaire, ses usages autorisés, la durée de vie du Certificat, la Signature électronique du Certificat par l'AC et son identité, etc. Le format standard de Certificat est défini dans la recommandation X.509 v3 et dans la RFC 5280. Dans le cadre de la présente PSCEQAD/DPSCEQAD, un Certificat désignera généralement celui utilisé par le RCPS de manière persistante pour cacheter des documents et qui lui est délivré par l'AC « Sunnystamp Legal Persons CA 1 » gérée par Lex Persona.

Clé Privée : clé d'une Bi-clé destinée à rester sous le contrôle exclusif de son titulaire et utilisée pour créer la signature ou le cachet électronique.

Clé Publique : clé d'une Bi-clé pouvant être rendue publique pour vérifier la signature ou le cachet électronique.

Client : entité légale ayant contractualisé avec Goodflag afin d'utiliser le SCEQAD pour cacheter électroniquement des documents.

Module de Création de Cachets (MCC) : module édité par Goodflag, qui fonctionne à l'initiative d'un Utilisateur, sous le contrôle du RCPS, en vue de faire cacheter un ou plusieurs document(s) par un Certificat de cachet. En particulier, il calcule l'empreinte SHA 256, SHA 384 ou SHA 512 des documents qui sont ensuite intégrées à une Transaction de cachet. Une fois la Transaction

effectuée avec succès, le MCC intègre le(s) cachet(s) électronique(s) produit(s) par le SCEQAD au(x) document(s) concerné(s). Lex Persona propose différents MCC (mono-document, multi-documents), en fonction des besoins métiers des Clients.

QSCD : dispositif qualifié de création de signature électronique au sein duquel la Clé Privée de cachet est générée, protégée et utilisée sans quitter le dispositif.

Signature Activation Data (SAD) : données d'activation de cachet permettant au RCPS d'autoriser l'opération de cachet et au SCEQAD d'activer, sous contrôle logique approprié, l'utilisation de la Clé Privée dans le QSCD.

Signature Activation Module (SAM) : composant qui met en œuvre les données d'activation de cachet et assure que l'utilisation de la Clé Privée se fait sous le contrôle exclusif du RCPS. Le SAM est chargé d'interpréter la demande de cachet et d'autoriser l'opération au QSCD distant.

RCPS : personne physique identifiée qui utilise le SCEQAD pour cacheter un ou plusieurs document(s) dans le cadre d'une Transaction de cachets déterminée.

Transaction de cachet : opération déclenchée à l'initiative d'un RCPS habilité par le RL et ayant pour finalité le cachet d'un ou plusieurs document(s) par un Signataire.

Utilisateur de Cachet (UC) : personne physique ou morale, ou système applicatif, qui se fie à un cachet produit par le SCEQAD pour vérifier l'intégrité d'un document cacheté et l'identité du Sujet.

5. Acronymes

AC	Autorité de Certification
AE	Autorité d'Enregistrement
CECAD	Cachet Electronique Qualifié A Distance
CGU	Conditions Générales d'Utilisation
DPSCEQAD	Déclaration des Pratiques de Service de Cachet Électronique Qualifié à Distance
HSM	Hardware Security Module
MCC	Module de Création de Cachets
OID	Object Identifier
PSCEQAD	Politique de Service de Cachet Électronique Qualifié à Distance
QSCD	Qualified Signature Creation Device
SAD	Signature Activation Data
SAM	Signature Activation Module
SCEQAD	Service de Cachet Électronique Qualifié à Distance
UC	Utilisateur de Cachet

6. Politique de service appliquée

Le SCEQAD est un service de confiance de création de cachet électronique qualifié à distance, qui s'appuie notamment :

- Sur un service de délivrance de Certificat qualifié conforme à [ETSI_319_411-2] au niveau QCP-l-qscd, et dont la Clé Privée associée à la Clé Publique figurant dans le Certificat est stockée dans un QSCD qualifié à distance, lui-même s'appuyant ;

- Sur un service de gestion de QSCD à distance conforme à [ETSI_119_431-1] au niveau NSP + EUSPv2 et dont la politique fait l'objet du présent document.

Le SCEQAD repose sur une architecture garantissant une séparation stricte des rôles et un cloisonnement des environnements : MCC → SCEQAD → SAM → QSCD.

Le SCEQAD n'accède jamais directement au QSCD. Le SAM constitue le point de contrôle logique d'activation, opéré dans un environnement isolé, non accessible depuis Internet, et protégé contre toute tentative d'intrusion physique et logique.

L'activation de la Clé Privée de type RSA 3072 bits est conditionnée à la vérification cumulative de : (i) l'authentification du RCPS et (ii) la fourniture des SAD.

La Clé Privée est générée, stockée et utilisée exclusivement au sein du QSCD ; elle n'est jamais exportable, duplicable ou accessible en clair.

Le SCEQAD ne traite que des empreintes cryptographiques SHA 256, SHA 384 ou SHA 512 calculées par le MCC ; les données en clair ne sont jamais accessibles au SCEQAD, au SAM ni au QSCD.

Les présentes CGU sont spécifiques au SCEQAD. Elles ne valent pas, sauf stipulation expresse, pour d'autres services de confiance, pour d'autres niveaux de cachet ou pour des services d'orchestration applicative extérieurs au périmètre du SCEQAD.

7. Limitations d'usage du service

Le SCEQAD ne peut être utilisé que pour la création de cachets électroniques qualifiés de personnes morales dans le cadre d'une Transaction de cachets déterminée. Il ne peut pas être utilisé pour créer des signatures ou des cachets qui sont hors périmètre du SCEQAD, et de manière plus générale pour réaliser des opérations cryptographiques autres que celles prévues par les présentes CGU et les politiques applicables.

Le Certificat qualifié utilisé dans le cadre du SCEQAD ne peut être utilisé que pour cacheter les documents d'une Transaction de cachets initiée par un MCC.

Les cachets produits par le SCEQAD ne portent que sur les documents dont l'empreinte SHA 256, SHA 384 ou SHA 512 a été intégrée à la Transaction de cachets.

Le RCPS ne doit pas utiliser le SCEQAD dans un contexte illicite, frauduleux ou contraire aux lois et règlements applicables. Le service ne dispense pas le Client, le RCPS ou l'UC de vérifier l'adéquation des documents cachetés à leur contexte métier ou réglementaire.

Sous réserve des limitations légales applicables, les dommages résultant d'un usage du service au-delà des limitations prévues par les présentes CGU, par la politique de service ou par la politique de certification applicable ne sont pas couverts par les engagements de Goodflag.

8. Obligations du RCPS

Le RCPS s'engage notamment à :

- Agir au nom et pour le compte du Sujet dans le respect des habilitations qui lui ont été conférées ;
- Utiliser personnellement et exclusivement ses moyens d'authentification ;

- Préserver la confidentialité, l'intégrité et la disponibilité de ses SAD ;
- Vérifier la légitimité, la finalité et le contexte de chaque opération de cachet ;
- S'assurer de l'exactitude et de la complétude des données avant leur soumission ;
- Ne pas déléguer, partager ou transférer ses moyens d'authentification ;
- Ne pas tenter de contourner ou compromettre les mécanismes de sécurité du service ;
- Signaler sans délai toute compromission, suspicion de compromission ou anomalie ;
- Se conformer à l'ensemble des politiques applicables.

Toute utilisation conjointe des moyens d'authentification et des SAD sous le contrôle du RCPS vaut manifestation explicite de sa volonté d'effectuer une opération de cachet engageant le Sujet.

Le RCPS demeure responsable de l'usage des moyens d'authentification placés sous son contrôle. Toute défaillance imputable à une mauvaise utilisation de ces moyens, à leur compromission du fait du RCPS ou à des informations erronées fournies au service peut affecter la possibilité de cacheter, donner lieu à la révocation du Certificat qualifié ou l'opposabilité des éléments techniques associés.

9. Informations destinées aux UC et autres parties se fiant au service

Les UC et, plus généralement, les parties qui se fient aux cachets produits via le SCEQAD doivent vérifier le cachet électronique, le Certificat qualifié associé, la chaîne de certification et les informations de confiance publiées par Goodflag / Lex Persona ou par les AC concernées, au moyen d'outils et de procédures adaptés.

Compte tenu de la durée de validité du Certificat qualifié qui est limitée dans le temps (3 ans), l'UC doit en tenir compte lors de la vérification des cachets. La vérification doit porter, a minima, sur l'intégrité du document signé, la validité du Certificat à la date du cachet, la chaîne de certification applicable et, le cas échéant, les informations de confiance et d'horodatage associées.

Les UC doivent respecter les limitations d'usage du Certificat et des cachets produits. Une confiance accordée au-delà du périmètre fonctionnel ou temporel décrit dans les présentes CGU, dans la politique de service ou dans les politiques de certification applicables relève de la responsabilité de la partie qui s'y fie.

Les informations nécessaires à la vérification des Certificats et des cachets, y compris les politiques applicables et les Certificats d'autorité pertinents, sont publiées dans le dépôt officiel de Goodflag / Lex Persona ou rendues disponibles par les moyens prévus par les politiques de certification applicables.

10. Durée de conservation des journaux d'événements

Le SCEQAD journalise les événements nécessaires à la sécurité, à la traçabilité et à la valeur probante des opérations réalisées, notamment les identifiants techniques de Transaction de cachet, les horodatages, les résultats des contrôles, la référence du Certificat, ainsi que les événements significatifs intervenant lors de l'authentification et de l'exécution de la Transaction de cachet.

Les journaux d'événements sont conservés pendant une durée compatible avec les exigences réglementaires, normatives et contractuelles applicables au service. Les journaux relatifs aux Transactions sont, sauf conditions particulières, conservés pendant dix ans. La durée de

conservation calendaire applicable aux journaux d'événements techniques du SCEQAD est fixée dans le corpus documentaire interne et dans les politiques applicables.

Pendant leur durée de conservation, les journaux et éléments probants font l'objet de mesures destinées à préserver leur intégrité, leur confidentialité et leur disponibilité, conformément au corpus de sécurité applicable au SCEQAD.

Goodflag conserve les données d'audit 10 ans.

11. Limitations de responsabilité

Goodflag assume, en tant que prestataire de services de confiance qualifié lorsque le cadre juridique l'exige, les responsabilités qui lui incombent en application du règlement eIDAS, du droit français applicable et des textes pris pour leur application. Les présentes CGU ne limitent pas les responsabilités impératives auxquelles il ne peut être légalement dérogé.

Sous réserve des dispositions d'ordre public applicables, Goodflag ne saurait être tenue responsable :

- D'une utilisation du SCEQAD, du Certificat qualifié ou des informations de validation en dehors du périmètre, de l'objet ou de la durée pour lesquels ils ont été prévus ;
- Des conséquences d'informations erronées, incomplètes ou obsolètes fournies par le Client, l'Utilisateur habilité ou le RCPS ;
- De l'indisponibilité ou du dysfonctionnement de moyens d'authentification, de réseaux de communication ou de services tiers extérieurs au périmètre de responsabilité de Goodflag ;
- Des dommages indirects, pertes d'exploitation, pertes de chance, pertes financières ou pertes de données qui ne résultent pas directement d'un manquement démontré de Goodflag à ses obligations légales ou contractuelles ;
- De la confiance accordée par un UC ou une autre partie au-delà des limitations d'usage décrites dans les présentes CGU et dans les politiques applicables.

Le RCPS demeure responsable de l'usage de ses moyens d'authentification, du contrôle qu'il exerce sur sa volonté de signer et, plus généralement, du respect de ses propres obligations. Les limitations du présent article ne s'appliquent pas en cas de dol, de faute lourde ou lorsqu'une telle limitation est interdite par la loi applicable.

12. Droit applicable

Les présentes CGU sont soumises au droit français, sous réserve des règles impératives plus protectrices éventuellement applicables au RCPS lorsqu'elles ne peuvent être écartées par convention.

Les effets juridiques du cachet électronique qualifié, les obligations relatives au service de confiance et les conditions de preuve sont appréciés conformément au règlement eIDAS, aux normes applicables et au droit français.

13. Plaintes et règlement des litiges

Toute réclamation relative à l'utilisation du SCEQAD, au déroulement d'une Transaction de cachets, à l'émission d'un Certificat qualifié dans le cadre du service, ou à l'application des présentes CGU peut être adressée en premier lieu au support du Client qui a soumis les documents à signer, lorsqu'il est l'interlocuteur opérationnel du RCPS.

Lorsque la réclamation porte directement sur le fonctionnement du SCEQAD, sur la délivrance des Certificats qualifiés ou sur les engagements relevant de Goodflag / Lex Persona, elle peut également être adressée à Goodflag par les moyens de contact indiqués à l'article 15. Goodflag met en œuvre une procédure interne de traitement des plaintes et réclamations.

En cas de litige, les parties s'efforcent de rechercher une solution amiable. A défaut de règlement amiable, en cas de litige relatif à l'interprétation, la formation, la validité ou le respect des présentes CGU, et faute d'être parvenus à un accord ou à une transaction dans un délai d'un (1) mois à compter de l'apparition du différend, les Parties donnent compétence expresse et exclusive aux Tribunaux de Troyes, nonobstant pluralité de défendeurs, d'action en référé ou d'appel en garantie ou de mesure conservatoire.

14. Évaluation de conformité et schéma d'évaluation

Le SCEQAD relève d'un cadre normatif fondé notamment sur le règlement eIDAS, ETSI EN 319 401, ETSI EN 319 411-2 et ETSI TS 119 431-1. Lorsqu'il est présenté comme service de confiance qualifié ou lorsqu'une évaluation de conformité est requise, le service est destiné à être évalué ou est évalué selon le schéma de conformité applicable aux prestataires de services de confiance, par un organisme d'évaluation compétent et selon les référentiels en vigueur.

L'état de conformité du SCEQAD et le schéma d'évaluation effectivement appliqué sont indiqués dans la documentation de conformité mise à disposition par Goodflag / Lex Persona, le cas échéant dans son dépôt documentaire officiel, disponible sur le site de Goodflag / Lex Persona.

Lorsqu'une conformité a été évaluée, cette évaluation ne vaut que dans les limites du périmètre, de la version du service et du schéma d'évaluation concernés.

15. Coordonnées de contact

Les coordonnées de contact de Goodflag / Lex Persona pour les questions relatives au SCEQAD sont les suivantes :

Goodflag / Lex Persona
9, avenue Maréchal Leclerc
10120 Saint-André-les-Vergers
France
Courriel : pki-at-sunnystamp.com (remplacer les caractères « -at- » par « @ »)
Téléphone : +33 (0)3 25 43 90 78
Site de publication / repository : https://pki2.sunnystamp.com/repository

16. Engagements de disponibilité

Le SCEQAD est fourni avec un objectif de disponibilité compatible avec sa finalité de service de confiance. Sauf engagement particulier convenu avec le Client, le service est accessible en ligne vingt-quatre heures sur vingt-quatre et sept jours sur sept, hors cas de force majeure, opérations de maintenance, mises à jour, incidents de sécurité, défaillances de réseaux ou indisponibilités imputables à des services tiers ou à des composants extérieurs au périmètre de responsabilité de Goodflag.

Goodflag peut interrompre ou limiter temporairement l'accès au SCEQAD lorsque cela est nécessaire pour préserver la sécurité, l'intégrité, la confidentialité, la conformité ou la continuité du service. Lorsque les circonstances le permettent, une information appropriée est communiquée aux parties concernées.

Sauf stipulation expresse contraire, les présentes CGU ne constituent pas un engagement de niveau de service individualisé au bénéfice du Signataire.

17. Protection des données à caractère personnel

Dans le cadre du SCEQAD, Goodflag traite des données à caractère personnel nécessaires à l'authentification du RCPS, à la création de cachets électroniques qualifiés, à la constitution des journaux, et au respect des obligations légales et réglementaires applicables.

Selon les traitements concernés, Goodflag intervient soit en qualité de responsable de traitement, soit en qualité de sous-traitant pour le compte du Client, conformément au rôle réellement exercé pour l'opération considérée. Les données sont traitées conformément au règlement (UE) 2016/679 (RGPD), à la législation nationale applicable et au corpus documentaire de Goodflag relatif à la protection des données personnelles.

Le refus de fournir certaines données nécessaires à l'identification, à l'authentification ou à la preuve peut empêcher la poursuite de la Transaction, la délivrance du Certificat qualifié ou la création du cachet. Les personnes concernées peuvent exercer leurs droits auprès du Client lorsque celui-ci détermine les finalités du traitement, ou auprès de Goodflag selon les modalités d'information qui leur sont communiquées. Les coordonnées du délégué à la protection des données de Goodflag / Lex Persona sont dpo-at-goodflag.com (remplacer les caractères « -at- » par « @ »).

18. Confidentialité

Goodflag met en œuvre les mesures nécessaires pour protéger la confidentialité des informations dont il a la charge dans le cadre du SCEQAD. Sont notamment considérés comme confidentiels, sous réserve de leur nature et des obligations légales de publication, les journaux d'événements, les éléments de preuve, les données d'activation, les procédures internes de sécurité et les dossiers d'enregistrement associés au service.

Ne sont pas considérées comme confidentielles les informations qui doivent être publiées en application des textes, des normes ou des politiques applicables, notamment celles nécessaires à la vérification des Certificats et des cachets.

19. Sécurité

Le SCEQAD s'appuie sur un ensemble de mesures techniques et organisationnelles destinées à assurer la sécurité des opérations de cachet, notamment l'utilisation des Clés Privées exclusivement dans un QSCD, la non-exportation des Clés Privées, la mise en œuvre de données d'activation, la journalisation des événements sensibles, la protection des communications, le cloisonnement des environnements, ainsi que les mécanismes de supervision, de détection d'anomalies et de traitement des incidents.

Le module d'activation de cachet (SAM) utilisé dans le cadre du SCEQAD ne constitue pas lui-même un QSCD, mais il est exploité dans un environnement de sécurité destiné à garantir que l'activation du cachet ne peut intervenir qu'après authentification, contrôle de cohérence et expression explicite de la volonté du RCPS. Le cachet est créé exclusivement dans le QSCD.

Le RCPS reconnaît qu'Internet et les réseaux de communication peuvent présenter des risques résiduels. Il lui appartient de mettre en œuvre, sur ses propres équipements, les mesures de sécurité appropriées pour protéger son environnement, ses données et ses moyens d'authentification.

20. Effets juridiques et convention de preuve

Conformément au règlement eIDAS, l'effet juridique et la recevabilité comme preuve en justice d'un cachet électronique créé par le SCEQAD ne peuvent être refusés au seul motif que ce cachet se présente sous une forme électronique. Egalement, un cachet électronique qualifié produit par le SCEQAD bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié.

Les parties reconnaissent la valeur probante des journaux, éléments techniques, Certificats, horodatages, dossiers de preuve et autres données générés ou conservés dans le cadre du SCEQAD, sous réserve de l'appréciation souveraine des juridictions compétentes. Ces éléments ont vocation à établir, notamment, l'identité du RCPS, le déroulement de la Transaction, l'acceptation des CGU, l'authentification, l'acte de cachet et l'intégrité des documents signés.

Le recours au SCEQAD n'a pas pour effet de modifier les règles de validité matérielle des documents cachetés, ni les exigences substantielles éventuellement applicables aux documents concernés en vertu de textes spécifiques.

21. Dispositions finales

Si l'une quelconque des dispositions des présentes CGU était déclarée nulle, invalide ou inopposable, les autres stipulations demeureraient en vigueur, sauf si l'économie générale du document s'en trouvait affectée.

Goodflag peut faire évoluer les présentes CGU pour tenir compte d'une évolution du service, du cadre légal, réglementaire ou normatif, ou de ses pratiques documentées. Toute nouvelle version entre en vigueur à la date qu'elle indique et devient applicable aux utilisations postérieures du SCEQAD. Les présentes CGU sont rédigées en langue française. Elles peuvent être communiquées par voie électronique et conservées sur support durable.