CONDITIONS GENERALES D'UTILISATION DES CERTIFICATS 2D-DOC GOODFLAG

ARTICLE 1 : PRÉSENTATION DE LEX PERSONA / GOODFLAG

Lex Persona est une Société par Actions Simplifiée, dont le siège social est situé au 9 av. Maréchal Leclerc, 10120, Saint André-les-Vergers, France, ci-après dénommée Goodflag, représentée par David Coridun, son Directeur Général.

ARTICLE 2 : OBJET

Les présentes Conditions Générales d'Utilisation (CGU) ont pour objet de définir les conditions d'Utilisation du Service de fourniture de Certificat 2D-DOC (Certificat) délivré par l'Autorité de Certification (AC) FR07, conformément à la Politique de Certification/Déclaration des Pratiques de Certification (PC/DPC), à travers le Formulaire de demande de Certificat, le Formulaire de révocation de Certificat et le Formulaire de changement de Responsable de la Clé Privée du Sujet (RCPS) de Certificat. Lors de l'utilisation de l'un de ces Formulaires, le Demandeur reconnait :

- Avoir pris connaissance des présentes CGU et les accepter sans réserve ;
- Avoir transmis ces CGU au RCPS et au Représentant Légal (RL) de l'Entité Légale qui les acceptent également sans réserve ;
- Disposer de la pleine capacité juridique et des habilitations pour s'engager au titre des présentes CGU.

Les présentes CGU sont opposables, le cas échéant, au Demandeur, au RCPS, au RL de l'Entité Légale dès l'envoi d'un Formulaire par le Demandeur ainsi qu'aux Utilisateurs de Certificats (UC). Ils sont informés que leur engagement ne nécessite aucune signature. Les présentes CGU peuvent être modifiées à tout moment par Goodflag. Chaque nouvelle version des CGU entre en vigueur à compter de la date de sa publication. Concernant les Formulaires, les CGU applicables sont celles disponibles sur le Formulaire au moment de sa transmission. Le présent document tient également lieu de Déclaration d'IGC au sens de l'annexe A de [ETSI_319_411-1].

ARTICLE 3 : DÉFINITIONS

Les termes utilisés dans les présentes CGU écrits en majuscule ont, sauf stipulation contraire, la même définition que celle donnée dans cette section.

Autorité de Certification (AC)
Au sein d'un Prestataire de Service de Certification Électronique (PSCE), une AC a en charge, au nom et sous la responsabilité de ce PSCE, de l'application d'au moins une Politique de Certification / Déclaration des Pratiques de Certification (PC/DPC), et est identifiée comme telle, en tant qu'émetteur, dans les Certificats émis au titre de cette PC/DPC. L'AC sans épithète désigne l'AC dont le nom est FR07 qui délivre les Certificats 2D-DOC. Elle est gérée par Goodflag dont l'adresse est 9 av. Maréchal Leclerc, 10120, Saint André-les-Vergers, France. Courriel : pki-at-sunnystamp.com (après avoir remplacé les caractères « -at- » par le symbole « @ ») - Téléphone : +33 (0)3 25 43 90 78. Son site de publication est : https://pki2.sunnystamp.com/repository. Le site de publication est disponible 24h/24 et 7j/7 en conditions normales de fonctionnement.

Autorité d'Enregistrement

Les missions principales de l'Autorité d'Enregistrement (AE) consistent à :

- Vérifier l'identité d'un Sujet pour lequel est demandé un Certificat ;
- Vérifier l'identité de l'Entité Légale du Souscripteur qui demande un Certificat ;
- Vérifier que l'Entité Légale est bien un participant du programme 2D-DOC régi par l'ANTS
- Vérifier l'identité du Représentant Légal (RL) de l'Entité Légale du Souscripteur qui demande un Certificat ;
- Vérifier la capacité du RL vis-à-vis de l'Entité Légale du Souscripteur qui demande un Certificat ;
- Vérifier l'identité du Responsable de la Clé Privée du Sujet (RCPS) et sa nomination par un RL de l'Entité Légale du Souscripteur ;
- Authentifier et transmettre à l'AC toute demande de création et de révocation de Certificat ;
- Archiver les données relatives à l'identification du Sujet, du RCPS, de l'Entité Légale du Souscripteur et de son RL.

L'AE est gérée et opérée par Goodflag.

Bi-clé

Combinaison d'une Clé Privée et d'une Clé Publique utilisée pour effectuer des opérations cryptographiques.

Cachet

Chiffrement de l'empreinte de données à cacheter avec la Clé Privée associée à un Certificat de personne morale.

Certificat

Ensemble d'informations garantissant l'association entre l'identité d'un Sujet 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 :

- L'identité du Sujet du Certificat ;
- La Clé Publique du Sujet du Certificat ;
- Le(s) usage(s) autorisé(s) de la Clé publique ;
- La durée de vie du Certificat ;
- L'identité de l'AC ;
- La signature de l'AC.

Le format standard de Certificat est défini dans la recommandation X.509 v3 et dans la RFC 5280. Dans le cadre des présentes CGU, le terme Certificat sans épithète est utilisé pour désigner le Certificat 2D-DOC d'un Sujet.

Clé Privée

Clé d'une Bi-clé d'une entité devant être utilisée exclusivement par cette entité.

Clé Publique

Clé d'une Bi-clé d'une entité pouvant être rendue publique.

Code 2D-DOC
Un Code 2D-DOC est un type de codes-barres à deux dimensions de type Datamatrix constitué de modules noirs disposés dans un carré à fond blanc. L'agencement de ces points définit l'information que contient le Code 2D-DOC qui est sécurisée à l'aide d'une signature numérique fondée sur une cryptographie asymétrique avec des certificats de type ECDSA. Ce Code 2D-DOC respecte les spécifications définies par l'ANTS.

Déclaration des Pratiques de Certification (DPC)
Ensemble de pratiques qu'une AC met en œuvre pour émettre, gérer, révoquer et renouveler les Certificats qu'elle émet dans le cadre d'une PC.

Demandeur
Personne physique qui soumet un Formulaire à l'AE. A noter que le Demandeur ne signe jamais le Formulaire.

Entité Légale
Terme utilisé pour désigner exclusivement la personne morale à laquelle le Souscripteur et le Sujet sont rattachés, et au nom de laquelle ce dernier utilise son Certificat.

Formulaire
Terme qui désigne l'un des documents suivants fournis par l'AE : demande de Certificat, demande de révocation de Certificat et demande de changement de Responsable de la Clé Privée du Sujet (RCPS) de Certificat. Ces documents peuvent être au format PDF ou au format Web interactif. A un Formulaire peu(ven)t être associée(s) une ou plusieurs pièce(s) jointe(s) au format PDF.

Infrastructure de Gestion de Clés (IGC)
Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs Certificats utilisés par des services de confiance. Une IGC peut être composée d'une Autorité de Certification, d'un Opérateur de Certification, d'une Autorité d'Enregistrement centralisée et/ou locale, de Mandataires de Certification, d'une entité d'archivage, d'une entité de publication, etc.

Liste des Certificats Révoqués (LCR)
Fichier daté et signé, comportant, pour une période donnée, les informations relatives aux Certificats délivrés par une Autorité de Certification et qui ont été révoqués.

Object IDentifier (OID)
Identifiant universel, représenté sous la forme d'une suite d'entiers séparés par des points. Les OID sont organisés sous une forme hiérarchique avec des nœuds visant à faciliter l'interopérabilité entre différents logiciels.

Politique de Certification/Déclaration des Pratiques de Certification (PC/DPC)
Ensemble de règles, identifié par un nom une série de chiffres séparés par des points, définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC/DPC peut également, si

nécessaire, identifier les obligations et les exigences portant sur les autres intervenants, notamment les Sujets et les Utilisateurs de Certificat (UC).

Règlement eIDAS
Règlement de l'Union européenne no 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance. Lorsqu'il est fait spécifiquement référence à des modifications apportées par le règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le Règlement eIDAS, on citera alors le Règlement eIDAS (« version 2 »).

Réponse OCSP
Information retournée par l'AC, en temps réel et sur demande, indiquant le statut de révocation d'un Certificat délivré par l'AC.

Représentant Légal (RL)
Le Représentant Légal (RL) est une personne physique disposant des pouvoirs de représenter le Sujet de par la loi. Elle dispose de la faculté de procéder à des demandes d'émission et de révocation de Certificats au bénéfice des Sujets qu'elle aura expressément définis.

Responsable de la Clé Privée du Sujet
Un Responsable de la Clé Privée du Sujet (RCPS) est une personne physique agissant pour le compte du Souscripteur et qui est dûment mandaté par le Représentant Légal de ce dernier qui lui délègue les responsabilités suivantes :

- La responsabilité de la Clé Privée associée à la Clé Publique contenue dans le Certificat ;
- La responsabilité des étapes du cycle de vie du Certificat, et en particulier celles qui consistent à :
    - Se faire remettre un Certificat par l'Autorité d'Enregistrement ;
    - Procéder le cas échéant à la demande de révocation d'un Certificat.

Le Responsable de la Clé Privée du Sujet est enregistré par l'Autorité d'Enregistrement et est en relation directe avec elle. La nomination d'un Responsable de la Clé Privée du Sujet est obligatoire.

Service de création de Cachets
Service de confiance de création de Cachets opéré par Goodflag et pouvant être mis à disposition d'un Souscripteur pour lui permettre de cacheter des Codes 2D-DOC ou des documents par une personne morale dans le cadre d'une Transaction de Cachet, à l'aide d'un Certificat approprié délivré par l'Autorité de Certification. La Clé Privée du Sujet, associée au Certificat, est générée par l'Autorité de Certification et utilisée de manière sécurisée par le Service de création de Cachets pour signer les Codes 2D-DOC ou les documents de la Transaction de Cachet. Dans le contexte d'utilisation du Service de création de Cachets, le Souscripteur, via son Responsable de la Clé Privée du Sujet, met en œuvre des mécanismes d'authentification forte, fournis par l'Autorité d'Enregistrement, permettant d'assurer que seuls les Certificats des Sujets du Souscripteur seront mis en œuvre dans le cadre de ses Transactions de Cachet.

Souscripteur
Le Souscripteur est une Entité Légale qui demande un Certificat pour un Sujet par l'intermédiaire d'un Responsable de la Clé Privée du Sujet. Dès lors qu'un Responsable de la Clé Privée du Sujet ne

peut plus assumer les responsabilités décrites ci-dessus (du fait d'un changement d'affectation, du départ de l'entreprise, de la rupture du contrat de service avec le Responsable de la Clé Privée du Sujet ou de l'entité de laquelle il dépend, etc.), le Souscripteur doit :

- Nommer un nouveau Responsable de la Clé Privée du Sujet à l'aide du Formulaire de demande de changement de RCPS ;
- Ou effectuer une demande de révocation auprès de l'Autorité d'Enregistrement.

Sujet

Un Sujet est une application, un service, un serveur qui utilise le Certificat et sa Clé Privée associée pour sécuriser des données informatiques afin de garantir leur intégrité et leur authenticité. Le Sujet est identifié dans le Certificat comme ayant la capacité de mettre en œuvre la Clé Privée associée à la Clé Publique contenue dans le Certificat. Dans le cas d'un Certificat 2D-DOC le Sujet comporte 4 caractères seulement.

Transaction de Cachet

Opération de courte durée, gérée par le Service de création de Cachets, durant laquelle le Certificat d'un Sujet est mis en œuvre, et permettant d'apposer un Cachet électronique sur des données de cette transaction avec sa Clé Privée « distante » associée à son Certificat et opérée par le Service de création de Cachets.

Utilisateur de Certificats (UC)

Toute personne physique ou morale qui utilise un Certificat délivré par l'AC, pour ses propres besoins, et qui doit pour cela le vérifier préalablement.

ARTICLE 4 : CARACTÉRISTIQUES DES CERTIFICATS

L'AC délivre des Certificats au RCPS nommé et identifié par un Représentant Légal de l'Entité Légale du Souscripteur. Ces Certificats ont une durée de validité maximale de 3 ans et ne peuvent être utilisés que pour cacheter les documents de la Transaction de Cachet pour laquelle ils ont été spécialement créés.

L'AC délivre ainsi deux types de Certificats :

- Les certificats utilisés par ses répondeurs OCSP pour signer les réponses OCSP, qui disposent d'une Clé Privée de type RSA 2048 bits ;
- Les Certificats 2D-DOC « ETSI QCP à destination de personnes morales », identifiés par l'OID 1.3.6.1.4.1.22542.100.1.1.5.2, conformes à la norme [ETSI_319_411-2] pour le niveau QCP-l, qui disposent d'une Clé Privée de type ECDSA FRP256v1.

L'AC est elle-même émise par l'AC racine « Sunnystamp Root CA G2 » et leur certificats sont disponibles à l'adresse suivante : https://pki2.sunnystamp.com/repository.

ARTICLE 5 : FORMULAIRE DE DEMANDE DE CERTIFICAT

Le Formulaire de demande de Certificat au format Web doit être dument complété par le Demandeur avec les informations suivantes :

- Informations relatives au Demandeur, à l'Entité Légale, au Représentant Légal, au RCPS ;
- Informations relatives au Sujet du Certificat 2D-DOC.

Le Demandeur doit également téléverser via le Formulaire les pièces suivantes :

- Un Kbis ou un avis de situation SIRENE de l'Entité Légale ;
- Un justificatif de participation de l'Entité Légale au programme 2D-DOC ;
- Tout document justifiant de la qualité de RL de l'Entité Légale.

Ce Formulaire doit également fournir une demande de Certificat d'authentification au format PKCS#10 générée par le RCPS, qui permettra à l'AC de fournir un Certificat d'authentification au RCPS. Ce Certificat d'authentification permettra à l'AC de chiffrer les données d'activation du Certificat 2D-DOC à l'attention du RCPS, et, le cas échéant, d'authentifier le serveur métier du Souscripteur lorsque ce dernier accède au Service de création de Cachets.

De manière optionnelle, le Formulaire pourra comporter l'adresse IP du serveur métier du Souscripteur afin de permettre au Service de création de Cachets de l'authentifier au lieu d'utiliser le Certificat d'authentification.

Le Formulaire de demande au format Web doit ensuite être envoyé par le Demandeur directement à l'Autorité d'Enregistrement Goodflag (AE) via le bouton prévu à cet effet dans le Formulaire. Les informations communiquées au sein du Formulaire de demande de Certificat ne pourront être modifiées une fois le Formulaire signé. Il appartient au Demandeur et au RCPS de s'assurer que le Formulaire ne présente aucune information erronée. L'Entité Légale reconnait et accepte qu'en cas d'informations erronées, une fois le Formulaire signé, elle devra effectuer un nouveau paiement pour un nouveau Certificat et remplir un nouveau Formulaire de demande de Certificat.

ARTICLE 6 : CONTRÔLE DE LA DEMANDE DE CERTIFICAT

L'AE effectue un contrôle qui permet :

- De vérifier l'identité de l'Entité Légale à l'aide des informations fournies sur le Kbis ou, le cas échéant, l'avis de situation SIRENE ;
- De vérifier la capacité du RL de l'Entité Légale à l'aide des informations fournies sur le Kbis ou sur tout document fourni à cet effet ;
- De vérifier la participation de l'Entité Légale au programme 2D-DOC ;
- De vérifier l'identité du RCPS et du RL de l'Entité Légale en vérifiant les signatures électroniques qualifiées du Formulaire au format PDF et de ses pièces jointes associées ;
- De vérifier chaque champ du Certificat.

L'AE notifiera le Demandeur de tout Formulaire de demande de Certificat incomplet ou incorrect à l'adresse courriel renseignée par le Demandeur, et ce dernier devra adresser le Formulaire de demande modifié ou complété des informations erronées ou manquantes dans un délai de 10 jours ouvrés.

L'AE dispose d'un délai maximum de 5 jours ouvrés pour contrôler la demande de Certificat. Lorsque le Formulaire de demande de Certificat a été vérifié par l'AE, cette dernière l'envoie pour signature électronique qualifiée au RL puis au RCPS avec les pièces justificatives fournies. Ces derniers disposent d'un délai de 10 jours ouvrés pour signer le Formulaire ou, le cas échéant, émettre des objections.

ARTICLE 7 : LIVRAISON ET ACCEPTATION DU CERTIFICAT 2D-DOC

La confection du Certificat et du Certificat d'authentification associé, ainsi que le paramétrage du Service de création de Cachets sont effectués dans un délai maximum de 5 jours ouvrés après la signature du Formulaire de demande par le RL et le RCPS.

Ces opérations donnent lieu à la fourniture d'un fichier de livraison adressé par courriel par l'AE au RCPS et au Demandeur. En cas de non réception du fichier de livraison, il appartient à ces derniers d'en effectuer le signalement auprès de l'AE et, le cas échéant, de demander la révocation du Certificat auprès de l'AE. L'absence de réponse au courriel du fichier de livraison dans les 24h qui suivent son envoi par l'AE vaut acceptation du Certificat 2D-DOC et du Certificat d'authentification par le RCPS.

Le fichier de livraison est un fichier au format « texte » qui contient les éléments suivants :

- Le Certificat 2D-DOC au format PEM ;
- L'URL du Service de création de Cachets ;
- Les données d'activation de la Clé Privée du Certificat 2D-DOC, nécessaires au serveur métier pour appeler le Service de création de Cachets ;
- Le Certificat d'authentification associé au RCPS au format PEM, qui peut servir à l'authentification du serveur métier vis-à-vis du Service de création de Cachets, le cas échéant.

Le fichier de livraison est ensuite chiffré par l'AC à l'aide de la clé publique du Certificat d'authentification associé au RCPS, au format texte encodé en Base64. Il appartient alors au RCPS de déchiffrer le fichier de livraison à l'aide de la Clé Privée correspondant au Certificat d'authentification.

ARTICLE 8 : ENTRÉE EN VIGUEUR - DURÉE

Les présentes CGU entrent en vigueur à la date d'envoi du Formulaire et prendront fin au jour de la fin de validité de la Bi-clé. La durée de vie de la Bi-clé est de 3 ans.

ARTICLE 9 : CONDITIONS DE REMBOURSEMENT

L'envoi d'un Formulaire de demande de Certificat entraine l'émission du Certificat par l'AC. Dès lors, la demande ne peut être annulée et aucun remboursement n'est possible. En revanche, en cas d'erreur imputable à l'AE ou l'AC ayant pour conséquence que le Certificat émis ne correspond pas au Formulaire de demande, un nouveau Certificat sera émis.

ARTICLE 10 : OBLIGATION DES PARTIES

1. Le Demandeur reconnait avoir l'obligation de communiquer des informations exactes à l'AE.

2. Le RCPS reconnait, le cas échéant, avoir l'obligation de :

- Vérifier les informations renseignées au sein d'un Formulaire par le Demandeur ;
- Maintenir la Clé Privée sous le seul contrôle de la personne morale associée ;

- Cesser toute utilisation de la Clé Privée en cas de compromission, ou suspicion de compromission de la Clé Privée ;
- Informer sans délai l'AE de toute perte, vol, compromission ou suspicion de compromission de la Clé Privée ;
- Respecter les usages autorisés du Certificat ;
- Demander à l'AE la révocation du Certificat lors de la survenance d'un des faits énumérés dans la PC à l'aide du Formulaire de révocation de Certificat ;
- Cesser toute utilisation de la Clé Privée en cas de compromission, ou suspicion de compromission de l'AC ;
- Signer les Formulaires qui lui sont adressés par l'AE.

3. Le RL reconnait, le cas échéant, avoir l'obligation de :
- Vérifier les informations renseignées au sein du Formulaire par le Demandeur ;
- Maintenir la Clé Privée sous le seul contrôle de la personne morale associée ;
- Informer sans délai l'AE de toute perte, vol, compromission ou suspicion de compromission de la Clé Privée ;
- Informer sans délai l'AE en cas de modification des informations contenues dans le Certificat. En cas de changement de RCPS, il doit remplir ou faire remplir sans délai le Formulaire de changement de RCPS de Certificat ;
- Respecter les usages autorisés du Certificat ;
- Demander à l'AE la révocation du Certificat lors de la survenance d'un des faits énumérés dans la PC à l'aide du Formulaire de révocation de Certificat ;
- Signer le Formulaire qui lui est adressé.

ARTICLE 11 : OBLIGATION DE GOODFLAG

1. L'AC à l'obligation de :
- Se conformer aux normes et règlementations (notamment au règlement eIDAS) ;
- Gérer une Liste des Certificats Révoqués (LCR) pour permettre la vérification du statut de révocation des certificats ;
- Révoquer sous 24h un Certificat en cas de compromission de la Clé Privée ou sur demande de l'AE, du RL ou du RCPS ;
- Mettre en place un plan de continuité d'activité ;
- Vérifier le Formulaire qui lui est adressé ;
- Se conformer à la PC.

2. L'AE à l'obligation de :
- Identifier et vérifier l'identité des personnes concernées (RCPS, Représentant Légal) ainsi que celle de l'Entité Légale ;
- Appliquer la PC et notamment vérifier tous les attributs du champ « Subject » à renseigner dans le Certificat, à l'exception de l'attribut « serialNumber », et tout document permettant de justifier le lien entre l'attribut « O » et l'Entité Légale du Souscripteur si ces informations diffèrent ;
- Traiter les demandes de révocation ;
- Assurer la confidentialité et la sécurité des données recueillies tout au long du cycle de vie du Certificat ;

- Signer les Formulaires qu'elle émet.

ARTICLE 12 : PUBLICATION DES CERTIFICATS

Le Certificat ne fait l'objet d'aucune publication par l'AC à l'exception d'un Certificat 2D-DOC qui est publié, dans un délai de 24h maximum après son émission, dans un annuaire destiné à permettre la vérification des Cachets correspondants.

ARTICLE 13 : USAGE DU CERTIFICAT

1. Généralités
Le Certificat 2D-DOC permet au Service de création de Cachets de Goodflag, de cacheter des Codes 2D-DOC ou des documents dans le but de garantir leur intégrité, leur authenticité ainsi que leur contenu.

2. Utilisation de la Clé Privée et du Certificat par le Sujet
L'utilisation par le Sujet, de sa Clé Privée et de son Certificat associé, est strictement limitée au Service de création de Cachets et doit respecter :
- Les exigences définies dans [PC/DPC], en particulier les usages définis dans la section 1.4 ;
- Les CGU ;
- Toute obligation supplémentaire éventuellement imposée au RCPS par le Souscripteur, ne remettant pas en cause les clauses précédentes.

La Clé Privée du Sujet est utilisée exclusivement par le Service de création de Cachets sous le contrôle du RCPS, qui l'utilise dans le cadre d'une Transaction de Cachet spécifique. L'accès au Service de création de Cachets nécessite :
- D'une part l'utilisation des données d'activation du Certificat transmises au RCPS concomitamment à sa délivrance par l'AE de manière sécurisée ; et,
- D'autre part l'authentification du serveur métier du Souscripteur effectuée 1) soit à l'aide du Certificat d'authentification (transmis par l'AC lors de la délivrance du Certificat 2D-DOC) et dont la Clé Privée est sous le contrôle exclusif du RCPS, 2) soit à l'aide de l'adresse IP du serveur métier du Souscripteur transmise dans le formulaire de demande de Certificat.

3. Stockage de la Clé Privée
La Clé Privée relative au Certificat 2D-DOC du Sujet est générée et utilisée exclusivement sur un dispositif cryptographique de type HSM certifié FIPS 140-2 level 3.

ARTICLE 14 : UTILISATEURS DU CERTIFICAT (UC)

Les obligations des UC sont les suivantes :
- Respecter les obligations décrites dans les présentes CGU ;
- Vérifier que l'extension « KeyUsage » contenue dans le Certificat est conforme à l'utilisation du Certificat ;
- Vérifier que l'OID de la PC/DPC est contenu dans l'extension « Certificate Policies » du Certificat ;

- Vérifier la validité de la chaîne de certification (dates de validité, signature des Certificats, statut de révocation) en partant du Certificat du Sujet et en remontant au moins jusqu'au certificat de l'AC.

ARTICLE 15 : CONFORMITÉ RÈGLEMENTAIRE

Le Certificat émis est conforme aux éléments précisés dans la PC. L'AE garantit le délai de livraison et la conformité du Certificat à la règlementation en vigueur et notamment au règlement eIDAS.
L'AC est certifiée conforme, pour les certificats référencés par l'OID 1.3.6.1.4.1.22542.100.1.1.5.2 pour les Certificats 2D-DOC, conformes à la norme [ETSI_319_411-2] au niveau QCP-l.

Le certificat de conformité est valable 2 ans et est délivré à la suite d'un audit réalisé par un organisme accrédité selon la norme [ETSI_319_403]. En complément de ces certifications, l'AC fait également qualifier les mêmes offres suivant le référentiel de qualification de services de l'ANSSI (https://cyber.gouv.fr/referentiels-dexigences-anssi) pour intégrer la Liste des Services de Confiance eIDAS (https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home).

Les références documentaires utilisées dans les présentes CGU sont les suivantes :

- [ETSI_319_403] : ETSI EN 319 403 V2.3.1 (2020-06). Trust Service Provider Conformity Assessment. Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers. https://www.etsi.org/deliver/etsi_en/319400_319499/31940301/02.03.01_60/en_31940301v020301p.pdf.
- [ETSI_319_411-1] : ETSI EN 319 411-1 V1.4.1 (2023-10). Policy and security requirements for Trust Service Providers issuing certificates. Part 1: General requirements. https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.04.01_60/en_31941101v010401p.pdf.
- [ETSI_319_411-2] : ETSI EN 319 411-2 V2.5.1 (2023-10). Policy and security requirements for Trust Service Providers issuing certificates. Part 2: Requirements for trust service providers issuing EU qualified certificates. https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.05.01_60/en_31941102v020501p.pdf.

ARTICLE 16 : FIN DE VIE DU CERTIFICAT

1. Révocation. Les circonstances donnant lieu à la révocation du Certificat sont évoquées dans la PC. Il s'agit notamment des cas de compromission d'un élément de sécurité, de demande du RCPS, du RL, de l'AE, de l'AC. La demande de révocation peut être également liée à un défaut de règlement. Toute demande de révocation du Certificat par l'Entité Légale par l'intermédiaire du RCPS ou du RL doit être adressée à l'AE par l'intermédiaire du Formulaire de demande de révocation de Certificat 2D-DOC. Une fois le Formulaire de demande de révocation vérifié par l'AE, cette dernière l'envoie pour signature électronique qualifiée à la personne à l'origine de la demande de révocation. Toute demande de révocation sera traitée dans un délai maximal d'1 jour ouvré.

2. Expiration du Certificat. Le RCPS et le RL seront informés de l'expiration prochaine du Certificat, dans un délai de 3 mois en amont de celle-ci, à leur adresse de courriel figurant dans le Formulaire de demande de Certificat.

3. Renouvellement du Certificat. Il n'y a pas de processus de renouvellement des Certificats.

ARTICLE 17 : CHANGEMENT DE RCPS

En cas de changement de RCPS, l'Entité Légale devra adresser sans délai le Formulaire de Changement de RCPS à l'AE. Tout manquement à cette obligation peut entrainer la révocation du Certificat par l'AC. Une fois le Formulaire de demande de changement de RCPS vérifié par l'AE, cette dernière l'envoie pour signature électronique qualifiée au nouveau RCPS et au RL avec les pièces justificatives demandées. Ces derniers disposent d'un délai de 5 jours ouvrés pour signer le Formulaire ou, le cas échéant, émettre des objections. Toute demande sera traitée dans un délai maximal de 5 jours ouvrés.

ARTICLE 18 : SIGNALEMENT D'UN CERTIFICAT MALVEILLANT OU DANGEREUX

Pour signaler un Certificat potentiellement malveillant ou dangereux (par exemple, en cas de suspicion de compromission de la Clé Privée, d'utilisation non conforme ou non autorisée, ou tout autre type de fraude : détournement d'usage, comportement inapproprié, etc.), ou pour tout autre problème lié au Certificat, veuillez contacter Goodflag à l'adresse certificat-at-goodflag.com (après avoir remplacé les caractères « -at- » par le symbole « @ ») en indiquant en objet « Certificat suspecté malveillant ou dangereux ».

ARTICLE 19 : MARQUE

1. Goodflag reste seule propriétaire de ses marques, noms, logos, sigles, graphismes et autres signes distinctifs.

2. L'Entité Légale s'interdit de porter atteinte à l'ensemble de ces signes distinctifs de manière directe ou indirecte et de quelque façon que ce soit. En particulier l'Entité Légale s'interdit de modifier, retirer, masquer, altérer, déplacer, en tout ou partie, par quelque moyen que ce soit, tout signe distinctif de Goodflag.

ARTICLE 20 : DONNÉES PERSONNELLES

Les informations communiquées sont traitées dans le strict respect des lois et règlements en vigueur, en particulier de la loi n°78-17 modifiée du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que le règlement européen 2016/679 du 27 avril 2016 sur la protection des données personnelles. Les données personnelles communiquées sont enregistrées dans un fichier informatisé pour l'enregistrement de la demande de certificat, le contrôle des informations, la fourniture, la révocation et l'expiration du Certificat et la gestion des dossiers clients. Ces données personnelles sont confidentielles et ne seront utilisées que dans les finalités visées. Elles sont conservées pendant une durée de 7 ans à compter de la date d'expiration du Certificat. Pendant cette période, Goodflag met en place tous moyens aptes à assurer la confidentialité et la sécurité

des données personnelles délivrées par l'Entité Légale, de manière à empêcher leur endommagement, effacement ou accès par des tiers non autorisés. Goodflag s'engage à ne pas divulguer à des tiers autres que ses sous-traitants, les données personnelles sans l'autorisation préalable de la personne concernée à moins d'y être contraints en raison d'un motif légitime (obligation légale, lutte contre la fraude ou l'abus, exercice des droits de la défense, etc.). Les sous-traitants en question sont soumis à une obligation de confidentialité et ne peuvent utiliser les données personnelles qu'en conformité avec nos dispositions contractuelles et la législation applicable. Le délégué à la protection des données de Goodflag est joignable à l'adresse de courriel suivante : dpo-at-goodflag.com (après avoir remplacé les caractères « -at- » par le symbole « @ »). Les personnes concernées peuvent exercer leur droit d'accès, de rectification, de portabilité, d'effacement ou de limitation de traitement aux données les concernant et les faire rectifier ou supprimer en contactant : Goodflag, 9 avenue Maréchal Leclerc 10120 Saint-André-les-Vergers France ou par courriel à dpo-at-goodflag.com (après avoir remplacé les caractères « -at- » par le symbole « @ »). Les personnes concernées disposent également d'un droit d'opposition au traitement de leurs données pour des motifs légitimes sauf si ces données sont collectées pour respecter une obligation légale, si elles sont nécessaires à l'exécution d'un contrat auquel elles sont parties ou encore si elles sont utilisées pour une finalité pour laquelle elles ont donné leur accord. Elles ont la possibilité d'introduire toute réclamation auprès de la Commission Nationale Informatique et Libertés (CNIL).

ARTICLE 21 : RESPONSABILITÉ

Goodflag ne pourra pas être tenue pour responsable d'une utilisation non autorisée ou non conforme des données d'authentification, des certificats, des LCR, ainsi que de tout autre équipement ou logiciel mis à disposition. Goodflag décline sa responsabilité pour tout dommage direct ou indirect résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le Sujet.

ARTICLE 22 : CONFIDENTIALITÉ

Il est convenu entre les Parties que les informations échangées à l'occasion du traitement des Formulaires sont confidentielles. Chaque Partie ne communiquera les informations confidentielles communiquées par l'autre Partie qu'aux seules personnes, salariés ou tiers, dont il sera nécessaire qu'elles en connaissent pour l'exécution ou la gestion de la demande. Les Parties sont tenues de préserver le caractère confidentiel desdites informations en prenant au moins les mêmes dispositions que celles qu'elles prennent habituellement pour protéger leurs propres informations confidentielles de nature analogue et devront faire respecter à l'ensemble de leur personnel et prestataires intéressés, quel que soit leur statut, la même obligation de secret et de confidentialité pour l'ensemble des informations visées ci-dessus. De manière expresse, les Parties conviennent que ne seront pas considérées comme confidentielles :

- Les informations tombées dans le domaine public par une voie autre que le non-respect du présent engagement de confidentialité ;
- Les informations précédemment connues de la Partie réceptrice qui ne sont pas soumises à une obligation de confidentialité ;
- Les informations obtenues de manière licite auprès d'un tiers.

Les dispositions du présent article demeureront en vigueur pendant toute la durée de validité de la Bi-clé et pendant une durée de deux ans à compter de sa fin, pour quelque cause que ce soit.

ARTICLE 23 : DISPOSITIONS DIVERSES

1. Si une ou plusieurs stipulations des CGU sont tenues pour non valides ou déclarées telles en application d'une loi, d'un règlement ou à la suite d'une décision définitive d'une juridiction compétente, les autres stipulations garderont toute leur force et leur portée.

2. En cas de difficulté d'interprétation ou de contradiction entre l'un quelconque des titres figurant en-tête des clauses, et l'une quelconque des clauses, les titres seront déclarés inexistants.

ARTICLE 24 : LOI APPLICABLE - ATTRIBUTION DE COMPÉTENCE

Les Présentes CGU sont régies par le droit français. L'AC dispose d'une procédure de gestion des plaintes et réclamations qui consiste pour le demandeur à ouvrir un ticket sur le site de support de l'AC : https://support.lex-persona.com. EN CAS DE LITIGE ET APRÈS TENTATIVE D'UNE CONCILIATION AMIABLE, COMPÉTENCE EXPRESSE EST ATTRIBUÉE AU TRIBUNAL DE COMMERCE DE TROYES, NONOBSTANT PLURALITÉ DE DÉFENDEUR OU APPEL EN GARANTIE, MÊME POUR LA PROCÉDURE D'URGENCE OU LES PROCÉDURES CONSERVATOIRES, EN RÉFÉRÉ OU PAR REQUÊTE.

ANNEXE 1 : ACRONYMES

Acronyme	Définition
AC	Autorité de Certification
AE	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANTS	Agence Nationale des Titres Sécurisés
CGU	Conditions Générales d'Utilisation
DN	Distinguished Name
DPC	Déclarations des Pratiques de Certification
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	electronic IDentification And trust Services
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
IGC	Infrastructure de Gestion de Clés
LCP	Lightweight Certificate Policy
LCR	Liste de Certificats Révoqués
LPTSP Board	Lex Persona Trust Service Provider Board
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PC	Politique de Certification
PCA	Plan de Continuité d'Activité
PDF	Portable Document Format
PKCS	Public Key Cryptographic Standard
PSCE	Prestataire de Service de Certification Électronique
QCP	Qualified Certificate Profile
QSCD	Qualified Signature Creation Device
RCPS	Responsable de la Clé Privée du Sujet
RL	Représentant Légal
RFC	Request For Comment
UC	Utilisateurs de Certificat
UE	Union Européenne