Accord d'Utilisation des Certificats délivrés par l'Infrastructure de Gestion de Clés Sunnystamp

Version 1.2 applicable à partir du 16/06/2021

Préambule

Toute personne qui reçoit ou consulte un document signé électroniquement doit vérifier le Certificat qui a servi à la signature dudit document.

De manière similaire, toute personne qui vérifie un horodatage (également appelé contremarque de temps) doit vérifier le Certificat qui a servi à certifier l'horodatage.

Egalement, toute personne qui vérifie un Certificat, dès lors qu'il n'est pas une ancre de confiance et/ou auto signé, doit vérifier le Certificat « parent » qui a délivré ledit Certificat.

Enfin, toute personne qui reçoit, télécharge ou consulte un Certificat peut librement accéder à son contenu et doit vérifier les conditions d'utilisation des données qu'il contient.

Ces obligations s'imposent à la personne qui devient de facto un « Utilisateur de Certificat », dénommé UC dans la suite du document.

1 Objet du document

L'Infrastructure de Gestion de Clés (IGC) Sunnystamp met à la disposition des UC les moyens nécessaires à la vérification des Certificats délivrés par l'IGC Sunnystamp, qui sont :

- Des Certificats d'Autorités de Certifications (AC) qui permettent à l'UC de construire un chemin complet de certification du Certificat à vérifier jusqu'à l'atteinte d'un Certificat considéré par l'UC comme une ancre de confiance ;
- Des Listes de Certificats Révoqués (LCR) des Certificats de signature, d'horodatage ou d'AC, qui permettent à l'UC de vérifier le statut de révocation de ces Certificats ;
- Des répondeurs OCSP qui permettent à l'UC de vérifier le statut de révocation d'un Certificat en temps réel.

En accédant au contenu d'un Certificat délivré par l'IGC Sunnystamp et/ou en utilisant les informations décrites ci-dessus dans le contexte de la vérification d'un certificat délivré par l'IGC Sunnystamp, l'UC accepte et consent sans réserve aux termes du présent Accord.

2 Durée de l'accord

Le présent Accord prend effet :

- Au moment du téléchargement par l'UC d'un Certificat délivré par l'IGC Sunnystamp ;
- Au moment de la consultation et/ou de l'utilisation par l'UC des informations contenues dans un Certificat délivré par l'IGC Sunnystamp ;
- Au moment du téléchargement par l'UC d'une LCR délivrée par l'IGC Sunnystamp ;
- Au moment de la consultation et/ou de l'utilisation par l'UC des informations contenues dans une LCR délivrée par l'IGC Sunnystamp ;
- Au moment de la connexion par l'UC à un répondeur OCSP de l'IGC Sunnystamp ;
- Au moment de la consultation et/ou de l'utilisation par l'UC des informations contenues dans une réponse OCSP délivrée par l'IGC Sunnystamp.

Le présent Accord reste en vigueur tant que l'UC s'appuie sur l'une quelconque des informations ou des usages décrits ci-dessus.

3 Définitions et acronymes

Autorité de Certification (AC)
Au sein d'un Prestataire de Service de Certification Electronique (PSCE), une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une PC/DPC et est identifiée comme telle, en tant qu'émetteur (champ « issuer » du Certificat).

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'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.

Clé Privée : clé d'une bi-clé asymétrique d'une entité devant être utilisée exclusivement par cette entité.

Clé Publique : clé d'une bi-clé asymétrique d'une entité pouvant être rendue publique.

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

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.

Horodatage : cachetage électronique effectué sur des données associées à un temps particulier visant à garantir l'antériorité des données vis-à-vis de ce temps particulier. Est également appelé contremarque de temps.

Liste des Certificats Révoqués (LCR) : liste signée, publiée par une AC et contenant à un instant donné la liste des Certificats révoqués par l'AC.

Object Identifier (OID) : identifiant universel, représenté sous la forme d'une suite d'entiers. Les OID sont organisés sous une forme hiérarchique avec des nœuds visant à faciliter l'interopérabilité entre différents logiciels.

Politique de Certification (PC)
Ensemble de règles, identifié par un OID), définissant les exigences auxquelles une Autorité de Certification 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 UC.

Répondeur OCSP : service qui renseigne sur le statut de révocation d'un Certificat en publiant son statut sous la forme d'un contenu signé par un certificat de répondeur OCSP. De fait, ce contenu signé est appelé « réponse OCSP ». OCSP est l'acronyme de « Online Certificate Status Protocol ».

Signature électronique : processus consistant à chiffrer l'empreinte d'un contenu à l'aide de la Clé Privée correspondant à la Clé Publique associée à un Certificat. La vérification de cette signature électronique nécessite donc d'accéder à la Clé Publique fournie dans le Certificat dont il est par conséquent nécessaire d'en vérifier l'intégrité et l'authenticité en vue de garantir l'identité du signataire associé. De plus à une signature électronique est généralement associée un acte juridique réalisé par le signataire à l'origine de l'opération.

Utilisateur de Certificats (UC) : toute personne physique ou morale qui utilise un Certificat délivré par l'une des AC de l'IGC Sunnystamp, pour ses propres besoins, et qui doit pour cela le vérifier préalablement.

4 Acceptation

Par le présent Accord, l'UC reconnait et accepte :

- Qu'il dispose de l'ensemble des informations nécessaires pour décider d'utiliser les données figurant dans un Certificat ou une LCR ou une réponse OCSP délivré par l'IGC Sunnystamp ;
- Qu'en cas de manquement de l'UC aux obligations définies par le présent Accord, il est seul responsable des dommages qui pourraient en résulter.

5 Certificats émis par l'IGC Sunnystamp

Les Certificats émis par l'IGC Sunnystamp qui définissent le périmètre du présent accord sont les suivants :

- Le Certificat de l'AC racine auto signée de l'IGC Sunnystamp « Sunnystamp Root CA G2 » ;
- Le Certificat de l'AC intermédiaire « Sunnystamp Natural Persons CA » ;
- Les Certificats destinés à des personnes physiques représentées ou non par une Entité Légale et délivrés par l'AC intermédiaire « Sunnystamp Natural Persons CA » ;
- Le Certificat de l'AC intermédiaire « Sunnystamp Legal Persons CA » ;
- Les Certificats d'horodatage destinés à des personnes morales et délivrés par l'AC intermédiaire « Sunnystamp Legal Persons CA » ;
- Les Certificats de signature de réponses OCSP.

Les Autorités de Certification identifiées ci-dessus sont conformes aux règles et aux exigences prévues par les politiques identifiées dans le tableau suivant :

Certificat d'AC	OID de la PC du certificat émis	Certification de la PC	Description / délivre
Sunnystamp Root CA G2	1.3.6.1.4.1.22542.100.1.1.0.1	ETSI EN 319 411-1 NCP+	AC Racine de l'IGC / AC intermédiaire
Sunnystamp Natural Persons CA	1.3.6.1.4.1.22542.100.1.1.1.2	ETSI EN 319 411-1 LCP	AC intermédiaire / Certificat mono-transaction de personne physique ETSI LCP Certificat technique de réponse OCSP
	1.3.6.1.4.1.22542.100.1.1.1.3	Aucune	AC intermédiaire / Certificat mono-transaction de personne physique OPEN REG Certificat technique de réponse OCSP
Sunnystamp Legal Persons CA	1.3.6.1.4.1.22542.100.1.1.2.2	ETSI EN 319 411-1 NCP+	AC Intermédiaire / Certificats d'horodatage ETSI NCP+ Certificat technique de réponse OCSP
	1.3.6.1.4.1.22542.100.1.1.2.3	Aucune	AC Intermédiaire / Certificats d'horodatage logiciel Certificat technique de réponse OCSP

6 Obligations de l'UC

Un UC doit :

- Vérifier que le Certificat a bien été délivré par l'AC ;
- Vérifier si le Certificat est conforme aux exigences techniques, fonctionnelles, légales, règlementaires ou normatives appropriées à l'usage qu'il souhaite en faire ;
- Vérifier que l'OID de la PC contenu dans le Certificat d'entité finale correspond bien à celui de la PC applicable dans le présent accord ;
- Vérifier le statut de révocation du Certificat, ainsi que la validité de l'ensemble des certificats constituant la chaîne de certification, en consultant notamment les informations de révocation publiées par l'AC et dont les URL sont indiquées dans le Certificat (LCR(s) ou répondeur(s) OCSP) ;
- Utiliser les logiciels et matériels adéquats pour vérifier les signatures électroniques et les horodatages qu'il souhaite utiliser.

7 Limites de l'utilisation d'un Certificat

L'IGC Sunnystamp ne peut être tenue responsable d'une utilisation inappropriée du Certificat au regard de la PC y afférente.

L'UC est informé, par le présent Accord que la Clé Privée associée au Certificat qu'il souhaite utiliser est potentiellement soumise au risque de compromission ou de vol. Bien que l'IGC Sunnystamp prenne toutes les mesures qu'elle peut mettre en œuvre pour éviter qu'un tel évènement se produise, ce dernier peut ne pas être détecté immédiatement. En particulier la mise à jour du statut de révocation du Certificat dépend de la rapidité du propriétaire de la Clé Privée à déclarer son vol ou sa compromission.

Par conséquent l'IGC Sunnystamp ne saurait voir sa responsabilité engagée :

- Dans le cas d'une utilisation frauduleuse de la Clé Privée associée au Certificat dans l'intervalle de temps compris entre le moment exact de compromission de la Clé Privée et la mise à jour par l'IGC Sunnystamp du statut de révocation du Certificat et de sa publication ;
- Dans le cas d'une signature électronique ou horodatage considéré comme indument valide du fait de l'absence de référence de temps fiable qui doit être utilisée pour vérifier le statut de révocation du Certificat.

8 Garanties

L'IGC Sunnystamp garantit aux UC :

- L'exactitude de l'ensemble des informations contenues dans le Certificat à la date d'enregistrement du dossier de demande de Certificat, conformément à la PC identifiée dans le Certificat, à l'exception des informations dont la vérification n'est pas prévue par cette PC ;

- La conformité du Certificat avec la PC identifiée dans le Certificat.

9 Limitations de garantie et limitations de responsabilité

L'IGC Sunnystamp ne peut être rendue responsable d'un quelconque dommage direct ou indirect (tel que mais non limité à la perte financière ou la perte de données) découlant de, ou connexe à, l'utilisation attribuée à un Certificat émis par l'IGC Sunnystamp.

À l'exception des garanties décrites dans la section précédente du présent Accord, l'IGC Sunnystamp exclut toute autre garantie, expresse ou implicite, notamment toute garantie :

- D'adéquation du Certificat à un usage spécifique ;
- De satisfaction d'une exigence particulière de l'UC.

Par le présent Accord, l'UC engage sa seule responsabilité pour tout dommage causé à un tiers du fait :

- D'un manquement de l'UC aux obligations au titre du présent Accord ;
- De l'utilisation d'un Certificat en dehors des conditions prévues par le présent accord ou par la PC relative à l'AC ayant émis le Certificat utilisé ;
- De l'absence de vérification par l'UC de la validité d'un Certificat et du statut de révocation dudit Certificat afin de déterminer si le Certificat était valide à la date de référence pour la vérification du Certificat.

10 Force majeure

En cas de force majeure, tel que défini par les tribunaux français, les obligations des parties seront automatiquement suspendues dans les hypothèses d'événements indépendants de leur volonté expresse empêchant l'exécution normale du présent Contrat.

11 Nullité

Dans le cas où une disposition du présent Accord s'avérerait être invalide, illégale ou non exécutoire par une loi, un règlement ou par la décision définitive d'une juridiction compétente, la validité, la légalité et le caractère exécutoire des autres clauses ne seront en aucun cas affectés ou réduits.

12 Droits applicables

Le présent Accord, aussi bien pour les règles de fond que de forme, est régi par la loi française et ce, quelques soient les lieux d'exécution des obligations substantielles ou accessoires.

13 Résolution des litiges

En cas de difficulté pour l'interprétation, l'application et/ou l'exécution de l'Accord, préalablement à toute procédure judiciaire ou administrative ayant pour objet le présent contrat, les parties conviennent de rechercher une résolution amiable du litige. A défaut d'accord amiable entre les parties, la compétence expresse est attribuée aux tribunaux de Paris.

14 Non-cession

Sauf accord exprès de l'IGC Sunnystamp, les droits qui sont octroyés à l'UC dans le cadre de cet Accord ne sont ni cessibles ni transférables.