Sunnystamp PKI

Sunnystamp Legal Persons CA

Procédure de demande de certificat

Version 1.1

Technopole de l'Aube en Champagne – CS 90601 – 10901 Troyes Cedex 9
Tél. : +33 (0)3 25 43 90 78 – Fax : +33 (0)9 81 40 30 08 – www.lex-persona.com
SARL au capital de 30 000 Euros – R.C.S. Troyes 480 622 257 – Code NAF 6202A – TVA FR01480622257

Sunnystamp PKI

Sunnystamp Legal Persons CA

Procédure de demande de certificat

Version 1.1

Etat des validations

	Vérificateur	Approbateur
Nom	François DEVORET	Julien PASQUIER
Fonction	LPCSP Board Chair	Sunnystamp PKI Manager

Historique des révisions

Version	Date	Auteur	Commentaires
1.0	19/06/2017	François DEVORET Julien PASQUIER	Création du document
1.1	03/11/2017	Julien PASQUIER	Ajout de l'authentification du RL par téléphone

Table des matières

1 Acronymes et définitions

AC	Autorité de Certification « Sunnystamp Legal Persons CA » appartenant au domaine Sunnystamp PKI.
AE	Autorité d'Enregistrement de l'AC.
Certificat	Certificat de cachetage ou d'horodatage délivré par l'AC.
Dashboard	Document Excel, rempli par les OAE, et contenant la traçabilité des demandes de création et de révocation de Certificats traités par l'AE.
LPCSP Board	Lex Persona Certification Service Provider Board. Organe responsable de la gouvernance des services de confiance de gestion des identités électroniques délivrées par Lex Persona.
OAE	Opérateur de l'AE ayant le rôle de confiance « Registration Officer » dans l'AC.
RCPS	Responsable de la Clé Privée du Sujet.
RL	Représentant Légal.
Sunnystamp PKI	Domaine, géré par le LPCSP Board, qui concerne les services de gestions des identités numériques de la plate-forme Sunnystamp.
UUID	Universal Unique Identifier

2 Introduction

Ce document décrit le processus de délivrance, d'un Certificat de cachetage ou d'horodatage, par l'Autorité de Certification « Sunnystamp Legal Persons CA » appelée AC dans le reste du document.

3 Processus de délivrance d'un Certificat

3.1 Origine de la demande de Certificat

Un Certificat est demandé par le RCPS désigné par un RL de l'entité légale pour laquelle est demandé le Certificat.

Le RCPS et le RL peuvent être une seule et même personne, mais ils seront considérés comme séparés dans le processus de demande de Certificat.

3.2 Formulaire de demande de Certificat

La demande d'un Certificat est formulée par le biais d'un formulaire PDF interactif, qui permet au RCPS de remplir les informations nécessaires à la délivrance du Certificat.

Ces informations sont les suivantes :

- La requête de certificat conforme au standard PKCS#10 PEM contenant la clé publique issue de la génération par le RCPS de la bi-clé sur un support cryptographique de niveau FIPS 140-2 Level 2 minimum ; la requête est signée avec la clé privée afin de prouver à l'AE la possession par le RCPS de la clé privée associée à la clé publique contenue dans cette requête de certificat.
- Le type du Certificat : cachetage ou horodatage.
- Les caractéristiques du Certificat, constitués des attributs CN, O, OI, C, OU, L, qui seront vérifiées par l'AE et intégrées par l'AC dans le champ « subject » du Certificat.
- Les informations de contact relatives au RCPS.
- Les informations de contact relatives au RL.
- Les pièces justificatives nécessaires à la demande de Certificat incorporées dans des champs du formulaire prévus à cet effet (pièce d'identité en cours de validité du RCPS, Kbis récent de l'entité légale).
- Les informations optionnelles de facturation du Certificat.

Le formulaire contient également les conditions générales d'utilisation du Certificat. Il est certifié par Lex Persona pour en garantir l'intégrité et l'authenticité.

Le formulaire constitue l'accord de souscription et doit être signé par le RCPS et le RL.

3.3 Processus de validation et de signature de la demande de Certificat

Les étapes ci-dessous décrivent le processus de validation et de signature de la demande de Certificat :

1. Le formulaire de demande de Certificat est téléchargé par le RCPS ou par le RL suite à l'invitation d'un commercial de Lex Persona ou de l'un de ses partenaires qui lui aura communiqué, le cas échéant, une référence commerciale relative à un devis, une proposition commerciale, un contrat d'acquisition de certificats, etc.
2. Le formulaire est téléchargeable en accès libre mais nécessite de connaître son adresse. Une notice décrivant les consignes d'utilisation du formulaire et le processus de demande de Certificat est également téléchargeable sur Internet.
3. Le formulaire est alors complété dans son intégralité par le RCSP et le RL. Dans l'hypothèse où aucune référence commerciale n'a été préalablement communiquée à la personne en charge de remplir le formulaire, cette dernière devra renseigner une référence commerciale relative à son entité. Le remplissage du formulaire consiste à renseigner les champs d'information requis ainsi que l'intégration de justificatifs (tels que pièce d'identité, Kbis,

Avis SIRENE, Procès-Verbal de Conseil d'Administration, etc.), sous la forme de pièces jointes.

4. Une fois le formulaire complété, et les justificatifs nécessaires intégrés au formulaire, un circuit de validation et de signature du formulaire, appelé Parapheur dans la suite du document, doit être créé par le RCPS sur la plate-forme [Sunnystamp], dont l'utilisation est gratuite et libre d'accès :
   - Le RCPS doit disposer au préalable d'un compte Sunnystamp, qui est gratuit. S'il n'en dispose pas, il peut s'inscrire à l'adresse [SunnystampSignUp] en s'assurant de renseigner ses informations personnelles en cohérence avec celles renseignées dans le formulaire.
   - Une fois connecté à son compte Sunnystamp, le RCPS clique sur le bouton « Faire signer » pour créer le Parapheur.
   - Le nom du Parapheur est laissé au choix du RCPS ; il pourra astucieusement comporter par exemple les termes « Demande certificat de cachetage {CN} pour {Entité} », les variables {CN} et {Entité) étant respectivement remplacées par le « Common Name » du Certificat demandé et le nom de l'entité légale pour laquelle le Certificat est demandé. Les notifications par e-mail doivent être celles par défaut.
   - Le RCPS doit ensuite fournir le formulaire comme document unique du Parapheur. La case à cocher « Visualiser » devra rester cochée. Aucune pièce annexe ne doit être fournie. Le type de signature par défaut doit être utilisé.
   - La 1ère étape du Parapheur est une étape de validation :
     - Adresse mail : ae-slp@sunnystamp.com ;
     - Opération : Valider ;
     - Aucune information particulière relative au destinataire ne doit être spécifiée.
   - La 2ème étape du Parapheur est une étape de signature du RCPS :
     - Adresse mail : celle du RCPS ;
     - Opération : Signer ;
     - Aucune information relative au destinataire autre que celles renseignées par défaut ne doit être fournie ;
     - Les informations renseignées par défaut ne doivent pas être modifiées.
   - La 3ème étape du Parapheur est une étape de signature du RL:
     - Adresse mail : celle du RL spécifié dans le formulaire ;
     - Opération : Signer ;
     - Si le RL désigné par le RCPS ne dispose pas d'un compte Sunnystamp alors le RCPS précisera dans les informations du destinataire, et de manière cohérente avec les informations du formulaire, les prénom, nom, numéro de téléphone portable et entité du RL et précisera que ces informations ne sont pas modifiables en laissant les cases cochées prévues à cet effet ;

- Aucune information relative au destinataire autre que celles renseignées par défaut ne doit être fournie ;

- La 4ème étape du Parapheur est une étape de validation (similaire à la 1ère) :
  - Adresse mail : ae-slp@sunnystamp.com ;
  - Opération : Valider ;
  - Aucune information particulière relative au destinataire ne doit être spécifiée.
- Ces 4 étapes doivent impérativement être effectuées en série et respecter l'ordre décrit ci-dessus. Aucune personne à informer ne doit être renseignée.
- Si le RCPS signe avec son certificat personnel de niveau RGS** ou ETSI EN 319 411-1 NCP+ ou supérieur, il n'a pas besoin de créer la 3ème étape dans laquelle il devait signer.
- Si la première et la dernière étape doivent impérativement être celle d'une validation par l'Autorité d'Enregistrement, il est en revanche possible pour le RCPS d'ajouter d'autres étapes de validation intermédiaires qui pourront lui permette de faire valider sa demande par d'autres personnes de son choix ou bien qui lui sont imposées par l'entité qui demande le Certificat. Cependant, aucune autre signature ne doit être prévue dans ce Parapheur.
- Le RCPS lance le Parapheur.

5. L'AE est automatiquement notifiée par mail. Un OAE effectue alors les tâches suivantes :
   - Il clique sur le lien fourni dans le mail.
   - Il se connecte à son compte Sunnystamp et démarre le processus de validation du formulaire, en commençant par la vérification de son contenu.
   - En cas d'erreur, d'absence d'information, de défaut de justificatif, ou de difficulté d'interprétation d'un justificatif, l'OAE rejette le Parapheur en indiquant dans les commentaires de rejet les explications nécessaires et met à jour le Dashboard en passant le statut de la demande à « Rejetée ». Dans ce cas, le RCPS qui a créé ce Parapheur est notifié par mail et peut ainsi consulter les causes de l'erreur puis effectuer les corrections qui s'imposent dans le formulaire, pour finalement soumettre un nouveau Parapheur avec le formulaire corrigé. A noter qu'à partir du formulaire rejeté, le RCPS peut en un clic recréer automatiquement un Parapheur identique et modifier tout ou partie des éléments du Parapheur (formulaire, destinataires, etc.).
   - Si tout est correct, l'OAE valide le Parapheur.
6. Le RCPS est automatiquement notifié par mail. Il effectue alors les tâches suivantes :
   - Il clique sur le lien fourni dans le mail.
   - Il se connecte à son compte Sunnystamp avec son identifiant et son mot de passe.
   - Il vérifie le formulaire ainsi que les pièces justificatives.
   - S'il constate une erreur, le RCPS doit rejeter son Parapheur et indiquer dans les commentaires de rejet les explications nécessaires. Le RCPS reçoit alors une

notification par mail du rejet du Parapheur, et peut effectuer les corrections qui s'imposent afin de resoumettre le formulaire corrigé.

- Après vérification, le RCPS peut alors consentir aux engagements indiqués dans le formulaire et signer le Parapheur avec un certificat délivré par la plate-forme Sunnystamp.

7. Le RL de l'entité est automatiquement notifié par mail. Il effectue alors les tâches suivantes :
   - Il clique sur le lien fourni dans le mail.
   - Si le RL de l'entité dispose d'un compte Sunnystamp, il se connecte à son compte Sunnystamp avec son identifiant et son mot de passe. Si le RL de l'entité ne dispose pas d'un compte Sunnystamp, le lien fourni dans le mail l'amène directement sur la page de signature.
   - Le RL de l'entité vérifie le formulaire ainsi que les pièces justificatives.
   - En cas d'erreur, le RL de l'entité doit rejeter le Parapheur en indiquant dans les commentaires de rejet les explications nécessaires. Le RCPS est alors automatiquement notifié par mail du rejet du Parapheur, et peut consulter les causes de l'erreur pour effectuer les corrections qui s'imposent et resoumettre le formulaire corrigé dans un nouveau Parapheur.
   - Après vérification, le RL de l'entité peut alors consentir aux engagements indiqués dans le formulaire et signer le Parapheur avec un certificat délivré par Sunnystamp.
8. L'AE est ensuite automatiquement notifiée par mail. Un OAE effectue alors les tâches suivantes :
   - Il clique sur le lien fourni dans le mail.
   - Il se connecte à son compte Sunnystamp et lors de la validation, il vérifie que la validation initiale a bien été effectuée par l'AE.
   - Il télécharge le formulaire et utilise la plate-forme Sunnystamp afin de vérifier les signatures électroniques du RCPS et du RL.
   - La vérification des signatures électroniques est effectuée en appliquant une politique de validation de signature qui limite volontairement l'éventail des familles de certificats habilitées à signer des demandes de Certificat :
     - Certificats délivrés par la plate-forme Sunnystamp ;
     - Certificats de niveau ETSI ou RGS.
   - Si des erreurs sont présentes lors de cette vérification, alors l'OAE informe le RCPS, en lui indiquant la nature des erreurs rencontrées ainsi que la marche à suivre pour corriger ces erreurs et met à jour le Dashboard en passant le statut de la demande à « Rejetée ».
   - Si aucune erreur n'est présente, alors l'OAE s'intéresse plus particulièrement au certificat utilisé par le RL pour signer le formulaire :

- Si le certificat est un certificat délivré par la plate-forme Sunnystamp, ou de niveau RGS* ou ETSI EN 319 411-1 LCP ou NCP, cela signifie que l'OAE doit authentifier le RL et s'assurer qu'il autorise bien cette demande de certificat. Pour cela l'OAE doit contacter directement le RL par téléphone sur le numéro officiel de l'entreprise et mettre à jour le [Dashboard], en spécifiant la date de cet appel et le numéro de téléphone composé.
- Si le certificat est un certificat de niveau RGS 2* ou supérieur, ou bien EN 319 411-1 NCP+ ou supérieur, alors cela signifie que l'authentification par téléphone du RL n'est pas nécessaire.

- L'OAE s'intéresse ensuite au certificat utilisé par le RCPS pour signer le formulaire :
  - Si le certificat est un certificat délivré par la plate-forme Sunnystamp, ou de niveau RGS* ou ETSI EN 319 411-1 LCP ou NCP, cela signifie que la vérification en face à face de l'identité du RCPS est nécessaire ;
  - Si le certificat est un certificat de niveau RGS 2* ou supérieur, ou bien EN319 411-1 NCP+ ou supérieur, alors cela signifie que la vérification en face à face de l'identité du RCPS n'est pas nécessaire.
- L'OAE enregistre l'e-mail et le formulaire dans un répertoire désigné à cet effet et procède à son archivage.
- L'OAE met à jour le Dashboard en passant le statut de la demande à « En cours ».
- Si l'une des étapes précédentes échoue, alors l'OAE met à jour le Dashboard en passant le statut de la demande à « Rejetée ».
- Si tout est correct l'OAE valide le Parapheur. Un mail de notification est automatiquement envoyé au RCPS pour l'avertir que le Parapheur est désormais terminé.

Le RCPS peut suivre l'avancement du Parapheur sur la plate-forme depuis la liste des Parapheurs « En cours », dans l'onglet « Parapheurs ». Si l'un des validateurs ou signataires tarde à valider ou signer, il est possible pour le RCPS d'effectuer une relance depuis ce même écran.

3.4 Génération du Certificat par l'AE

Une fois le Parapheur terminé, l'OAE effectue les opérations suivantes :

- Il se connecte au VPN de Lex Persona ;
- Il utilise son navigateur Web pour se connecter à l'interface d'administration EJBCA en utilisant son certificat d'authentification de « Registration Officer » : https://pki-mz-slp.sunnystamp.com:8443/ejbca/adminweb
- Il crée un nouveau « End Entity » en recopiant précisément les caractéristiques du Certificat à créer qui sont renseignées dans le formulaire et en générant de manière aléatoire :
  - Un UUID (16 octets) pour le « username » ;
  - Un code de 10 chiffres pour le « password » qui servira de code de révocation.

Le « Serial number » de ce End Entity, et qui sera contenu dans l'attribut « serialNumber » du champ « subject » du Certificat à créer, doit être le « username » (UUID).

- Il renseigne le « username » et le code de révocation dans le Dashboard. Si le RCPS ou le RL souhaite révoquer le Certificat, il devra préciser ce code de révocation dans le formulaire de demande de révocation pour authentifier sa demande auprès de l'AE. Si le RCPS ou le RL a oublié ou perdu le code de révocation, il pourra être contacté par l'AE qui l'authentifiera en vérifiant par téléphone les informations présentes dans les éléments en sa possession (formulaire de demande, pièces justificatives, etc.).
- Il se connecte ensuite à la page d'enrôlement d'EJBCA, renseigne le username et le password du « End Entity EJBCA » qu'il vient de créer, ainsi que la CSR contenue dans le formulaire.
- L'AC génère le Certificat et lui transmet.
- Il vérifie les informations relatives au Certificat et notamment celles contenues dans le champ « subject » par rapport à celles spécifiées dans le formulaire. S'il détecte une anomalie, il devra faire une demande de révocation.
- Il enregistre le Certificat généré dans le même répertoire que celui du formulaire de demande de Certificat.
- Il archive le Certificat sur les serveurs d'archivage de Dijon (P-SAV01.sunnystamp.com) et Reims (P-SAV04.sunnystamp.com).

3.5 Remise du Certificat par l'AE

Une fois le Certificat généré, un OAE se charge de mettre en œuvre le processus de remise du Certificat au RCPS qui se déroule de la façon suivante :

1. L'OAE prépare sur la plate-forme Sunnystamp le Parapheur de remise du Certificat au RCPS. Ce Parapheur de remise doit contenir comme nom « Remise du certificat de cachetage {CN} pour {Entité} », les variables {CN} et {Entité) étant respectivement remplacées par le « Common Name » du Certificat et le nom de l'entité légale pour laquelle le Certificat a été demandé. Il doit contenir les étapes suivantes :
    - Dans le cas où la vérification d'identité en face à face est requise, la validation par un OAE de l'étape d'authentification en face à face du RCPS:
        - Adresse mail : ae-slp@sunnystamp.com
        - Opération : Valider ;
        - Le commentaire qui sera affiché au destinataire devrait indiquer la mention « Authentification en face à face du RCPS » ;
        - Aucune autre information particulière relative au destinataire ne doit être spécifiée.

      Dans ce cas, l'OAE met à jour le [Dashboard], en ajoutant la date prévue pour le face à face avec le RCPS ainsi que ses informations personnelles : nom, prénom, téléphone, adresse e-mail.
    - La validation par le RCPS de la réception du Certificat :

- Adresse mail : adresse mail du RCPS ;
- Opération : Valider ;
- Le commentaire qui sera affiché au destinataire devrait indiquer la mention « Merci de bien vouloir valider la remise de votre certificat « {CN} » pour {Entité} », les variables {CN} et {Entité) étant respectivement remplacées par le « Common Name » du Certificat et le nom de l'entité légale pour laquelle le Certificat a été demandé ;
- Aucune autre information particulière relative au destinataire ne doit être spécifiée.

- La validation par un OAE de la complétion du processus de remise :
  - Adresse mail : ae-slp@sunnystamp.com ;
  - Opération : Valider ;
  - Le commentaire qui sera affiché au destinataire devrait indiquer la mention « Processus de remise du certificat au RCPS terminé » ;
  - Aucune autre information particulière relative au destinataire ne doit être spécifiée.

2. L'OAE lance ce Parapheur de remise. Un mail de notification est alors automatiquement envoyé à l'AE si une vérification en face à face est nécessaire ou au RCPS dans le cas contraire.
3. Si la vérification de l'identité du RCPS lors d'un face à face avec l'AE est requise, alors l'AE est automatiquement notifiée par mail et un OAE doit réaliser les étapes suivantes :
   - Prendre rendez-vous avec le RCPS pour la vérification de son identité lors d'un face à face physique.
   - Communiquer au RCPS les prérequis au rendez-vous (pièce d'identité identique à celle contenue dans le formulaire, etc.).
   - Réaliser les actions suivantes lors du face-à-face physique avec le RCPS :
     - Vérifier la pièce d'identité du RCPS (état général, points de vérification habituels, vérification de la correspondance entre la photo figurant sur la pièce d'identité avec le RCPS) ;
     - Faire signer au RCPS le PV de vérification de son identité ;
     - Cosigner le PV de vérification.
   - Met à jour le [Dashboard] en ajoutant la date de réalisation du face à face
   - Archiver le PV signé.
   - Se connecter à son compte Sunnystamp et valider la 1ère étape du Parapheur de remise.
4. Le RCPS est automatiquement notifié par mail. Il effectue alors les tâches suivantes :
   - Il clique sur le lien fourni dans le mail et se connecte à son compte Sunnystamp avec son identifiant et son mot de passe.

- Il valide la remise du Certificat. S'il refuse, l'OAE est notifié et pourra prendre contact avec le RCPS pour lui demander les raisons de son refus. Le cas échéant l'OAE annule le Parapheur de délivrance et révoque le Certificat.

5. L'OAE est automatiquement notifié par mail. Il effectue alors les tâches suivantes :
   - Il clique sur le lien fourni dans le mail et se connecte à son compte Sunnystamp avec son identifiant et son mot de passe.
   - Il valide le Parapheur de remise.
   - Il envoi par e-mail au RCPS et au RL le code de révocation généré précédemment.
   - Il met à jour la demande dans le Dashboard en passant le statut de la demande à « Terminée ».