



Sunnystamp PKI

Sunnystamp Legal Persons CA

Procédure de révocation de certificat

Version 1.0

Tous droits réservés

Sunnystamp PKI**Sunnystamp Legal Persons CA****Procédure de révocation de certificat****Version 1.0****Etat de validation**

	Vérificateur	Approbateur
Nom	Imane PASQUIER	François DEVORET
Fonction	Responsable SMSI	LPCSP Board Chair

Historique des révisions

Version	Date	Auteur	Commentaires
1.0	10/07/2017	Julien PASQUIER	Version initiale

Table des matières

1	Acronymes et définitions	3
2	Introduction.....	4
3	Origine d'une demande de révocation	4
4	Transmission d'une demande de révocation à l'AE	4
5	Traitement d'une demande de révocation par l'AE.....	4

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 délivré par l'AC et faisant l'objet d'une demande de révocation.
Dashboard	Document Excel, rempli par les OAE, et contenant la traçabilité des demandes de création et de révocation de Certificats traitées par l'AE.
LPCSP Board	Lex Persona Certification Service Provider Board. Organe responsable de la gouvernance des services de confiance de gestion des identités numériques délivrées par Lex Persona.
OR	Opérateur de Révocation. Il s'agit d'une personne habilitée, rattachée à l'AE, ayant le rôle de confiance de « Revocation Officer » dans l'AC.
PC/DPC	Politique de Certification et Déclaration des Pratiques de Certification de 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 gestion des identités numériques de la plate-forme Sunnystamp.

2 Introduction

Ce document décrit la procédure de révocation d'un Certificat émis par l'Autorité de Certification « Sunnystamp Legal Persons CA », appelée AC dans la suite du document.

3 Origine d'une demande de révocation

Comme l'indique la PC/DPC de l'AC, les personnes qui peuvent demander la révocation d'un Certificat sont les suivantes :

- Le RCPS ;
- Le RL ;
- Un membre de l'AC.

Dès que l'une des causes de révocation décrite dans la PC/DPC est détectée par l'une de ces personnes, elle doit, sans délai, demander à l'AE de révoquer le Certificat.

4 Transmission d'une demande de révocation à l'AE

Si le demandeur de la révocation est le RCPS ou le RL, il doit remplir le formulaire de demande de révocation et l'envoyer par e-mail à l'AE en renseignant en particulier le code de révocation du Certificat. Dans le cas où le RCPS ou le RL ne dispose plus du code de révocation (suite à sa perte ou son oubli), un OR l'appellera sur le numéro de téléphone spécifié dans le formulaire afin d'essayer de l'authentifier avant de procéder à la révocation du Certificat.

Si le demandeur de la révocation est un membre de l'AC, il doit remplir le formulaire de demande de révocation, et l'envoyer à l'AE dans un e-mail signé avec son certificat Lex Persona. Contrairement au RCPS et au RL, il n'a pas besoin de renseigner le code de révocation.

Le formulaire de demande de révocation est téléchargeable en accès libre depuis l'adresse <https://pki2.sunnystamp.com/repository>.

5 Traitement d'une demande de révocation par l'AE

Comme le stipule la PC/DPC, les demandes de révocation reçues par e-mail doivent être traitées par l'AE en moins de 24h.

Il y a toujours au moins un OR qui vérifie quotidiennement, entre 9h et 18h (heure de Paris), les e-mails reçus sur la boîte ae-slp@sunnystamp.com, week-end et jours fériés inclus.

La procédure de révocation par e-mail se déroule de la façon suivante :

1. Le demandeur envoie un e-mail à l'AE, à l'adresse ae-slp@sunnystamp.com, contenant en pièce jointe le formulaire de demande de révocation dûment rempli.
2. Si le demandeur est un membre de l'AC, il doit obligatoirement signer l'e-mail avec son certificat délivré par l'AC Interne Lex Persona.

3. L'OR réceptionne l'e-mail et ouvre le formulaire PDF en pièce jointe.
4. L'OR s'assure que les champs suivants du formulaire sont correctement remplis :
 - Le nom, prénom, fonction, adresse e-mail et numéro de téléphone du demandeur ;
 - Le numéro de série du Certificat à révoquer.
5. L'OR ouvre le Dashboard et s'assure que cette demande de révocation n'est pas déjà en cours de traitement, ou n'a pas déjà été traitée, par un autre OR. Si c'est le cas il arrête le traitement de cette demande.
6. L'OR enregistre cette demande de révocation dans le Dashboard en spécifiant le statut « En cours ».
7. L'OR se connecte au VPN Lex Persona avec son certificat d'authentification VPN.
8. L'OR se connecte à EJBCA en utilisant son certificat d'authentification de « Revocation Officer » : <https://pki-mz-slp.sunnystamp.com:8443/ejbca/adminweb/>
9. L'OR cherche le Certificat à révoquer à partir de son numéro de série.
10. Si le Certificat n'existe pas, a expiré ou a déjà été révoqué alors l'OR met à jour la demande dans le Dashboard avec le statut « Rejetée ». Il envoie un e-mail de « Rejet » au demandeur et le traitement de cette demande s'arrête ici.
11. L'OR enregistre l'e-mail et le formulaire de demande de révocation dans le répertoire de l'AE.
12. L'OR authentifie le demandeur de la façon suivante :
 - a) Si le demandeur est un membre de l'AC, l'OR vérifie la validité de la signature de l'e-mail en s'assurant notamment que le certificat du signataire a été délivré par l'AC Interne Lex Persona et que l'e-mail de l'expéditeur correspond bien à celui renseigné dans le formulaire.
 - b) Si le demandeur est le RCPS ou le RL :
 - a. Si le code de révocation est renseigné, l'OR vérifie sa validité en le comparant avec celui spécifié dans le Dashboard pour ce Certificat.
 - b. Sinon, l'OR contacte le demandeur au numéro spécifié dans le formulaire, afin de l'authentifier par le biais d'un jeu de 3 questions pour lesquelles une réponse précise et correcte devra être donnée :
 - Le nom de famille et les prénoms du RCPS figurant sur sa pièce d'identité utilisée lors de l'enregistrement ;
 - La date et le lieu de naissance du RCPS figurant sur sa pièce d'identité utilisée lors de l'enregistrement ;
 - L'adresse du domicile du RCPS figurant sur sa pièce d'identité utilisée lors de l'enregistrement.

Si le demandeur est le RL, il pourra consulter la pièce d'identité du RCPS utilisée lors de l'enregistrement, en la récupérant dans le formulaire de demande de certificat contenu dans les « Parapheurs terminés » de son compte Sunnystamp.

Si le demandeur ne décroche pas, l'OR lui envoie un e-mail pour lui indiquer que sa demande de révocation a bien été prise en compte et que l'AE, vient d'essayer de le contacter par téléphone pour l'authentifier afin de procéder à la révocation du Certificat, et va réessayer à nouveau de le contacter dans les 10 minutes à venir.

13. L'OR révoque le Certificat depuis l'interface d'administration d'EJBCA en indiquant la raison de révocation « unspecified ».
14. L'OR envoie un e-mail de notification aux RCPS et RL pour leur indiquer que le Certificat vient d'être révoqué avec succès.
15. Si le demandeur est un membre de l'AC, l'OR lui envoie un e-mail de notification pour lui indiquer que le Certificat vient d'être révoqué avec succès.
16. L'OR met à jour le Dashboard en indiquant le statut « Terminée » pour cette demande de révocation.