

Politique de création de cachet

Prestataire de service de Recommandé électronique
Letreco

Equisign

Version	Date	Description	Auteurs	Société
1.0	21 Mai 2018	Politique de scellement des preuves	G. LOTH DEMAY	Equisign
1.1	20/08/2018	Renommé en « Politique de création de cachet » Ajout de consignes de vérification des cachets	G. LOTH DEMAY	Equisign
1.2	11/03/2020	Le certificat de cachet est renouvelé au moins 3 mois avant son expiration.	G. LOTH DEMAY	Equisign

État du document - Classification	Référence
Validé - Public	

Ce document est la propriété exclusive de Equisign.
Son usage est réservé à l'ensemble des personnes habilitées selon leur niveau de confidentialité.
Sa reproduction est régie par le Code de la propriété intellectuelle qui ne l'autorise qu'à l'usage privé du copiste.

Sommaire

1	INTRODUCTION	4
1.1	PRESENTATION GENERALE.....	4
1.2	DOMAINE D'APPLICATION.....	4
1.3	IDENTIFICATION DU DOCUMENT	4
1.4	GESTION DE LA POLITIQUE	4
1.4.1	Entité gérant la politique	4
1.4.2	Point de contact.....	4
1.4.3	Procédure d'approbation de la politique	5
1.4.4	Amendements à la politique	5
1.5	DOCUMENTS ASSOCIES.....	5
2	DECLARATION DES PRATIQUES DE L'APPLICATION DE CREATION DE CACHET.....	6
2.1	EXIGENCES SUR LE FOURNISSEUR.....	6
2.2	EXIGENCES SUR L'APPLICATION DE CREATION/VERIFICATION DE CACHET	6
3	PARAMETRES METIER (BSP).....	6
3.1	PARAMETRES RELATIFS CAS D'USAGE.....	7
3.1.1	BSP (a) : Séquencement des cachets.....	7
3.1.2	BSP (b) : Données signées	7
3.1.3	BSP (c) : Lien entre les données signées et les cachets.....	7
3.1.4	BSP (d) : Population cible	7
3.1.5	BSP (e) : Responsabilités quant à la validation et l'extension des cachets.....	7
3.2	PARAMETRES D'ORIGINE JURIDIQUE/LEGALE/REGLEMENTAIRE	7
3.2.1	BSP (f) : Nature juridique des cachets	7
3.2.2	BSP (g) : Engagement des créateurs de cachet.....	7
3.2.3	BSP (h) : Garanties sur la date des cachets	7
3.2.4	BSP (i) : Formalités de création du cachet.....	8
3.2.5	BSP (j) : Pérennité des cachets	8
3.2.6	BSP (k) : Archivage	8
3.3	PARAMETRES RELATIFS AUX MOYENS ET INTERVENANTS IMPLIQUES DANS LE CYCLE DE VIE DES CACHETS	8
3.3.1	BSP (l) : Identité des créateurs de cachet	8
3.3.2	BSP (m) : Niveau de garantie pour l'authentification des créateurs de cachet.....	8
3.3.3	BSP (n) : Dispositif de création des cachets.....	8
3.4	AUTRES PARAMETRES	8
3.4.1	BSP (o) : Informations supplémentaires associées aux cachets	8

EQUISIGN	Politique de création de cachet Service Letreco
----------	--

3.4.2	<i>BSP (p) : Dimensionnement cryptographique</i>	8
3.4.3	<i>BSP (q) : Environnement technique.....</i>	9
4	EXIGENCES SUR LES MOYENS ET STANDARDS	9
5	AUTRES PROBLEMATIQUES METIERS ET LEGALES	9
6	AUDITS ET CONFORMITE	9

EQUISIGN	Politique de création de cachet Service Letreco
----------	--

1 INTRODUCTION

1.1 PRESENTATION GENERALE

Le présent document constitue la politique de création des cachets électroniques utilisés pour le scellement des données transmises via le service de recommandé électronique Letreco de la société Equisign, conformément à l'article 44, alinéa 1(d) du Règlement 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 et abrogeant la directive n°1999/93/CE, dit « Règlement eIDAS ».

Le plan et le contenu de cette politique visent la conformité aux spécifications techniques décrites dans [TS_119172].

1.2 DOMAINE D'APPLICATION

La présente politique s'applique aux cachets électroniques avancés apposés sur les preuves (d'envoi, de réception, etc.) produites par le service de recommandé électronique Letreco de la société Equisign.

Une description de ces preuves se trouve, en particulier, dans le document Politique et pratiques du service de recommandé électronique [POLITIQUE] (OID : 1.3.6.1.4.1.51763.1.1.x, où « x » est le numéro de version en vigueur de la politique) disponible sur le site <https://www.letreco.fr>.

1.3 IDENTIFICATION DU DOCUMENT

La présente politique est identifiée par l'OID suivant : 1.3.6.1.4.1. 51763.1.2.1.

1.4 GESTION DE LA POLITIQUE

1.4.1 Entité gérant la politique

La politique est gérée par les membres du comité de pilotage du service Letreco de Equisign.

1.4.2 Point de contact

Le point de contact pour toute demande relative à cette politique est :

Equisign Service Letreco Les Collines de l'Arche 76, route de la Demi-Lune 92057 Paris La Défense Cedex
--

EQUISIGN	Politique de création de cachet Service Letreco
----------	--

1.4.3 Procédure d'approbation de la politique

La politique est approuvée après examen et relecture par les membres du comité de pilotage, ou les personnes désignées par celui-ci. Cette relecture a pour objectif d'assurer :

- **La conformité de la politique avec les exigences réglementaires et normatives portant sur la fourniture d'un service de recommandé électronique qualifié.**
- **La concordance entre les engagements exprimés dans la politique et les moyens techniques et organisationnels mis en œuvre par Equisign et ses partenaires.**

1.4.4 Amendements à la politique

Equisign contrôle que tout projet de modification de la présente politique reste conforme aux exigences réglementaires et normatives applicables.

1.4.4.1 Procédures d'amendement

La politique est modifiée par des experts techniques de Equisign, sur demande du Comité de pilotage, puis soumise à l'approbation de celui-ci tel que défini au §1.4.3.

1.4.4.2 Mécanisme et période d'information sur les amendements

Conformément à [POLITIQUE], Equisign adressera annuellement à l'ANSSI et à l'organisme de certification une synthèse de l'ensemble des modifications apportées à la fourniture de ses services de confiance qualifiés, dont la présente politique fait partie.

1.4.4.3 Circonstances selon lesquelles l'OID doit être changé

Toute évolution de la présente politique ayant un impact majeur sur le service de recommandé électronique [POLITIQUE] doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels cachets correspondent à quelles exigences.

1.5 DOCUMENTS ASSOCIÉS

[POLITIQUE]	Politiques et Pratiques du service de recommandé électronique LETRECO OID : 1.3.6.1.4.1.51763.1.1.x (x = version en vigueur)
[TS_119172]	ESI - Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents, Version 1.1.1 de juillet 2015
[ANSSI_LRE]	Services d'envoi recommandé électronique qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, Version 1.0 du 3 janvier 2017 https://www.ssi.gouv.fr/uploads/2016/06/eidas_envoi-recommande-electronique-qualifie_v1.0_anssi.pdf
[ANSSI_PSCO]	Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, Version 1.2 du 5 juillet 2017 https://www.ssi.gouv.fr/uploads/2017/01/eidas_psc-qualifies_v1.2_anssi.pdf
[TS 102 640-3]	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy

EQUISIGN	<p align="center">Politique de création de cachet</p> <p align="center">Service Letreco</p>
----------	---

Requirements for REM Management Domains, version v2.1.2 de septembre 2011

2 DÉCLARATION DES PRATIQUES DE L'APPLICATION DE CREATION DE CACHET

2.1 EXIGENCES SUR LE FOURNISSEUR

La présente politique de formule aucune exigence sur le fournisseur de l'application de création de cachet.

2.2 EXIGENCES SUR L'APPLICATION DE CRÉATION/VÉRIFICATION DE CACHET

L'application de création de cachet électronique utilisé pour générer les cachets doit être en capacité de respecter les exigences de format définies ci-après et doit être exploitée dans les conditions conformes à la politique du service et donc en particulier aux exigences des documents [POLITIQUE], [ANSSI_LRE] et [ANSSI_PSCO].

Concernant la vérification du cachet, les utilisateurs du service de recommandé Letreco doivent vérifier la validité des cachets en effectuant les contrôles suivants :

- **Contrôle de présence d'un cachet et d'un jeton d'horodatage ;**
- **Contrôle de l'intégrité du document de preuve par validation cryptographique du cachet et du jeton d'horodatage ;**
- **Vérification du certificat de cachet utilisé :**
 - **Le certificat doit être l'un de ceux publiés par Equisign ou dans la liste de confiance eIDAS pour identifier le service Letreco qualifié ;**
 - **Le certificat doit être valide et non révoqué ni suspendu à la date de création du cachet;**
- **Vérification du certificat d'horodatage utilisé :**
 - **Le certificat doit être l'un de ceux publiés dans la liste de confiance eIDAS pour le service d'horodatage identifié dans la politique du service [POLITIQUE] (voir §3.1.3);**
 - **Le certificat doit être valide et non révoqué ni suspendu à la date de création de l'horodatage ;**
 - **Contrôle de la politique d'horodatage utilisée : L'OID de la politique d'horodatage indiquée dans le jeton doit correspondre au service d'horodatage identifié dans la politique du service [POLITIQUE] (voir §3.1.3).**

Les utilisateurs du service de recommandé sont libres d'utiliser les moyens qui leur conviennent.

3 PARAMÈTRES MÉTIER (BSP)

Remarque : le terme « BSP » correspond au terme « Business Scoping Parameters » de [TS_119172].

EQUISIGN	Politique de création de cachet Service Letreco
----------	--

3.1 PARAMÈTRES RELATIFS CAS D'USAGE

3.1.1 BSP (a) : Séquencement des cachets

Les cachets sont produits unitairement, à raison d'un unique cachet par preuve produite durant le cycle de vie d'une lettre recommandée électronique (LRE) envoyée.

3.1.2 BSP (b) : Données signées

Les données signées avec le cachet sont les preuves produites par le service. Il s'agit de documents au format PDF attestant des différentes étapes du cycle de vie d'une lettre recommandée électronique. Le contenu des preuves est détaillé dans [POLITIQUE].

3.1.3 BSP (c) : Lien entre les données signées et les cachets

Les cachets sont des signatures électroniques enveloppées des données, conformes au PAdES Baseline Profile (ETSI TS 103172, v.2.2.2), niveau « LT-Level ».

L'horodatage est effectué par un service d'horodatage électronique qualifié au sens du règlement eIDAS, indiqué dans la politique du service [POLITIQUE] et identifié par l'OID 1.3.6.1.4.1.22234.2.6.5.8 .

3.1.4 BSP (d) : Population cible

Les preuves sont destinées aux utilisateurs du service de recommandé électronique (expéditeurs et destinataires) Letreco

3.1.5 BSP (e) : Responsabilités quant à la validation et l'extension des cachets

Les cachets et le jeton d'horodatage inclus sont validés par le service Letreco dès leur réception.

Les cachets ne font pas l'objet d'extension.

3.2 PARAMÈTRES D'ORIGINE JURIDIQUE/LÉGALE/RÉGLEMENTAIRE

3.2.1 BSP (f) : Nature juridique des cachets

Les cachets sont des cachets électroniques avancés au sens de l'article 36 du Règlement eIDAS.

3.2.2 BSP (g) : Engagement des créateurs de cachet

Les cachets assurent l'authenticité des preuves produites par le service de recommandé électronique Letreco.

3.2.3 BSP (h) : Garanties sur la date des cachets

La date d'application des cachets est garantie par un jeton, d'horodatage électronique qualifié ajouté au document PDF conformément au format PAdES.

EQUISIGN	Politique de création de cachet Service Letreco
----------	--

3.2.4 BSP (i) : Formalités de création du cachet

Sans objet.

3.2.5 BSP (j) : Pérennité des cachets

La durée de validité du certificat de cachet est de 2 ou 3 ans. Le certificat est renouvelé par Equisign au moins trois mois avant sa fin de validité.

Afin de garantir la possibilité de pouvoir vérifier la signature pendant les 7 ans de conservation (en conformité avec l'exigence du §6.5 de la norme ETSI [TS 102 640-3]), la signature embarque les chaînes de certification et les informations de révocation selon le format PAdES Baseline Profile niveau « LT-Level ».

3.2.6 BSP (k) : Archivage

Les modalités d'archivage des preuves par Equisign sont décrites dans [POLITIQUE]. Les preuves sont archivées directement par Equisign et non par le service de génération des cachets.

Il appartient aux utilisateurs de conserver les preuves qui leur sont fournies.

3.3 PARAMÈTRES RELATIFS AUX MOYENS ET INTERVENANTS IMPLIQUÉS DANS LE CYCLE DE VIE DES CACHETS

3.3.1 BSP (l) : Identité des créateurs de cachet

L'unique créateur de cachet est la société Equisign, son identité est attestée par le certificat utilisé.

3.3.2 BSP (m) : Niveau de garantie pour l'authentification des créateurs de cachet

Le niveau de garantie est déterminé par la politique de certification utilisée pour générer le certificat de cachet ; se référer à [POLITIQUE].

3.3.3 BSP (n) : Dispositif de création des cachets

Les cachets sont créés dans un matériel cryptographique qualifié par l'ANSSI, conformément aux exigences du document [ANSSI_LRE].

3.4 AUTRES PARAMÈTRES

3.4.1 BSP (o) : Informations supplémentaires associées aux cachets

Sans objet.

3.4.2 BSP (p) : Dimensionnement cryptographique

Voir [ANSSI_LRE] et [ANSSI_PSCO].

EQUISIGN	Politique de création de cachet Service Letreco
----------	--

3.4.3 BSP (q) : Environnement technique

L'environnement technique de création de cachet électronique doit être conforme à la politique du service et donc en particulier aux exigences des documents [POLITIQUE], [ANSSI_LRE] et [ANSSI_PSCO].

4 EXIGENCES SUR LES MOYENS ET STANDARDS

Les moyens techniques et organisationnels mis en œuvre pour la création du cachet doivent être conformes à la politique du service et donc en particulier aux exigences des documents [POLITIQUE], [ANSSI_LRE] et [ANSSI_PSCO].

5 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

Voir le document [POLITIQUE].

6 AUDITS ET CONFORMITÉ

Voir le document [POLITIQUE].