MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES
Liberté
Égalité
Fraternité

Webinaire:

Demande de CEE : encadrement des pièces électroniques

DGEC – NOVEMBRE 2024

SEALWeb

Introduction

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES
Liberté
Égalité
Fraternité

Objectifs de l'encadrement des pièces électroniques :

- **mieux encadrer** la signature électronique, pour limiter les fraudes sur les dates des signatures et sur l'intégrité des informations portées par les pièces
- **harmoniser** les règles liées à la signature électronique pour toutes les pièces
- **confirmer** que la signature électronique est possible pour toutes les pièces
- **assouplir** la doctrine de la DGEC en cas d'identification d'un problème lié à une signature électronique

Rappel du contexte et des enjeux

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES
Liberté
Égalité
Fraternité

Contexte :
Des dossiers de demande de CEE font l'objet de fraude
Simplification des procédures et massification

Enjeux :
Réduire les risques de fraude ciblant les dossiers de demande de CEE

Les scénarios de fraude identifiés sont les suivants :

Scénarios affectant les pièces du dossier de demande de CEE
(*devis, RAI, attestation sur l'honneur, preuve de réalisation, autre pièce complémentaire*)

- Pièces du dossier antidatées et/ou altérées
- Usurpation d'identité du signataire personne physique ou morale sur les pièces du dossier signées
- Absence de consentement des signataires pour les pièces du dossier signées
- Signature des pièces du dossier par une personne physique ou morale fictive

Scénarios affectant les rapports de contrôle des travaux

- Rapport de contrôle antidaté et/ou altéré
- Usurpation d'identité de l'émetteur du rapport

Objectif : identifier les solutions permettant de couvrir les scénarios de risque cités et de se protéger contre les risques de contestation du contenu, de non-répudiation

Les solutions pour encadrer les pièces électroniques

Introduction

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES
Liberté
Égalité
Fraternité

Echanges dématérialisés / nouvelles habitudes :

- Tout se fait à distance,
- Les documents s'échangent au format électronique,
- Moins de face-à-face et les personnes s'identifient à distance,
- Etc.

Apparition de nouvelles menaces simplifiant la fraude (*ex : envoi d'email non authentifiée, envoi de document signé scanné, etc.*)

Nécessite la mise en place de dispositifs de protection adaptés à ces nouvelles menaces : la signature électronique et les services de confiance réglementés permettant de sécuriser les échanges électroniques

Quels sont ces dispositifs et quel est leur cadre d'application ?

Le règlement européen eIDAS

- Directive européenne sur la signature électronique de 1999 réformée par la Commission Européenne sous forme de règlement.
- Règlement imposé à tous les États membres de l'UE
- Objectifs :

Accélérer la transition vers la dématérialisation en évitant les problèmes d'interopérabilité,

Accroître la sécurité juridique en donnant des règles simples et claires de reconnaissance mutuelle entre les services de confiance des différents Etats membres,

SEALWeb

Les trois volets du Règlement :

La reconnaissance juridique de l'écrit numérique

L'identité électronique - eWallet

Les services de confiance

La signature électronique

Différents niveaux de signature électronique :

Signature simple	Sans protection particulière
Signature avancée avec un certificat non qualifié	Titre d'identité → Certificat électronique
Signature avancée avec un certificat qualifié	Face-à-face → Certificat électronique
Signature qualifiée	Face-à-face → Certificat électronique +

Signature avancée avec un certificat non qualifié	Signature avancée avec un certificat qualifié	Signature qualifiée
Recevable en justice Garantie sur l'intégrité des données signées	Recevable en justice Garantie sur l'identité du signataire et sur l'intégrité des données signées	Equivalente à une signature manuscrite Présomption de fiabilité

Les services de confiance

- Certificat de signature/cachet électronique
- Horodatage
- Envoi de recommandé électronique
- Vérification de signature
- Préservation de signature
- Certificat authentification de site Web
- Archivage électronique (NEW)
- Registre / *Blockchain* (NEW)
- Gestion d'un service de signature à distance (NEW)
- Attestation d'attributs (NEW)

Service non-qualifié	Service qualifié
Recevable en justice	Présomption de fiabilité Interopérable

Les solutions pour encadrer les pièces électroniques :

Seuls les quelques services qualifiés sélectionnés ont été retenus comme pertinents et utiles pour le contexte des demandes de CEE.

Les autres services de confiance n'ont pas été retenus à ce stade pour au moins l'une des raisons suivantes :

- *Considérés comme non-pertinents dans le contexte du projet,*
- *Pas encore déployés sur le marché donc non-utilisables (pas d'offres à date).*

SEALWeb

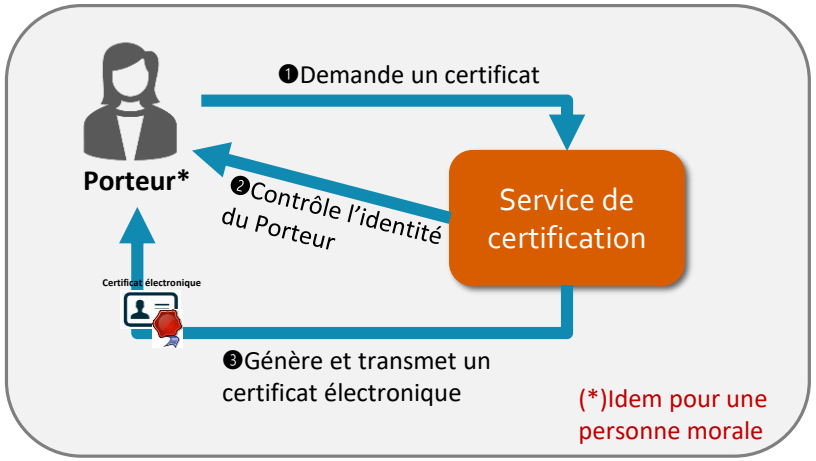
Services de confiance retenus :

Présentation des concepts

Service de fourniture de certificat électronique qualifié

Fournit des certificats électroniques qualifiés :

- *De signature pour les personnes physiques*
- *De cachet pour les personnes morales*

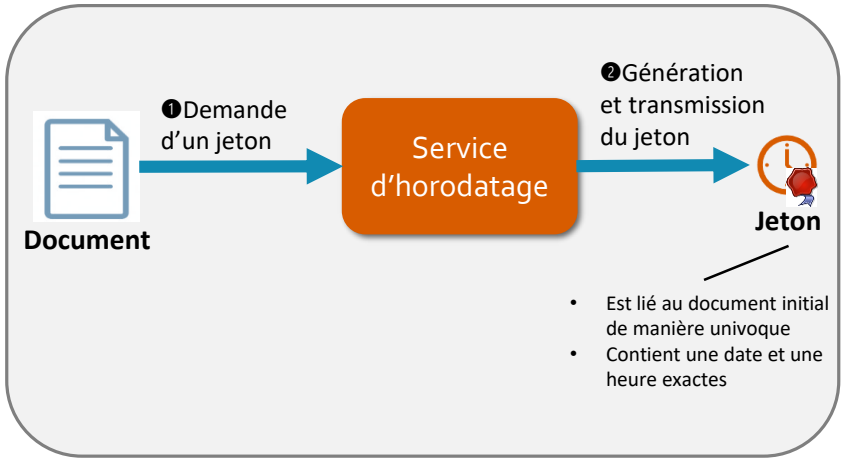


Sécurité/garantie apportée

- Garantie forte sur l'identité du porteur de certificat (*personne physique ou personne morale*)

Service d'horodatage électronique qualifié

Fournit une preuve (*contremarque de temps ou jeton*) qu'un document existait à une date donnée



Sécurité/garantie apportée

- Présomption d'intégrité du document
- Présomption d'exactitude de la date
- Présomption d'existence du document à un instant précis

Les solutions pour encadrer les pièces électroniques :

- Signature simple
- Signature avancée avec un certificat non qualifié
- **Signature avancée avec un certificat qualifié**
- Signature qualifiée

Principe :

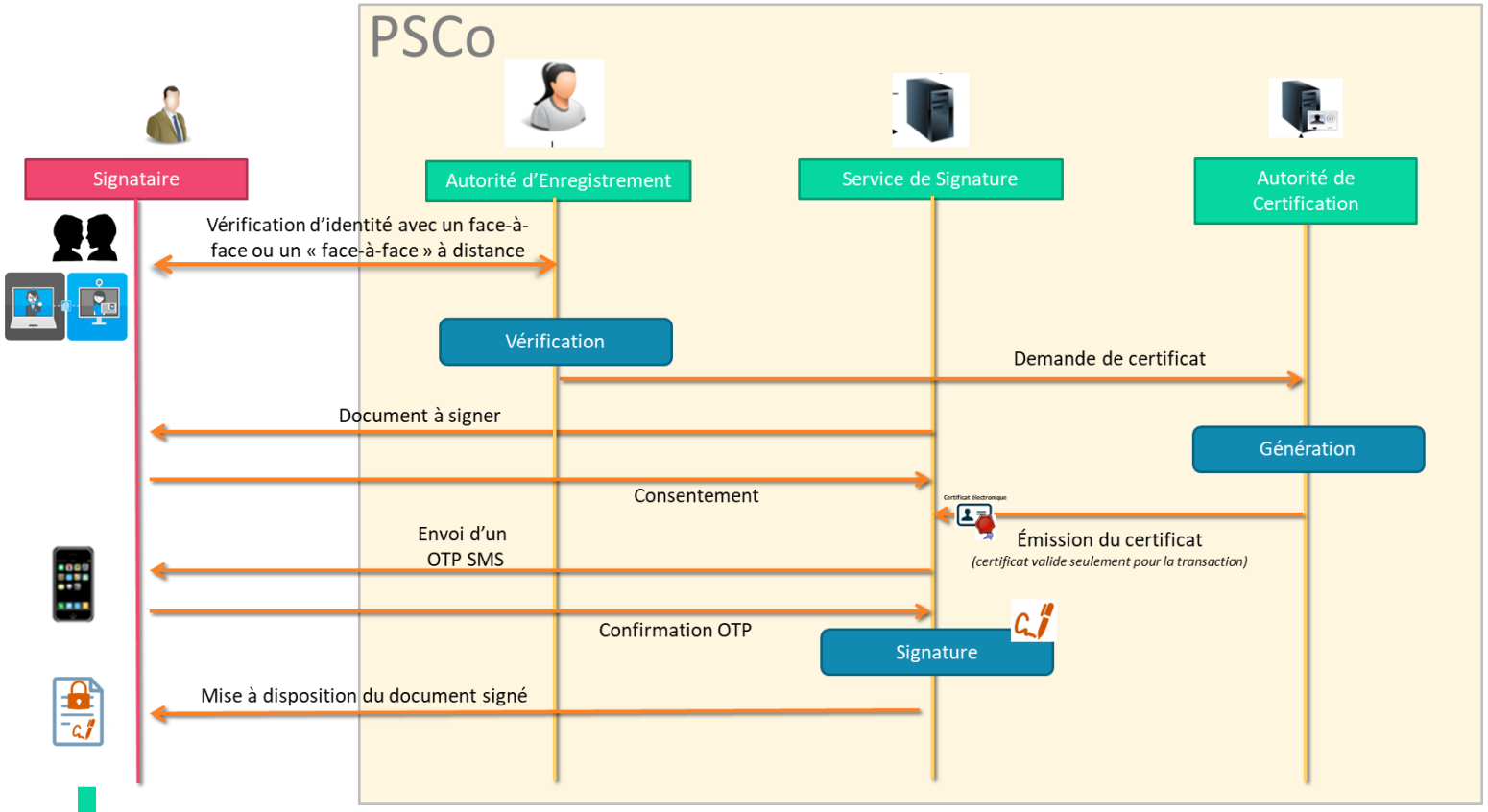
- Identifier le signataire par un face-à-face ou un dispositif équivalent à distance (*ex : Prestataire de vérification d'identité à distance - PVID*)
- Authentifier le signataire (*par des systèmes à double facteur*)
- Générer un certificat qualifié dont la clé privée est stockée dans un support cryptographique (*carte-à-puce, HSM, etc.*)

HSM

Niveau de signature électronique retenu :

Présentation du concept

Signature avancée avec un certificat qualifié



- Garantie sur l'intégrité du contenu du document
- Garantie forte sur l'identité du signataire
- Garantie la non-répudiation du signataire

SEALWeb

Les solutions pour encadrer les pièces électroniques :

- Cachet simple
- Cachet avancé avec un certificat non qualifié
- **Cachet avancé avec un certificat qualifié**
- Cachet qualifié

Principe :

- Obtenir, au préalable, un certificat de cachet au nom de la personne morale. Nécessite la vérification d'identité d'un représentant de la personne morale par un face-à-face ou un dispositif équivalent à distance (*ex : Prestataire de vérification d'identité à distance - PVID*)
- Authentifier le Responsable du certificat
- Générer un certificat qualifié dont la clé privée est stockée dans un support cryptographique (*carte-à-puce, HSM, etc.*)

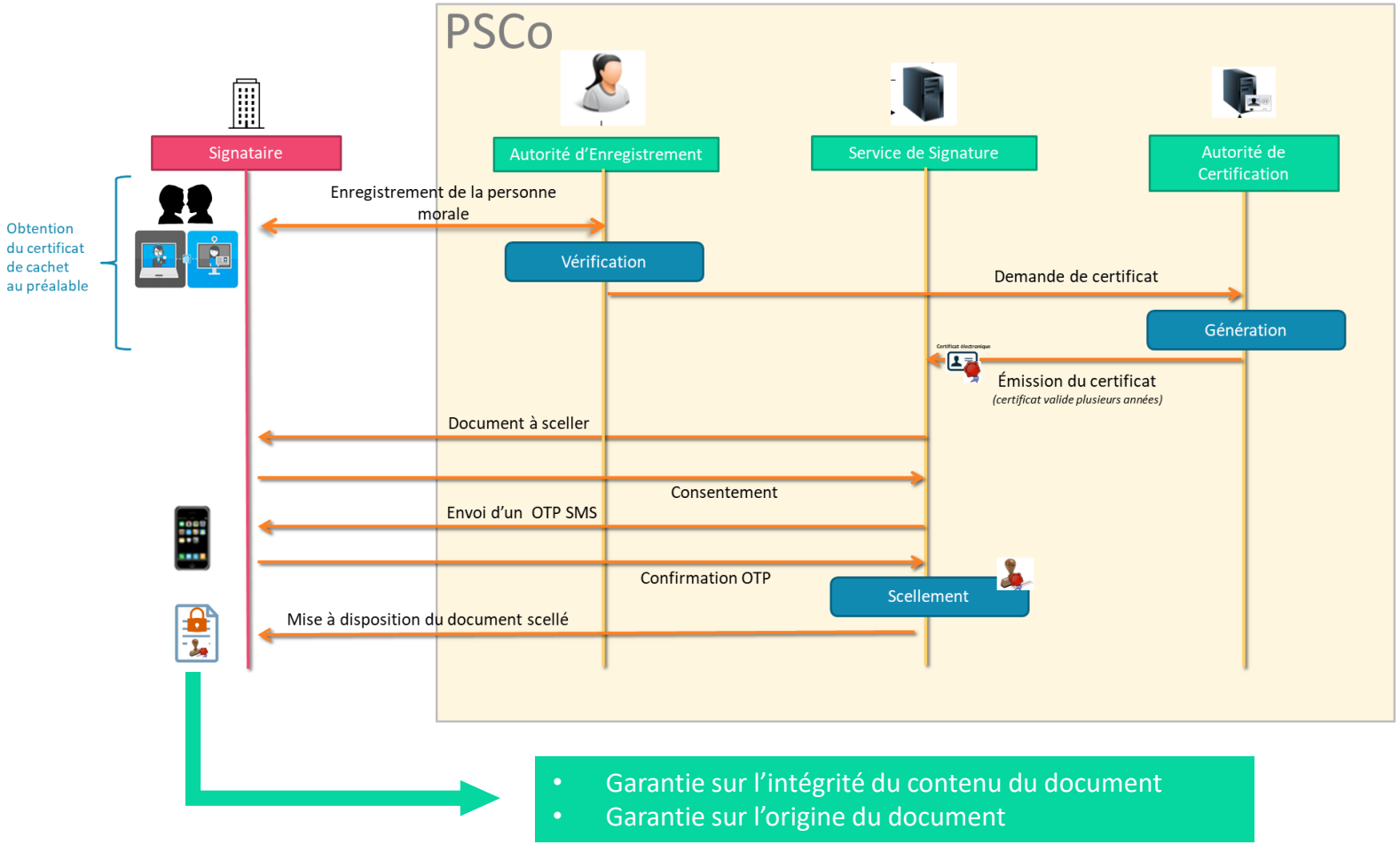
HSM

SEALWeb

Niveau de signature électronique retenu :

Présentation du concept

Cachet avancé avec un certificat qualifié

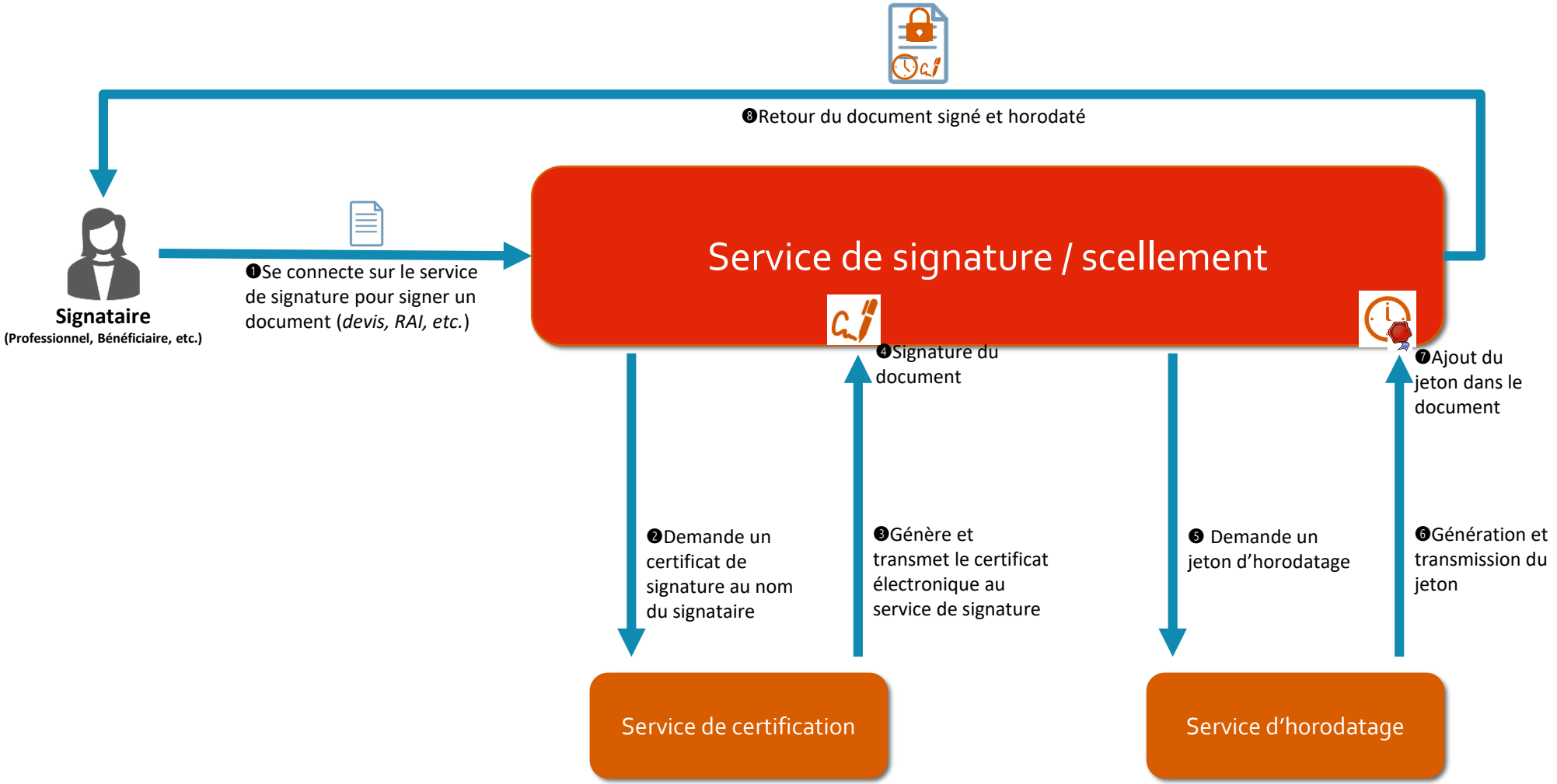


- Garantie sur l'intégrité du contenu du document
- Garantie sur l'origine du document

Les solutions pour encadrer les pièces électroniques

Articulation des services de confiance et du niveau de signature retenus

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES
Liberté
Égalité
Fraternité



Les solutions pour encadrer les pièces électroniques

Validité de la signature électronique / Format de la signature avancée

MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE, DE L'ÉNERGIE, DU CLIMAT ET DE LA PRÉVENTION DES RISQUES
Liberté Égalité Fraternité

Un document signé électroniquement doit être vérifiable dans le temps.

La validation de la signature d'un document consiste principalement à vérifier que :

- Le certificat était émis par une Autorité de Certification Qualifiée (reconnue)
- Le certificat était bien valide au moment de la signature
- Le certificat n'était pas révoqué au moment de la signature

La signature d'un document signé peut donc être vérifiée pendant une longue période en intégrant toutes les informations nécessaires pour garantir sa validité et permettre une validation autonome et pérenne

Plusieurs informations sont embarquées dans le document signé :

- Le certificat du signataire
- La chaine de certification complète
- Les données sur l'état de certificat du signataire
- L'horodatage de la signature qui prouve le moment précis de sa réalisation
- L'horodatage des données sur l'état de certificat du signataire

Format **AdES LT** (*Advanced Electronic Signature Long Term*)

permet de prolonger la validité de la signature au-delà de la durée de vie du certificat du signataire.

Format à exiger au fournisseur de service de signature

Les solutions pour encadrer les pièces électroniques

Exemples de secteurs dans lesquels les services de confiance sont déjà déployés

MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE, DE L'ÉNERGIE, DU CLIMAT ET DE LA PRÉVENTION DES RISQUES
Liberté
Égalité
Fraternité

BANQUE

Dématérialisation de la souscription à des offres de crédits (contrats)

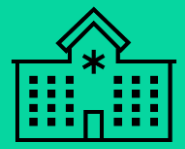
Signature électronique
(service de certification + service d'horodatage)

Notaire

NOTARIAT

Signature des actes authentiques

Signature électronique
(service de certification + service d'horodatage)



Compagnie AAA

ASSURANCE

Dématérialisation des échanges entre les courtiers et les assureurs

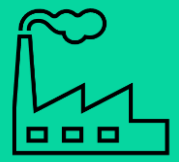
Signature électronique
(service de certification + service d'horodatage)

Copro

SYNDIC DE COPROPRIETE

Envoi de convocations et de PV d'Assemblée Générale

Envoi recommandé électronique



INDUSTRIE

Sécurisation des communications entre équipements

Service de certification

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ADMINISTRATION

Authentification des agents et protection des documents

Service de certification

SEALWeb

Mise en œuvre des dispositifs

Démarche pour la mise en place des services de confiance

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES
Liberté
Égalité
Fraternité

Les services de confiance retenus (service de certification et service d'horodatage) ainsi que le service de signature sont fournis par des Prestataires de Service de Confiance

Différents scénarios de mise en œuvre peuvent être envisagés :

Contractualisation à une offre Saas de signature « tout-en-un » auprès d'un PSCo et comprenant :

- La fourniture des certificats de signature + la fourniture de jeton d'horodatage pour chaque signature + l'usage de la solution de signature permettant d'orchestrer ces différents services de manière à générer une signature électronique permettant d'apporter les effets juridiques attendus

Recommandé

Sélectionner le fournisseur PSCo pour chaque composant (certification, horodatage, signature) et construire l'offre de signature :

- Inconvénients : à la charge du client d'intégrer et d'orchestrer les différents services fournis, solution difficile à construire puisque les PSCo peuvent ne pas offrir leur service à la pièce pour l'intégrer dans une offre de signature concurrente, par exemple : *un PSCo qui fournir sa solution de signature électronique imposera la solution d'horodatage utilisée (la sienne ou celle d'un partenaire)*

Peu recommandé compte-tenu de la complexité d'un tel projet et des volumes cibles

Mise en œuvre des dispositifs

Usage optionnel : cachet / scellement

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES
Liberté
Égalité
Fraternité

Contexte :

Utilisation optionnelle (*en remplacement de la signature électronique*) pour les cas particuliers précisés dans le tableau précédent : pour certains acteurs et pour certaines pièces.

Description :

Un certificat de cachet permettant de faire du scellement est délivré pour 2 ou 3 ans et est hébergé par un PSCo

→ Avantage : réutiliser le même certificat

Conditions de mise en œuvre :

- Réservé seulement aux personnes morales (*de type Professionnel et Contrôleur*)
- Au préalable : les personnes morales qui souhaitent sceller leurs documents et n'utiliser qu'un seul certificat, doivent obtenir en amont un certificat de cachet qualifié auprès d'un PSCo.

Inconvénients

- Usage limité à certaines pièces étant donné que le scellement a une couverture juridique différente d'une signature électronique (pas de non-répudiation).
- Dans les faits, le certificat de cachet est délivré pour 2 ou 3 ans et est hébergé par un PSCo qui est charge de son exploitation. Le propriétaire du certificat de cachet a donc deux solutions :
  - *Soit utiliser le service de signature du PSCo qui lui a fourni son certificat de cachet,*
  - *Soit utiliser n'importe quel service de signature à condition d'héberger lui-même son certificat de cachet*

  → ***Contraintes majeures :*** *nécessite d'opérer un HSM et engendre une complexité l'intégration.*

Mise en œuvre des dispositifs

Synthèse des services à utiliser par pièce

MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE, DE L'ÉNERGIE, DU CLIMAT ET DE LA PRÉVENTION DES RISQUES
Liberté Égalité Fraternité

	Professionnel	Bénéficiaire	Contrôleur
Devis	ou (option) + Jeton	+ Jeton	NA
RAI	ou (option, si RAI unilatéral) + Jeton	+ Jeton	NA
Attestation sur l'honneur	+ Jeton	+ Jeton	NA
Preuve de réalisation	+ Jeton	NA	NA
Pièces complémentaires	ou (option) + Jeton	NA	NA
Contrôle de l'opération	NA	NA	ou (option) + Jeton

LEGENDE :

- Signature électronique
- Scellement électronique
- Horodatage (Jeton)

SEALWeb

Mise en œuvre des dispositifs

Les Prestataires de Confiance (fournisseurs)

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES
Liberté
Égalité
Fraternité

Offre complète de signature électronique en mode Saas*

docusign

CERTEUROPE
AN INFOCERT COMPANY

DOCAPOSTE

CERTIGNA by tessi

yousign

Universign
by Signaturit Group

cegedim

LEX persona

Offre de certificat de cachet en mode Saas*

ChamberSign
Autorité de certification des CCI

DOCAPOSTE

LEX persona

cegedim

CERTIGNA by tessi

docusign

CERTEUROPE
AN INFOCERT COMPANY

Universign
by Signaturit Group

yousign

* Liste non exhaustive basée sur la Trusted List eIDAS FR

Mise en œuvre des dispositifs

Les coûts à prévoir

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES
Liberté
Égalité
Fraternité

Coût d'une signature composé :
- Du coût de délivrance d'un certificat qualifié
- Du coût du jeton d'horodatage associé à la signature

Exemple :

Pour un document signé par deux parties, on prévoit :
- 2 signatures électroniques avancées avec certificats qualifiés
- 2 horodatages (1 associé à chaque signature)

Coût moyen d'une signature avancée avec certificat qualifié :	**1,5 € environ**	Pour 500 signatures *(dégressif pour des volumes supérieurs)*
Coût d'une vérification d'identité à distance	**2 € environ**	

Coût d'un certificat de cachet	**Entre 300€ et 800€ /an**
Coût d'un scellement	**0,10€ environ**

Identifier **le volume potentiel de dossiers** à monter et donc de **documents à signer** pour identifier le **nombre de signatures** et le **nombre d'horodatages** consommés à l'année
→ Permet d'avoir une **estimation du coût du service global à l'année**.

Expérience utilisateur

Démo

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES

Liberté
Égalité
Fraternité

Démonstration d'une signature électronique

Modification de la FAQ (Q III.b.4)

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES
Liberté
Égalité
Fraternité

Dans quelle mesure l'utilisation de la signature dématérialisée dans les pièces archivées des opérations est-elle possible ?

- Si un bénéficiaire indique ne pas avoir signé un document issu du procédé de signature électronique décrit ci-dessus, ou que les données contrôlées ne correspondent pas à celles figurant sur le document qu'il a signé, il conviendra d'identifier l'origine de la fraude et ainsi le périmètre des opérations pouvant être concernées par la même problématique (par exemple : documents signés avec le même procédé, ou générés par le même professionnel, ou réseau de professionnels, ou mandataire). **Un plan de contrôle, qui devra être validé par la DGEC, devra être mis en oeuvre pour identifier les opérations impactées.**
- Les opérations générées selon un procédé de signature électronique qui n'est pas au moins celui de la proposition énoncée, sont non conformes à la réglementation et ne peuvent donner lieu à délivrance de CEE.
- Conformément à l'article L. 221-10 du code de l'énergie, les pièces constitutives d'une demande de certificats d'économies d'énergie peuvent être transmises, et également conservées par le demandeur de certificats d'économies d'énergie aux fins d'archivage, sur support durable.

Calendrier

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE,
DE L'ÉNERGIE, DU CLIMAT
ET DE LA PRÉVENTION
DES RISQUES
Liberté
Égalité
Fraternité

Envoi des contributions écrites d'ici le **11 décembre 2024**

A l'adresse mail : cee@developpement-durable.gouv.fr

Objet du mail : « Nom de la structure - Contribution Encadrement des pièces électroniques CEE »