

Webinaire le 14 novembre à 11h



CR²PA
Club de l'Archivage Managérial

Signature électronique

- Quel est le cadre réglementaire ?
- Quel niveau de signature ?
- Pourquoi vérifier la signature ?
- Quelle gestion de la preuve ?
- Comment l'archiver ?



Signature électronique :
Webinaire le 14 novembre 2022



CR²PA
Club de l'Archivage Managérial

Intervenants



Amélie Frézier,
Responsable des partenaires
stratégiques de Cecurity.com,
adhérent de la FnTC



Pascal Agosti,
Avocat associé,
Cabinet Caprioli & Associés,
adhérent de la FnTC



Jean-Mathieu Bonnefous,
Records Manager
du groupe Orano,
adhérent CR2PA



Nathalie Jubin,
Records and Information
Manager chez Engie
Global Energy
Management & Sales,
adhérent CR2PA



Chantal Pasquier,
Chargée de veille et
d'archivage, Egis
adhérent CR2PA



Programme

1. Qu'est-ce que la signature ?

- Définition
- Le cadre réglementaire
- Les différents niveaux de signature

2. Validation et gestion de la preuve

- Validation des signatures, pourquoi et comment vérifier ?
- Gestion de la preuve et de ses constituants.
- Archivage : que faut-il conserver, et qui archive quoi ?

3. Retour d'expérience sur la mise en place de la signature

- Cas d'usages: les questions à se poser et l'identification des documents à signer
- La question des preuves.

4. Notre prochain guide : "La signature électronique III : conservation à long terme des documents signés"

5. Questions / Réponses





Signature électronique :
Webinaire le 14 novembre 2022



1

Qu'est-ce que la signature électronique ?

Lire notre premier guide : "La signature
électronique : Définitions et cas d'usage"



Importance de la signature électronique :

Tous les types techniques de signatures électroniques répondant a priori ou a posteriori aux exigences de l'article 1367 C. civ. sont valables.

Seule la charge de la preuve est impactée : renversement de la charge.

Définition fonctionnelle de toutes les signatures (art. 1367 al. 1) :

- Identification de l'auteur ;
- Manifestation du consentement à l'acte ;
- Confère l'authenticité à l'acte quand elle est apposée par un officier public (acte authentique).



Un cachet électronique permet de « prouver qu'un document électronique a été délivré par une personne morale en garantissant l'origine et l'intégrité du document » (art. 3,25 Règlement eIDAS) .



Signature électronique : Webinaire le 14 novembre 2022



Les niveaux de signature

Niveau de signature	Description eIDAS
Électronique simple	C'est un ensemble de « données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer. »
Électronique avancée	C'est une signature électronique qui doit : • Être liée au signataire de manière univoque ; • Permettre d'identifier le signataire ; • Avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; • Être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.
Électronique qualifiée	C'est une « signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique. »



Signature électronique :
Webinaire le 14 novembre 2022



2

Validation et gestion de la preuve

Lire le deuxième guide :
"La signature électronique : Validation et Archivage"



La validation

3 questions fondamentales :

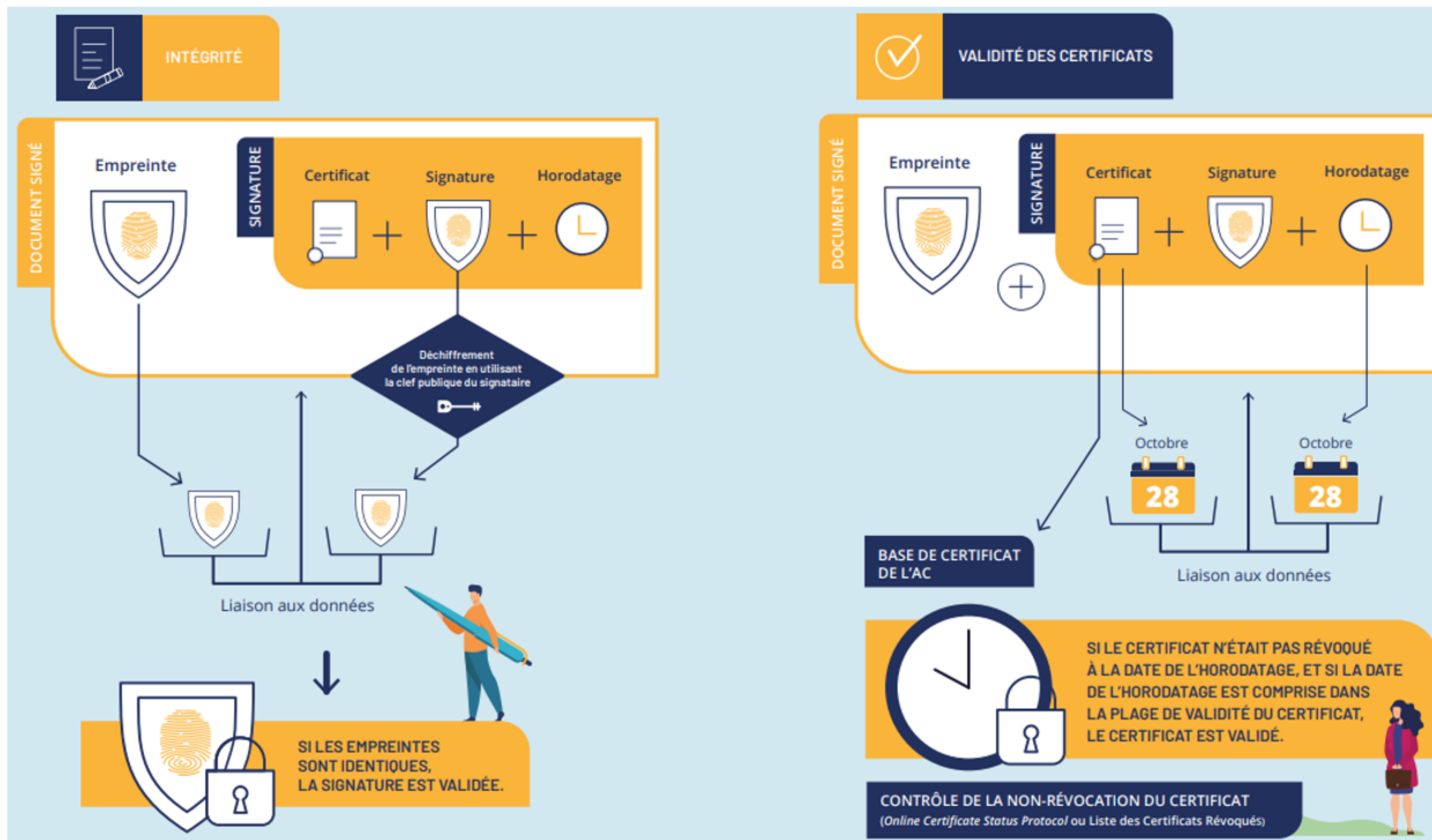
- Qu'est-ce que la validation ?
- Quels en sont les enjeux et les risques ?
- Quand et pourquoi la réaliser ?





Signature électronique : Webinaire le 14 novembre 2022

Qu'est-ce que la validation ?





Les enjeux et les risques de la validation

- S'assurer la validité de la signature et du certificat au moment de la signature.
- Réaliser la validation après expiration du certificat.





Quand et pourquoi valider une signature ?

- La recommandation FnTC: valider au plus tôt après l'acte de la signature.
- En plus de vérifier l'intégrité et l'authenticité de la signature, la validation est génératrice de preuves informatiques.





Le fichier de preuves, qu'est-ce que c'est ?

Il n'existe pas de définition légale.

« Ensemble des éléments créés lors de la conclusion d'un contrat pour un produit ou service entre un Client et un organisme puis conservé pendant un délai conforme aux exigences légales permettant ainsi d'assurer la traçabilité, la preuve de la réalisation de l'opération conclue, ainsi que sa restitution en cas de litige (expertise). Il peut s'agir notamment des traces d'authentification, des traces d'acceptation des documents contractuels, des traces sur les certificats, sur l'horodatage, contrat(s) signé(s) + données de connexion... ».

Quelle est son utilité ?

- **Convaincre un juge** ou une administration de la valeur juridique et de la force probante de l'écrit sous forme électronique auquel une personne recourt ;
- Vérification de la validité de la signature électronique **au moment de l'établissement de l'écrit sous forme électronique** mais aussi pendant toute la période de conservation et/ou de prescription légale.



Reconnaissance du fichier de preuves

CA Nancy, 14 février 2013

Appel de la décision du TI Epinal du 12 décembre 2011

- Fichier de preuve de la transaction, produit aux débats, a été émis par l'autorité de certification.
- Démonstration en justice du mode de fonctionnement et production d'une attestation du prestataire.
- « *la mention du numéro de l'avenant sur le fichier de preuve permet de vérifier que c'est bien cet avenant qui a été signé électroniquement par Monsieur X* ».

-> Action en paiement non forclosée pour la Banque.

Idem CA Douai, 2 mai 2013





Reconnaissance du fichier de preuves



CA Chambéry, 25 janvier 2018 :

- Admission de la fiabilité du procédé de signature électronique d'un contrat de crédit à la consommation, en se fondant sur le **fichier de preuve fourni par un prestataire de service de confiance**.
- **Une synthèse de fichier de preuve** de la transaction Q0IPPERS - PQSPASS -50972441639001-2015.5.5-8.18.41.1194, émanant de la société X. ayant la qualité de prestataire de service de gestion de preuve, qui atteste de la signature électronique le 05/05/2014 à 08:18:47 du document référencé par monsieur Sammy Y, dont elle précise l'adresse mail et qui mentionne le code d'identité du certificat électronique.

Cette décision place le prestataire de service de confiance
au cœur du procès en matière d'admissibilité de la preuve
de la signature électronique et de sa fiabilité.

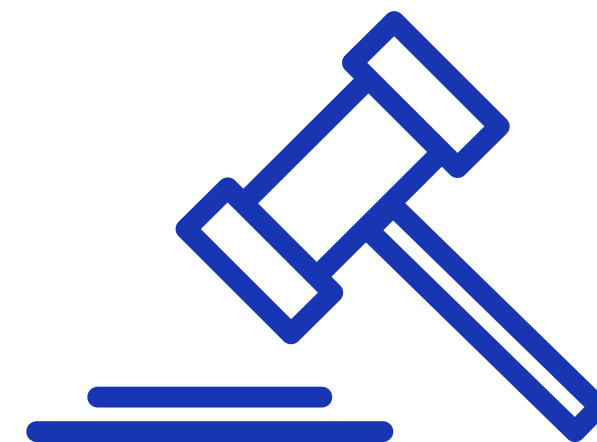


Mais aussi :

TI Nîmes 18 septembre 2018

Production par l'établissement de crédit

- D'une attestation de fiabilité des pratiques de l'opérateur de prestation ;
- Et d'une synthèse du fichier de preuve contenant toutes les informations utiles pour démontrer l'existence du contrat signé ainsi que du consentement du particulier.



-> Le Tribunal considère que ces éléments permettent d'authentifier la signature électronique du contrat par la cliente et que la preuve de l'existence du contrat est donc rapportée.

Nul besoin d'une signature électronique sécurisée bénéficiant de la présomption de fiabilité du procédé de signature conformément à l'article 1367, al. 2, 2ème phrase et au Décret du 28 septembre 2017 (désormais signature électronique qualifiée), une signature électronique simple (ou avancée) suffit. En revanche, une gestion maîtrisée de la preuve électronique, de son émission jusqu'au terme du délai d'archivage est résolument préconisée face à l'accroissement de ce type de contentieux. En effet, dans cette hypothèse il fallait prouver la fiabilité de la signature électronique.



Que se passe-t-il en l'absence de fichier de preuve ?

Cour d'appel, Grenoble, 1^{re} chambre civile, 15 Juillet 2020, n°19/00434

Une société de financement assigne sa cliente en remboursement d'un prêt qu'elle lui aurait consenti deux ans plus tôt.

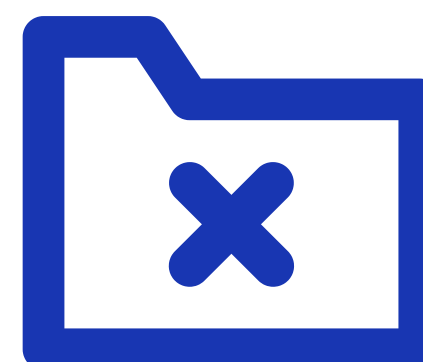
Le tribunal n'avait pas fait droit aux demandes de la société au motif que **le contrat de prêt produit ne comportait aucune signature.**

La Cour d'appel confirme le premier jugement en ce qu'il considère que la société de financement ne rapporte pas la preuve de sa créance.

La Cour retient que **le bordereau des pièces justificatives indique une pièce attestant de la signature électronique de l'assigné, pièce qui n'est pas effectivement versée au débat.**

La preuve de l'existence de la signature n'est pas apportée.
Sans preuve de l'existence de la signature, la preuve du consentement ne peut être apportée.

Il est donc essentiel de pouvoir disposer d'un fichier de preuve reprenant l'ensemble des opérations sur le contrat.





Quel doit être son contenu ?

Les éléments communs à tous les fichiers de preuve :

- Procédé d'identification utilisé (enrôlement,...)
- Niveau de certificat
- Procédé d'authentification utilisé au moment de la signature électronique
- La procédure de consentement
- Liste des éléments à archiver
- Horodatage de chaque action
- Preuve de validation





Archiver, conserver ?

Article 1366 du Code civil :

“L’écrit électronique a la même force probante que l’écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu’il soit établi et conservé dans des conditions de nature à en garantir l’intégrité ”

La conservation permet de rapporter la preuve des droits (c’est-à-dire des informations contenues dans un document) tandis que l’archivage a trait au support (le document proprement dit) à des fins juridiques.

Les normes Z 42-013 et Z 42-020 permettent de garantir l’archivage dans une solution à valeur probatoire



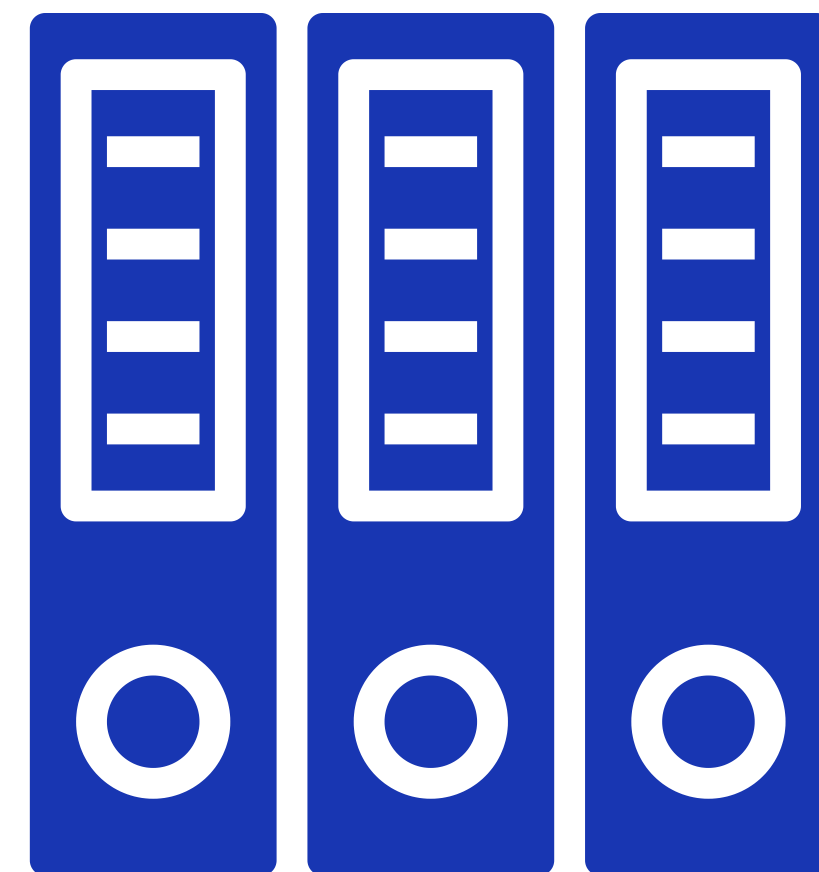


Que faut-il archiver ?

Il est important d'archiver le document signé, mais aussi et surtout sa signature (si elle n'est pas incluse dans le document), ainsi que les éléments de preuves.

Tout ceci permettra dans la durée :

- d'identifier le ou les signataires,
- de garantir l'intégrité, de rendre disponible toutes les informations aussi longtemps qu'il sera nécessaire.





Qui archive quoi ?

Il convient de suivre les procédures d'archivage électronique de son organisation (n'hésitez pas à consulter les mémos du CR2PA).

Une nécessité : définir les rôles et les responsabilités de chacun (Ne pas uniquement se fier aux outils de signature ou au format d'archivage) :

- Qui archive ? Comment et surtout à quel moment ?
- Le ou les signataires, le prestataire de signature, le prestataire d'archivage.

Ne pas oublier de définir les passerelles entre un prestataire de signature et un prestataire d'archivage

Point d'attention : selon le Tiers de Confiance et la solution utilisée, il est important de définir et de ne pas oublier dans le contrat , la notion de récupération et/ou l'archivage des éléments de preuve. Ceci n'est pas toujours automatique.



**Signature électronique :
Webinaire le 14 novembre 2022**



3

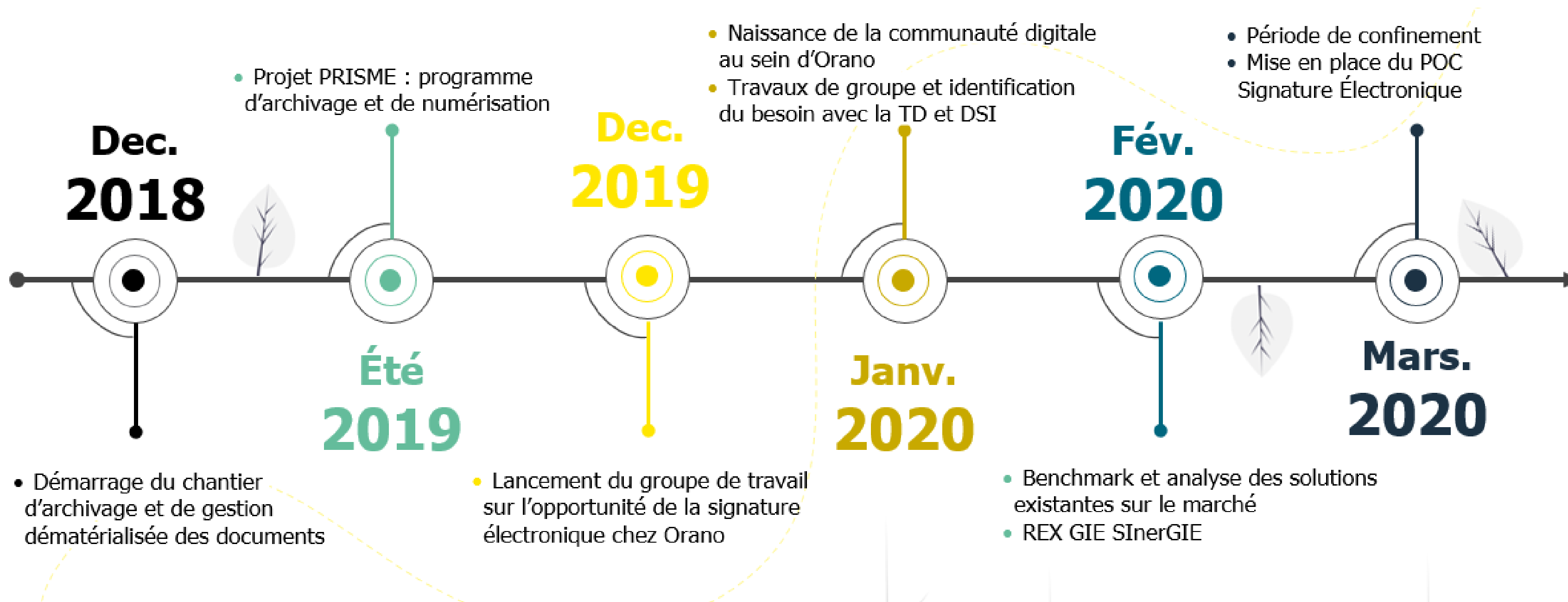
Retour d'expérience

Le déploiement de la signature électronique
au sein du Groupe Orano



Signature électronique : Webinaire le 14 novembre 2022

Une réflexion de fond chez Orano





Un projet qui trouve sa source dans les besoins exprimés





A. Les cas d'usage :

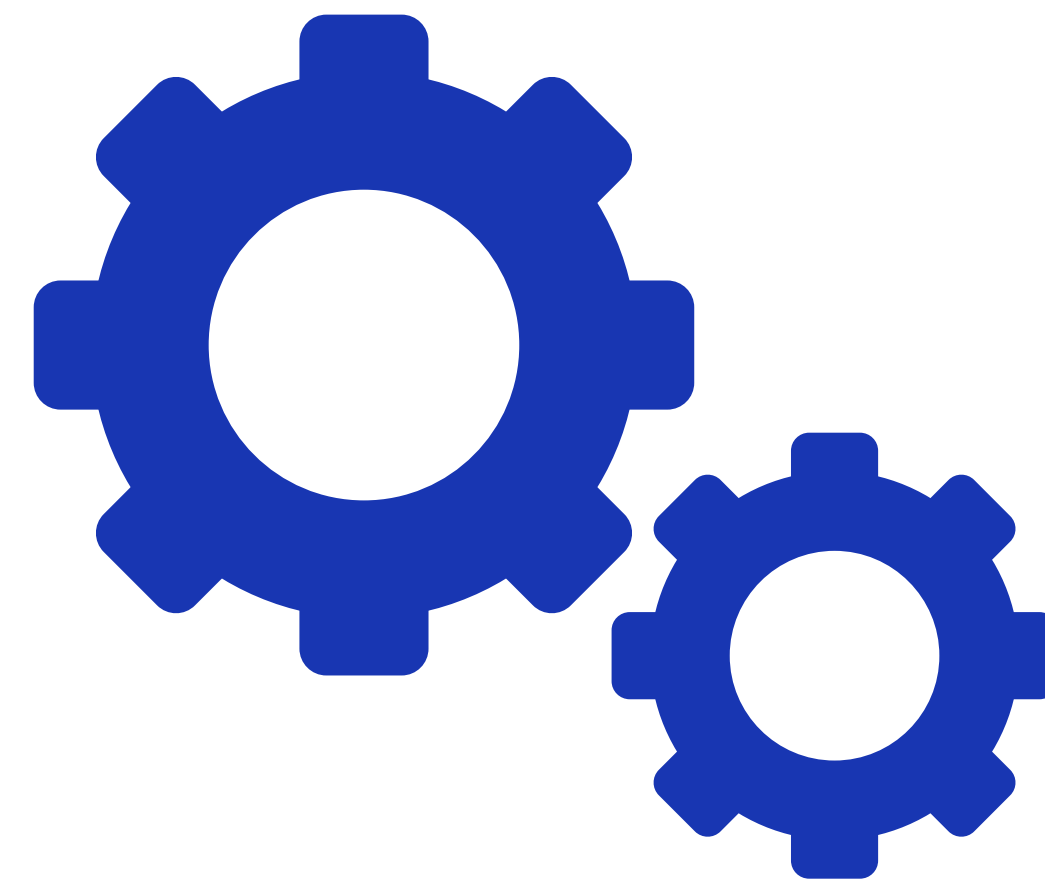
Les questions à se poser & l'identification des documents à signer





L'approche méthodologique proposée par les guides : une appréhension des enjeux

- Une implication initiale du réseau juridique du groupe
- La diffusion des principes de la signature électronique à l'occasion de réunions et rencontres juridiques
- La définition de besoins clairs
- Le cadrage de projet
- La maîtrise du périmètre de déploiement pour éviter une utilisation anarchique





**Signature électronique :
Webinaire le 14 novembre 2022**



B. La question des preuves





Le lien avec le Système d'Archivage Électronique d'Orano

- L'archivage électronique a du sens pour rapporter la preuve d'un droit dans le temps.
- La façon dont sont gérés tous les éléments nécessaires à prouver la recevabilité d'un document signé doit absolument prendre en compte leur archivage. La qualité de ce dernier est en effet indispensable pour disposer d'un ensemble fiable d'un point de vue légal et réglementaire.
- Une gestion maîtrisée de la preuve électronique, de son émission jusqu'au terme du délai d'archivage.
- Archivage des éléments de preuves (documents signés et éléments de preuve) dans le SAE d'Orano.



La gestion de l'Export-Control pour la signature électronique :



DECSI Flash - Importance 5/5 DJ-DECSI-2021-51

23 août 2021 • August 23rd, 2021

- Signature électronique

Export Control - Utilisation libre · DHL-21-605629

Problématique : Les données traitées par [redacted] sont susceptibles de transiter sur des serveurs français, allemands et néerlandais. Certains contrats peuvent contenir des données à double usage qui ne peuvent être exportées sans licence d'exportation préalable.

Décision du Service des Biens à Double Usage : Après examen des mesures de sécurité des flux et des serveurs et des conditions d'accès aux serveurs, le SBDU a émis un avis de non-classement : la signature de documents via [redacted] ne constitue pas une exportation de technologie au sens du règlement (CE) 428/2009 du 5 mai 2009 modifié.

Cas des documents signés comportant des données à double usage :
Les règles suivantes sont à respecter :

- L'envoi du contrat vers notre partenaire doit s'inscrire dans le cadre d'une licence d'exportation précédemment délivrée par le SBDU, en lien avec le projet.
- Orano informe le SBDU de l'utilisation de [redacted]
- Une traçabilité des échanges réalisés via [redacted] doit être conservée dans le SAE Orano.

- Un dialogue en pleine transparence avec le Service des Biens à Double Usage (SBDU) pour exposer le besoin et les pistes de réflexion.
- Orano a été le premier exportateur à porter le sujet signature électronique devant le SBDU.
- Des propositions de solutions et de processus en accord avec la réglementation.
- Une acculturation progressive avec les instances de régulations et / ou autorités (échanges avec l'ASN et l'IRSN).



**Signature électronique :
Webinaire le 14 novembre 2022**



C. Un exemple type du déploiement de la démarche à l'appui des guides





La mise en place de la signature électronique avec les établissements bancaires

- Besoin du département des Opérations de Financement et de Trésorerie.
- Prises de contact avec les établissements bancaires pour évoquer l'opportunité d'échanges dématérialisés signés électroniquement.
- Échanges sur les typologies documentaires concernés avec définition des bons niveaux de signatures.
- Conventions de preuves établies avec les établissements partenaires en vue de la mise en place des échanges via un PSCO.



Quelques éléments de conclusion : l'apport clé des guides

- Les guides ont permis de structurer la démarche de déploiement de la signature électronique au sein d'Orano.
- Un facteur X très important : l'implication en amont de la direction juridique pour l'appropriation du domaine, la définition et l'encadrement des cas d'usage.
- La connexion avec la gouvernance de l'information.
- L'archivage électronique comme réponse à la préservation des éléments de preuve à vocation probatoire.





**Signature électronique :
Webinaire le 14 novembre 2022**



PRÉSENTATION DE NOTRE GUIDE : « CONSERVATION À LONG TERME DES DOCUMENTS SIGNÉS ».

**22 NOVEMBRE 2022 - 17H30
HOTEL BEDFORD - PARIS**

<https://www.eventbrite.fr/e/billets-signature-electronique-presentation-du-nouveau-guide-fntc-cr2pa-464142210847>



Signature électronique :
Webinaire le 14 novembre 2022



Vos questions ?





FÉDÉRATION DES TIERS DE CONFIANCE DU NUMÉRIQUE

POUR EN SAVOIR PLUS SUR LA FNTC :
WWW.FNTC-NUMERIQUE.COM
INFOS@FNTC-NUMERIQUE.COM



POUR EN SAVOIR PLUS SUR LE CR2PA :
WWW.CR2PA.FR
CONTACT@CR2PA.FR