

<b>Statut du document</b>	Référence officielle du gouvernement fédéral américain par la NARA ( <i>National Archives and Records Administration</i> )
<b>Titre</b>	<i>Records Management Guidance for Agencies Implementing Electronic Signature Technologies</i> Directive aux Agences déployant la technologie de signature électronique
<b>Mot clé</b>	Conservation et métadonnées
<b>Source</b>	NARA <a href="http://www.nara.gov/records/policy/gpea.html">http://www.nara.gov/records/policy/gpea.html</a>
<b>Date de publication</b>	18 octobre 2000
<b>Nombre de pages</b>	12
<b>Langue</b>	Anglais
<b>Lien avec autres normes</b>	
<b>Situation actuelle</b>	
<b>Description</b>	<p>À l'heure où le gouvernement américain poursuit des objectifs ambitieux en matière de formulaires et de signatures électroniques, ce guide présente les pratiques recommandées en gestion des documents devant être conservés à des fins légales ou autres. Ces pratiques de gestion documentaire font partie intégrante des exigences d'affaires qui doivent être adaptées aux caractéristiques de l'information électronique. Ce guide s'adresse autant aux informaticiens qui développent des applications avec signature électronique, pour qu'ils saisissent les exigences de conservation des documents, qu'aux services de gestion documentaire, pour qu'ils reconduisent l'interprétation de leur savoir-faire disciplinaire sur un nouveau terrain: ceci, dans le but que les exigences de gestion documentaire se retrouvent au cœur des spécifications des applications. La <i>signature électronique</i> peut se faire par la signature numérique, l'emploi de NIP, de carte à puce, ou de biométrie.</p> <p>Le document doit souvent être conservé plus longtemps que le système, logiciel ou application qui a servi à le créer. Son cycle de vie relativement long oblige à des précautions dans les migrations de données qui pourraient être requises.</p> <p>Pour qu'un document soit fiable, on doit pouvoir y avoir accès techniquement et pouvoir vérifier son intégrité et son authenticité. Selon l'importance de la transaction que vient nouer un document et selon les risques de fraude qui y sont associés, des mesures proportionnées d'assurance peuvent être employées. Il faut assurer la conservation à la fois du contenu, de son contexte et de sa structure logique et physique. Au moins deux grandes approches existent pour garantir la fiabilité à long terme des documents signés électroniquement :</p> <ul style="list-style-type: none"> <li>- Établir la documentation entourant la validité des documents et recueillir les éléments d'information qui doivent l'être en complément pour être conservés avec le document pendant toute sa durée de conservation. Cette cueillette d'information, effectuée aussi près que possible du moment de signature, s'apparente aux activités de gestion documentaire dans sa partie contrôle administratif, i.e. de tenue de dossiers. Par rapport à la seconde approche, ces métadonnées apportent un degré d'indépendance face à la technologie en fournissant une source de validité plus facile à maintenir.</li> <li>- Garder la capacité de revalider les signatures numériques, ce qui contraint à conserver des certificats de clé publique et des chaînes de vérification d'autorités de certification à long terme. Cette approche risque de devenir plus lourde avec le temps.</li> </ul>

	<p>En réalité, on peut doser les deux approches, mais elles sont toutes deux nécessaires. Le commerce électronique oblige à disposer d'une capacité de validation de signature numérique aux fins de non-répudiation, sans rien enlever aux obligations de tenue de dossier, quoique les automates puissent éviter des tâches fastidieuses de saisie de métadonnées aux signataires de document. Quelle que soit l'approche choisie, il est exigé que le document reste accessible (lisible) pour sa durée de vie et qu'il comporte l'inscription, en caractères d'imprimerie, du nom du signataire et de la date de signature. La norme ISO/IEC JTC1/SC27 N1503 et N1505 sur la non-répudiation est recommandée comme cadre conceptuel de vérification.</p> <p>La NARA suggère une liste d'étapes à suivre pour assurer la fiabilité des documents électroniques signés qu'on produit ou qu'on reçoit. La modulation des solutions doit se faire en fonction des risques encourus en contexte. La marche à suivre pour la préservation à long terme n'est pas encore claire.</p>
--	---

## Remarque

### Lexique anglais-français

Trustworthy, trustworthiness                      Fiable, fiabilité

**Rédacteur :** Richard Parent  
**Organisation source :** Secrétariat du Conseil du trésor  
**Date de publication :** 12 décembre 2000  
**Raison d'être :** Connaissance technologique  
**Programme gouvernemental :** Inforoutes et ressources informationnelles  
**Nom du modificateur :**  
**Date de dernière modification :**  
**Note numéro :** 83