

# *Guide de l'archivage électronique sécurisé*

Recommandations pour la mise en œuvre  
d'un système d'archivage interne ou externe utilisant  
des techniques de scellement aux fins de garantir  
l'intégrité, la pérennité et la restitution des informations



*12 juillet 2000*

version V



## Membres du groupe de travail ayant participé à la rédaction du présent document :

- Nadia Antonin (Banque de France, EdiFrance), [nadia.antonin@banque-France.fr](mailto:nadia.antonin@banque-France.fr)
- François Bary (Cabinet d'expertise comptable CBA), [cbabary@club-internet.fr](mailto:cbabary@club-internet.fr)
- Franklin Brousse (Alain Bensoussan-Avocats), [ab@alain-bensoussan.tm.fr](mailto:ab@alain-bensoussan.tm.fr)
- Brigitte Candebat (Cessi / Cnam-TS), [brigitte.candebat@cnamts.fr](mailto:brigitte.candebat@cnamts.fr)
- Anne Cantéro (Cabinet d'avocats Eric Caprioli), [annecantero@yahoo.fr](mailto:annecantero@yahoo.fr)
- Michel Chevrier (Ialta), [michevrier@fr.europost.org](mailto:michevrier@fr.europost.org)
- Bruno Couderc (Aproged, BJC Consultants), [bcouderc@aol.com](mailto:bcouderc@aol.com)
- Pierre-Yves Fagot (Arthur Andersen International), [pierre.yves.fagot@fr.andersenlegal.com](mailto:pierre.yves.fagot@fr.andersenlegal.com)
- Caroline Gans (Protécra), [c.gans@protecrea.org](mailto:c.gans@protecrea.org)
- Odile Lajoix (Cabinet d'avocat) [info@avocats-conseils.org](mailto:info@avocats-conseils.org)
- Jean-Noël Le Roux (Neartek), [jean-noel.leroux@neartek.com](mailto:jean-noel.leroux@neartek.com)
- Michel Lesourd (CS-OEC, Edificas, EdiFrance), [mlesourd@wanadoo.fr](mailto:mlesourd@wanadoo.fr)
- Claude de Martel (CSN), [jd.mathias@notaires.fr](mailto:jd.mathias@notaires.fr)
- Pascal Martin-Retord (Cabinet d'expertise comptable PMR) [gmrpmr@aol.com](mailto:gmrpmr@aol.com)
- Jean-Claude Monnier (GED Software), [jean-claude.monnier@msg-software.com](mailto:jean-claude.monnier@msg-software.com)
- Jean-François Orosco (Cabinet d'expertise comptable HLB-Sogesco), [jf.orosco@wanadoo.fr](mailto:jf.orosco@wanadoo.fr)
- Etienne Pelletier (Ialta), [etiennep@aol.com](mailto:etiennep@aol.com)
- Bruno Picard (Aptilon), [bpicard@aptilon.com](mailto:bpicard@aptilon.com)
- Thierry Piette Coudol (Cabinet d'avocats Bertrand & associés, Ialta), [piettecoudol@wanadoo.fr](mailto:piettecoudol@wanadoo.fr)
- Pierre Pluvinage (CNHJ), [cnhj.informatique@huissier-justice.fr](mailto:cnhj.informatique@huissier-justice.fr)
- Gabriel Schmitt (Altaïr Technologies), [schmitt\\_gabriel@hotmail.com](mailto:schmitt_gabriel@hotmail.com)
- Gilles Trouessin (Cessi / Cnam-TS), [gilles.trouessin@cnamts.fr](mailto:gilles.trouessin@cnamts.fr)
- Gérard Weisz (Aproged, Sirius Systems), [siriusf@club-internet.fr](mailto:siriusf@club-internet.fr)

**sous la direction de** Michel Lesourd, expert-comptable diplômé, Directeur des Etudes informatiques pour la profession comptable du Conseil supérieur de l'Ordre des experts-comptables et Délégué général de l'association EDIFICAS, de Gabriel Schmitt, ingénieur informaticien, société Altaïr Technologies, et Thierry Piette Coudol, avocat, Cabinet d'avocats Bertrand & associés, Président de l'association IALTA.

Un **Comité de Suivi** procédera à une mise à jour du document. Toute observation, contribution ou critique peut lui être communiquée à l'une des adresses suivantes :

[mlesourd@wanadoo.fr](mailto:mlesourd@wanadoo.fr) ou [ialta@ialtafrance.org](mailto:ialta@ialtafrance.org)

Reproduction du document autorisée, moyennant la citation de l'intitulé exact du document "Guide de l'archivage électronique sécurisé" et de l'auteur "EDIFICAS & IALTA", en mentions claires, apparentes et parfaitement lisibles, et son affectation à une utilisation personnelle ou strictement non commerciale, quel que soit le support. Cependant, toute reproduction sur un support tel que cédérom, disquette ou tout autre média permettant une diffusion de masse, y compris mais sans limitation une diffusion sonorisée, visualisée, etc., doit être autorisée préalablement par écrit par l'auteur. La demande d'autorisation doit être adressée à l'une des adresses électroniques suivantes : [mlesourd@wanadoo.fr](mailto:mlesourd@wanadoo.fr), [ialta@ialtafrance.org](mailto:ialta@ialtafrance.org).



# Sommaire

<b>PRÉAMBULE</b> .....	<b>7</b>
<b>1. INTRODUCTION</b> .....	<b>9</b>
11. FINALITÉS DU GUIDE D'ARCHIVAGE ÉLECTRONIQUE SÉCURISÉ .....	9
12. DIMENSION JURIDIQUE DE L'ARCHIVAGE.....	9
<b>2. NOTIONS SOMMAIRES DE SCÉNARI</b> .....	<b>11</b>
21. COMPOSITION DES SCÉNARI .....	11
211. <i>Les éléments électroniques à archiver</i> .....	11
212. <i>Les acteurs</i> .....	11
213. <i>Les protocoles d'échanges</i> .....	11
22. TYPOLOGIE DES SCÉNARI .....	11
<b>3. OBJETS À ARCHIVER &amp; GESTION DES TABLES DES ARCHIVES</b> .....	<b>13</b>
31. OBJETS À ARCHIVER.....	13
32. GESTION DES TABLES DES ARCHIVES.....	13
321. <i>Gestion de la table des archives chez le donneur d'ordre</i> .....	13
322. <i>Gestion de la table des archives chez le tiers archiveur</i> .....	14
<b>4. PRÉSENTATION DU MODÈLE</b> .....	<b>15</b>
<b>5. LES ARCHIVES SONT CONFIÉES À UN TIERS ARCHIVEUR</b> .....	<b>17</b>
51. SCÉNARIO I : TÉLÉTRANSMISSION DES ARCHIVES.....	17
511. <i>TRAITEMENT 1 (sur l'initiative du donneur d'ordre)</i> .....	17
512. <i>TRAITEMENT 2 (sur l'initiative du tiers archiveur)</i> .....	18
513. <i>TRAITEMENT 3 (sur l'initiative du donneur d'ordre)</i> .....	19
52. SCÉNARIO III : TÉLÉTRANSMISSION DES DEMANDES D'ARCHIVES .....	19
521. <i>TRAITEMENT 1 (sur l'initiative du donneur d'ordre)</i> .....	20
522. <i>TRAITEMENT 2 (étape facultative sur l'initiative du tiers archiveur)</i> .....	20
523. <i>TRAITEMENT 3 (sur l'initiative du tiers archiveur)</i> .....	21
524. <i>TRAITEMENT 4 (sur l'initiative du donneur d'ordre)</i> .....	21
525. <i>TRAITEMENT 5 (sur l'initiative du tiers archiveur)</i> .....	22
<b>6. LES ARCHIVES RESTENT CONFIÉES AU DONNEUR D'ORDRE</b> .....	<b>23</b>
61. SCÉNARIO II : TÉLÉTRANSMISSION DU SCEAU DES ARCHIVES (DU MOYEN DE CONTRÔLE DE L'INTÉGRITÉ DES ARCHIVES).....	24
611. <i>TRAITEMENT 1 (sur l'initiative du donneur d'ordre)</i> .....	24
612. <i>TRAITEMENT 2 (sur l'initiative du tiers archiveur)</i> .....	25
613. <i>TRAITEMENT 3 (sur l'initiative du donneur d'ordre)</i> .....	26
62. SCÉNARIO IV : RESTITUTION DU SCEAU CHIFFRÉ DES ARCHIVES .....	26
621. <i>TRAITEMENT 1 (sur l'initiative du donneur d'ordre)</i> .....	27
622. <i>TRAITEMENT 2 (étape facultative sur l'initiative du tiers archiveur)</i> .....	27
623. <i>TRAITEMENT 3 (sur l'initiative du tiers archiveur)</i> .....	28
624. <i>TRAITEMENT 4 (sur l'initiative du donneur d'ordre)</i> .....	28
<b>7. RELATIONS AVEC LES AUTRES TIERS</b> .....	<b>29</b>
71. RÔLE ET FONCTION DE CES AUTRES TIERS .....	29
711. <i>Le tiers horodateur</i> .....	29
712. <i>Le tiers certificateur</i> .....	29
713. <i>Autres tiers archiveurs</i> .....	29
72. CUMUL DES FONCTIONS .....	30
73. FIN DU CONTRAT OU CESSATION D'ACTIVITÉ DU TIERS .....	31

<b>8.</b>	<b>TRAITEMENTS CHEZ LE DONNEUR D'ORDRE ET LE TIERS ARCHIVEUR.....</b>	<b>33</b>
81.	TRAITEMENTS.....	33
811.	<i>Traitements de constitution des objets à archiver chez le donneur d'ordre.....</i>	33
812.	<i>Traitements d'acquisition d'archives chez le tiers archiveur.....</i>	33
82.	GESTION DES TABLES.....	33
83.	ORGANISATION DE LA PROFESSION DE TIERS ARCHIVEUR.....	34
831.	<i>Au niveau du tiers archiveur.....</i>	34
8311.	Rôle, fonctions et organisation.....	34
8312.	Obligations.....	34
8313.	Responsabilités.....	35
832.	<i>Au niveau de la profession de tiers archiveur.....</i>	36
8321.	Rôle, fonctions et organisation.....	36
8322.	Obligations.....	36
8323.	Responsabilités.....	36
8324.	Garanties.....	36
833.	<i>Au niveau du donneur d'ordre.....</i>	37
8331.	Rôle, fonctions et organisation.....	37
8332.	Obligations.....	37
8333.	Responsabilités.....	37
8334.	Garanties.....	37
84.	EXIGENCES JURIDIQUES PRÉALABLES.....	38
841.	<i>Exigences juridiques préalables au niveau de la profession de tiers archiveur.....</i>	38
	Code de bonne conduite des tiers archiveurs.....	39
842.	<i>Exigences juridiques préalables entre tiers archiveur et donneur d'ordre.....</i>	39
8421.	Clause "Objet/Description du service".....	39
8422.	Clause "Obligation du tiers archiveur".....	40
8423.	Clause "Obligation du donneur d'ordre".....	40
8424.	Clause "Responsabilité".....	40
8425.	Clause "Garanties".....	41
8426.	Clause "Réversibilité".....	41
8427.	Clause "Autorisations".....	41
8428.	Clause "Conditions financières".....	41
8429.	Clause "Durée".....	41
84210.	Clause "Convention sur la preuve".....	41
84211.	Clauses génériques.....	42
843.	<i>Exigences juridiques préalables au niveau du donneur d'ordre.....</i>	42
<b>9.</b>	<b>SERVICES AJOUTÉS PAR LES TIERS ARCHIVEURS.....</b>	<b>43</b>
	<b>ANNEXE 1 - RÉCAPITULATION DES CODES UTILISÉS.....</b>	<b>45</b>
	<b>ANNEXE 2 - GLOSSAIRE DES ABRÉVIATIONS.....</b>	<b>49</b>
	<b>ANNEXE 3 - GLOSSAIRE.....</b>	<b>51</b>
	<b>ANNEXE 4 - SCÉNARI D'ÉCHANGES.....</b>	<b>57</b>
	<b>ANNEXE 5 - BIBLIOGRAPHIE.....</b>	<b>61</b>
	<b>ANNEXE 6 – PRINCIPAUX TEXTES APPLICABLES AU 30 JUIN 2000.....</b>	<b>63</b>

## Préambule

La dématérialisation des documents introduit une dimension nouvelle dans la gestion des personnes morales en favorisant la communication, le classement et la recherche d'informations.

De plus, l'émergence de la signature électronique dans de nombreux pays, dont la France, donne une plus grande actualité aux travaux menés sur l'archivage électronique rendu nécessaire pour assurer la sécurité des messages électroniques, tant sur le plan technique que juridique.

Dans ce contexte, la réforme du droit français de la preuve était devenue indispensable pour que les entreprises et les particuliers puissent profiter pleinement des nouvelles technologies.

C'est aujourd'hui chose faite, celle-ci s'appréhende sous le double objectif de la modification des textes législatifs, donc du Code civil et de l'intégration de dispositions techniques innovantes.

Aujourd'hui, le support d'archivage de la preuve n'est plus obligatoirement un support papier mais aussi un support électronique, notamment, dès lors que ce support répond aux caractères de fidélité et de pérennité énoncés par le Code civil ainsi qu'aux exigences futures d'intégrité et d'imputabilité de la preuve. C'est pourquoi, sensibilisés au problème de la conservation des documents et à sa rentabilité économique, les professionnels ont recouru à d'autres méthodes telles que l'archivage électronique des documents.

Le remplacement des supports physiques traditionnels (papier ou microforme) ou la prise en compte de documents d'origine électronique dans une solution de gestion électronique des documents (GED) implique dorénavant, notamment lorsque les projets ont pour vocation un archivage "légal", le respect de certaines recommandations telles que celles contenues dans la norme Afnor NF Z42-013. Cette norme décrit de façon spécifique pour le domaine de la GED et particulièrement pour celui de l'archivage électronique les principes permettant de s'assurer que les systèmes sont bien conçus et que leur exploitation respecte des procédures répertoriées et sécurisées. La finalité de cette norme est donc d'assurer l'intégrité et la fidélité des documents électroniques, stockés ou restitués au travers des systèmes de GED ainsi que la pérennité de l'archivage dans le cadre de la durée de conservation souhaitée. Les recommandations qui en découlent sont d'ordre technique, procédural et organisationnel.

Dans son prolongement et dans une logique pratique respectant les principes de sécurité attachés à la preuve, le présent document a pour objet de permettre à toute entreprise ou aux prestataires spécialisés en matière d'archivage d'établir une politique d'archivage sur la base de scénarii et de bonnes pratiques dont les principes sont définis ci-après.

Il convient de rappeler ici que la définition d'une politique d'archivage nécessite une démarche préalable d'analyse du patrimoine documentaire de l'entreprise (son origine, son utilisation et sa destination dans l'entreprise), ainsi que des obligations légales en matière de conservation des documents. Ensuite, il s'agit de déterminer les supports et les modes d'archivage retenus, puis, en fonction du mode d'archivage choisi, les modalités de mise en œuvre d'un archivage en interne, c'est-à-dire au sein de l'entreprise émettrice du document, par la création d'un service spécialisé ou en externe par un prestataire spécialisé.

Les méthodes exposées dans le présent document ne peuvent être mises en œuvre de manière effective sans la réalisation de ces démarches préalables postérieures à une analyse du document ou de la donnée dès sa création.

La détermination de cette méthodologie a été réalisée suivant trois orientations distinctes relatives :

- la détermination du type de document à archiver,
- la détermination du type de preuve à fournir en fonction du document,
- l'identification du type d'archivage.

En outre, une vaste réflexion doit être menée relativement aux conditions contractuelles accompagnant la mise en œuvre de la politique d'archivage.

Il s'agit notamment d'envisager et d'aménager des relations contractuelles avec des tiers archiveurs, tiers certificateurs ou certificateurs de services de signatures électroniques en liaison avec la directive européenne du 13 décembre 1999 sur les signatures électroniques et avec les prochains décrets d'application de la réforme actuelle du droit de la preuve en France.

La mise en œuvre de cette politique permet de réaliser une politique active en matière d'archivage électronique, en s'assurant de la valeur légale des supports électroniques utilisés en termes de :

- contrôle d'intégrité,
- vérification de l'imputabilité du document,
- conservation dans le temps du support,
- accessibilité à la preuve et à son support.

## 1. Introduction

### 11. Finalités du guide d'archivage électronique sécurisé

Le présent guide a pour objet de proposer différents *scénarii* de communication lorsqu'une organisation fait appel aux services d'un tiers archiveur dans le cadre de la mise en œuvre d'un système d'archivage électronique garantissant l'intégrité, la pérennité et la restitution des messages. Les aspects relatifs à la conception et à l'exploitation des systèmes d'archivage électronique ne sont pas abordés.

Le contenu de ce guide permet à chaque entité concernée par l'archivage de données électroniques de compléter son information afin de définir sa propre *Politique d'Archivage*. La sécurité liée à cette politique d'archivage trouvera sa pleine efficacité au sein d'une structure de gestion, appelée *Infrastructure à clés publiques* (ICP), constituée par l'utilisateur lui-même, si la taille de son entité le lui permet, ou dans le cadre d'une communauté d'utilisateurs, en cas contraire.

Ainsi, la définition de la Politique d'Archivage sera consécutive à la détermination, au sein de l'ICP et selon les finalités poursuivies, de :

- une *Politique de Certification* (PC), portant sur la mise en œuvre de certificats électroniques et le recours à des Prestataires de Services de Certification (PSC) dont la pratique sera définie dans un document intitulé « Déclaration des Pratiques de Certification (DPC)<sup>1</sup> »,
- une *Politique de Signature* qui traitera du caractère qualifié ou non du certificat, de la nature avancée ou non de la signature, de la compatibilité des dispositifs de création de signature avec les dispositifs de vérification, de la fonction sécuritaire ou juridique de la signature, etc<sup>2</sup>,
- une *Politique de Confidentialité* par chiffrement des données, recourant aux fonctions d'une tierce partie de confiance et nécessitant la sécurisation du transport. Les méthodes de chiffrement peuvent faire appel à un ensemble clé privée/clé publique et donc, à un certificat,
- une *Politique d'Horodatation*, faisant intervenir des tiers horodateurs (Time Stamping Authority, protocole développé par l'IETF) et comportant l'utilisation de jeton temporel de format X.509.

### 12. Dimension juridique de l'archivage

En devenant *conservation*, l'archivage acquiert une dimension juridique. Il est, en effet, communément admis par les juristes que le terme d'"archivage" concerne le support utilisé et le terme de « conservation », les droits des parties.

---

1 « Certificat électronique » : une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne, d'après la Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

2 « Signature électronique » : une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification, d'après la Directive précitée.

Une modification récente du Code Civil français souligne, en vue de l'administration de la preuve, les exigences de conservation et d'intelligibilité de l'écrit, quels que soient son support et ses modalités de transmission.

Le nouvel article 1316-1 du Code Civil dispose ainsi *in fine* :

*« L'écrit sous forme électronique est admis en preuve au même titre 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. »*

Et le nouvel article 1316 :

*« La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission. »*

## **2. Notions sommaires de scénarii**

### **21. Composition des scénarii**

Un scénario d'archivage met en scène les objets suivants :

1. Des éléments électroniques à archiver,
2. Des acteurs,
3. Des protocoles d'échanges.

#### **211. Les éléments électroniques à archiver**

Les éléments à archiver sont constitués au minimum de messages électroniques ainsi que de leur signature électronique. On entend par message tout type de fichier informatique, notamment les fichiers de données sonores, graphiques ou multimédia, les programmes, les messages non structurés (mails ou messages X.400) ou les messages structurés (EDI, XML). Le certificat électronique doit également être archivé. Certaines autres informations accompagnant ces messages doivent également être archivées, d'autres ignorées.

#### **212. Les acteurs**

Deux catégories d'acteurs sont identifiées :

- L'émetteur d'un message et son destinataire, l'un et l'autre ou les deux, archivant le message en fin d'échange. Ces acteurs sont appelés "donneur d'ordre",
- Le "tiers archiveur", auquel le donneur d'ordre confie soit l'archive, soit la clé des archives.

Selon la taille de l'entité professionnelle du donneur d'ordre, le tiers archiveur peut être interne ou externe à cette entité.

#### **213. Les protocoles d'échanges**

Les protocoles d'échanges sont ainsi caractérisés :

- Deux protocoles sont utilisés dans le scénario : un protocole d'archivage (transmission des éléments à archiver du donneur d'ordre vers le tiers archiveur), un protocole de désarchivage ou de restitution (transmission des éléments désarchivés du tiers archiveur vers le donneur d'ordre).
- Les protocoles comprennent des données de services indispensables au donneur d'ordre et garantissant la neutralité du tiers archiveur.
- Les protocoles présentent des mesures de sécurité spécifiques aux échanges électroniques.

## **22. Typologie des scénarii**

- 1<sup>er</sup> scénario :  
Un donneur d'ordre (une entreprise, une administration ou toute autre entité) envisage de dépo-

ser ses archives électroniques (données, programmes, images, sons, etc.) chez un tiers archiveur afin que ce dernier les gère pour son compte.

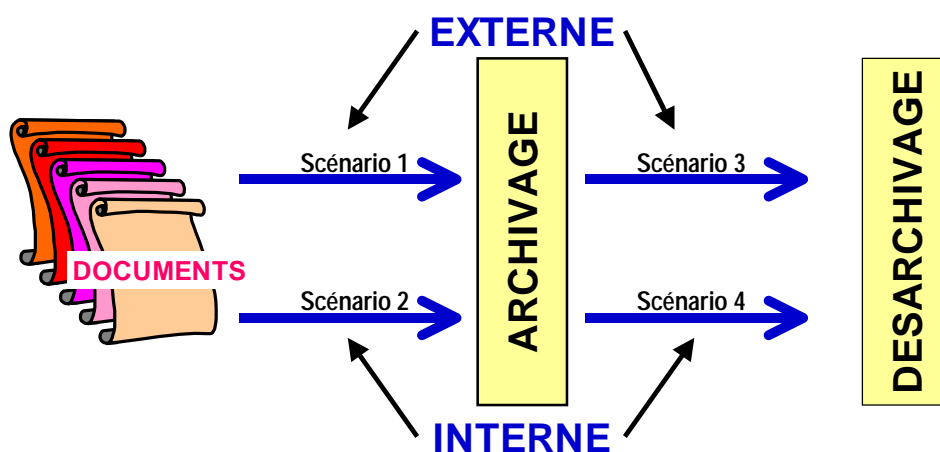
- 2<sup>e</sup> scénario :  
Le donneur d'ordre confie au tiers archiveur la clé des archives, à des fins probatoires ou de contrôle d'intégrité, et conserve l'archive elle-même dans ses propres services.
- 3<sup>e</sup> scénario :  
Les archives sont constamment à la disposition du donneur d'ordre, qui peut demander à tout moment au tiers archiveur de les lui restituer, pour des raisons de contrôle ou de preuve. Lorsque la restitution de l'archive est définitive, le donneur d'ordre peut demander au tiers archiveur de procéder à la destruction de l'archive.
- 4<sup>e</sup> scénario :  
Sur demande du donneur d'ordre, le tiers archiveur lui restitue la clé des archives.

Il n'a pas semblé utile dans le présent document de décrire dans le détail les données archivées et les services apportés.

Ainsi, quatre scénarii sont proposés :

1. Envoi des archives à un tiers archiveur,
2. Envoi d'une clé des archives à un tiers archiveur (les archives sont conservées par le donneur d'ordre),
3. Retour des archives au donneur d'ordre,
4. Retour d'une clé des archives au donneur d'ordre.

Ces quatre scénarii sont illustrés ci-après :



Dans le cas où un service ASP (Application Service Provider) est proposé par une société de services, afin de générer un moyen de preuve suffisant entre les deux cocontractants, le service de tiers archiveur ne peut être assuré que par un tiers indépendant du service ASP.

### 3. Objets à archiver & gestion des tables des archives

#### 31. Objets à archiver

Les objets à archiver sont constitués dans la présente étude uniquement de fichiers électroniques.

Un fichier électronique doit être compris comme un ensemble de données comprenant tout type de forme : texte, tableau, graphique, son, image, message, base de données, programme, certificat, etc. Dans la suite de l'étude, les éléments à archiver sont appelés *101\_lot\_fic*.

Remarques : Il a été décidé de ne pas procéder à l'archivage des CRL (liste de révocation des certificats), ces derniers étant sous la responsabilité des autorités qui les délivrent (ce sont donc ces derniers qui les archivent).

La confidentialité est assurée au départ chez le donneur d'ordre indépendamment du scénario.

#### 32. Gestion des tables des archives

##### 321. Gestion de la table des archives chez le donneur d'ordre

La table des archives chez le donneur d'ordre contient les informations suivantes (dans leur ordre d'arrivée) :

1. nom du tiers archiveur,
2. clé publique du tiers archiveur,
3. *101\_oen\_fic* : n° d'ordre d'envoi du fichier archivé chez le donneur d'ordre,
4. *101\_hen\_fic* : date d'envoi du fichier archivé chez le donneur d'ordre,
5. *101\_lot\_fic* : détail des identifiants des éléments constitutifs du fichier archivé,
6. *101\_sec\_fic* : sécurisation de transport lors de l'envoi par le donneur d'ordre,
7. *102\_ore\_lot* : n° d'ordre de réception du fichier par le tiers archiveur,
8. *102\_hre\_lot* : date de réception du fichier par le tiers archiveur,
9. *102\_sec\_are* (éventuellement) : sécurité transport du *102\_are\_blc* par le tiers archiveur,
10. *102\_scl\_ens* : sceau généré par le tiers archiveur pour le fichier archivé,
11. *201\_emp\_fic* : empreinte de l'élément à archiver *101\_lot\_fic*,
12. *201\_har\_fic* : date d'envoi du *101\_lot\_fic* donnée par le donneur d'ordre en interne,
13. *201\_hen\_fic* : date d'envoi du sceau du *101\_lot\_fic* donnée par le donneur d'ordre,
14. *201\_nar\_fic* : n° d'ordre interne d'envoi du *101\_lot\_fic* donné par le donneur d'ordre,
15. *201\_oen\_fic* : n° d'ordre d'envoi du sceau du *101\_lot\_fic* donné par le donneur d'ordre,
16. *201\_sec\_fic* : sécurité transport du sceau du *101\_ens\_lot* effectuée par le donneur d'ordre,
17. *202\_hre\_lot* : date de réception par le tiers archiveur du sceau de l'ensemble *101\_ens\_lot*,
18. *202\_ore\_lot* : n° d'ordre de réception par le tiers archiveur du sceau de l'ensemble *101\_ens\_lot*,
19. *202\_scc\_are* : sceau chiffré de l'empreinte *201\_emp\_fic*,
20. *301\_oen\_req* : n° d'ordre de la requête d'archives attribué par le donneur d'ordre,
21. *301\_hen\_req* : date de la requête d'archives chez le donneur d'ordre,
22. *301\_sec\_req* : sécurité de transport de la requête de demandes d'archives,
23. *303\_ore\_blc* : n° d'ordre de réponse à la demande du donneur d'ordre,
24. *303\_hre\_blc* : date de réponse à la demande du donneur d'ordre,

25. **401\_hen\_req** : date d'envoi de la requête d'empreinte par le donneur d'ordre,
26. **401\_oen\_req** : n° d'ordre de la requête d'empreinte par le donneur d'ordre,
27. **403\_hre\_blc** : date de la réponse de l'empreinte restituée donnée par le tiers archiveur,
28. **403\_ore\_blc** : n° d'ordre de l'empreinte restituée donné par le tiers archiveur,
29. **403\_res\_blc** : empreinte restituée par le tiers archiveur.

## 322. Gestion de la table des archives chez le tiers archiveur

La table des archives chez le tiers archiveur contient les informations suivantes (dans leur ordre d'arrivée) :

1. nom (ou code) du donneur d'ordre,
2. clé publique du donneur d'ordre,
3. **102\_ore\_lot** : n° d'ordre de réception du fichier par le tiers archiveur,
4. **102\_hre\_lot** : date de réception du fichier par le tiers archiveur,
5. **101\_ens\_lot** : ensemble du lot archivé,
6. **102\_scl\_ens** : sceau généré par le tiers archiveur sur le fichier archivé,
7. **202\_cpu\_are** : clé publique du tiers archiveur,
8. **202\_hre\_lot** : date de réception par le tiers archiveur du sceau de l'ensemble **101\_ens\_lot**,
9. **202\_ore\_lot** : n° d'ordre de réception par le tiers archiveur du sceau de l'ensemble **101\_ens\_lot**,
10. **202\_scc\_are** : sceau chiffré de l'empreinte **201\_emp\_fic**,
11. **202\_sec\_are** : sécurité transport du **202\_are\_blc** effectuée par le tiers archiveur,
12. **301\_oen\_req** : n° d'ordre d'envoi de la requête du donneur d'ordre,
13. **302\_ore\_req** : n° d'ordre de réception de la requête du donneur d'ordre,
14. **302\_hre\_req** : date de réception de la requête du donneur d'ordre,
15. **301\_dde\_req** : demande d'archives du donneur d'ordre,
16. **401\_dde\_req** : demande d'empreinte effectuée par le donneur d'ordre,
17. **402\_hre\_req** : date de la réponse à la requête **401\_dde\_req** donnée par le tiers archiveur,
18. **401\_oen\_req** : n° d'ordre de la requête d'empreinte par le donneur d'ordre,
19. **402\_ore\_req** : n° d'ordre de la réponse à la requête **401\_dde\_req** donné par le tiers archiveur,
20. **303\_res\_blc** : archives restituées,
21. **303\_ore\_blc** : n° d'ordre de réponse à la demande du donneur d'ordre,
22. **303\_hre\_blc** : date de réponse à la demande du donneur d'ordre,
23. **303\_sec\_blc** : sécurité transport de la réponse à la demande d'archives,
24. **304\_are\_blc** : accusé de réception des archives demandées,
25. **305\_ore\_blc** : n° d'ordre de communication/restitution des archives demandées,
26. **305\_hre\_blc** : date de communication/restitution des archives demandées,
27. **403\_hre\_blc** : date de la réponse de l'empreinte restituée donnée par le tiers archiveur,
28. **403\_ore\_blc** : n° d'ordre de l'empreinte restituée donné par le tiers archiveur,
29. **403\_res\_blc** : empreinte restituée par le tiers archiveur,
30. **403\_sec\_blc** : sécurité transport de la réponse à la demande d'empreinte.

En annexe 3, figure une table de gestion des archives qui reprend les étapes de traitement avec une répartition des fonctions entre donneur d'ordre et tiers archiveur.

## 4. Présentation du modèle

Pour l'ensemble des modèles, un format générique est adopté qui se présente comme suit :

Action	Données de service	Données	Sécurité
--------	--------------------	---------	----------

Les données de service ne sont jamais chiffrées.

La variable *var\_iab* générée lors du traitement *yy* dans le scénario *X* est représentée comme suit dans le présent document : *Xyy\_var\_iab*. La signification de la variable est la suivante :

- les trois premières lettres alphabétiques (*var*) désignent la sémantique associée à la variable : heure/date d'envoi (*hen*), heure/date de réception (*hre*), etc.,
- les trois suivantes, l'élément sur lequel s'applique cette variable : fichier (*fic*), lot (*lot*), bloc (*blc*), etc. L'annexe 1 (Récapitulation des codes utilisés) indique la valeur de chacune des codifications alphabétiques en usage dans le présent document.

Exemple : *102\_hre\_lot*, variable générée lors du traitement *02* du scénario *1* donc chez le tiers archiveur. Elle précise l'heure et la date de réception (*hre*) du lot entrant (*lot*).

L'opération n° *z* effectuée lors du traitement *yy* dans le scénario *X* sera numérotée comme suit : *X.yy.z* : exemple, *1.2.b* est l'opération n° *b* effectuée lors du traitement *02* du scénario *1*.



## 5. Les archives sont confiées à un tiers archiveur

### 51. Scénario I : télétransmission des archives

Le scénario I décrit l'opération suivante : un donneur d'ordre télétransmet des archives à un tiers archiveur.

Tout fichier électronique doit être transmis au tiers archiveur dans les conditions optimales de sécurité. En particulier, l'authentification et l'intégrité des fichiers formant un lot à archiver doivent être garanties par une sécurisation électronique.

Action	Données de service	Données	Sécurité
<b>TRAITEMENT 1 (chez le donneur d'ordre) - voir ci-dessous</b>			
Envoi d'un lot à archiver <b>101_ens_lot</b>	N° d'ordre envoi <b>101_oen_fic</b> Date d'envoi <b>101_hen_fic</b>	Eléments à archiver ( <b>101_lot_fic</b> )	Sécurité transport (intégrité) <b>101_sec_fic</b>
<b>TRAITEMENT 2 (chez le tiers archiveur) - voir ci-dessous</b>			
Envoi d'un accusé de réception <b>102_are_blc</b>	N° d'ordre envoi <b>101_oen_fic</b> N° d'ordre réception <b>102_ore_lot</b> Date de réception <b>102_hre_lot</b>	Sceau <b>102_scl_ens</b> de : <b>101_ens_lot</b> - n° d'ordre réception <b>102_ore_lot</b> - date de réception <b>102_hre_lot</b>	Sécurité transport (intégrité) <b>102_sec_are</b>
<b>TRAITEMENT 3 (chez le donneur d'ordre) - voir ci-dessous</b>			
Contrôle d'intégrité		Destruction ensemble archivé <b>101_lot_fic</b> Destruction Sécurité transport <b>102_sec_are</b>	

Les sécurisations électroniques (**101\_sec\_fic** / **102\_sec\_are**) utilisées pour la transmission des blocs dans les échanges donneur d'ordre / tiers archiveur distant (en effet, les sécurisations **101\_sec\_fic** et **102\_sec\_are** sont utilisées dans un sens pour la première et dans l'autre pour la seconde) respectent les procédures et protocoles habituels des sécurisations électroniques, en particulier sur la nécessité d'un certificat électronique.

Il est rappelé que, lors de la conclusion du contrat qui lie le donneur d'ordre au tiers archiveur, ce dernier lui communique une clé publique.

#### 511. TRAITEMENT 1 (sur l'initiative du donneur d'ordre)

Cette phase de traitement concerne la préparation du lot à archiver.

Il s'agit de procéder à l'archivage des fichiers électroniques chez un tiers archiveur distant. Il convient de prendre en considération :

- que l'émetteur se trouve face à de nombreux fichiers à archiver et qu'il doit gérer globalement son archivage (**101\_lot\_fic**),
- que certaines législations peuvent lui imposer un système de contrôle ou de suivi de l'archivage (ex.: la législation sur la dématérialisation de la facture impose pour l'échange électronique de ces documents une liste récapitulative et un fichier des partenaires),

- qu'en matière de gestion des archives, il convient de dater les envois de fichiers vers le tiers archiveur *101\_hen\_fic* et de les numéroter *101\_oen\_fic*.

Cet ensemble d'informations prend pour nom *101\_ens\_lot* (*101\_oen\_fic*, *101\_hen\_fic*, *101\_lot\_fic*, *101\_sec\_fic*).

Il convient de préciser par ailleurs, qu'en matière de gestion des archives, le donneur d'ordre doit créer (ou mettre à jour) une table de gestion des archives et de gérer les liens qui seraient nécessaires entre fichiers (message et certificat par exemple). C'est à cette occasion qu'il met à jour cette table des renseignements suivants : *101\_oen\_fic*, *101\_hen\_fic*, *101\_lot\_fic*, *101\_sec\_fic*, nom et clé publique du tiers archiveur.

Les opérations suivantes sont donc effectuées :

I.1.a Constitution de l'ensemble du lot *101\_ens\_lot*

I.1.b Transmission par le donneur d'ordre au tiers archiveur de l'ensemble *101\_ens\_lot* comprenant : *101\_oen\_fic*, *101\_hen\_fic*, *101\_lot\_fic*, *101\_sec\_fic*

I.1.c Mise à jour, par le donneur d'ordre, de sa table des archives avec *101\_oen\_fic*, *101\_hen\_fic*, *101\_lot\_fic*, *101\_sec\_fic*

Le niveau de sécurité voulu déterminera le type d'horodatage : horodatage interne, horodatage effectué par un tiers horodateur qui peut être différent le cas échéant du tiers archiveur.

## **512. TRAITEMENT 2 (sur l'initiative du tiers archiveur)**

Le tiers archiveur considère l'ensemble du lot (*101\_ens\_lot*) comme un tout homogène dont il est posé comme principe qu'il n'a pas une connaissance totale du contenu.

Lorsque le tiers archiveur reçoit l'ensemble du lot (*101\_ens\_lot*) de l'émetteur, il doit :

- affecter son propre numéro d'ordre à l'ensemble entrant *102\_ore\_lot*,
- dater l'ensemble entrant *102\_hre\_lot*.

Pour des besoins inhérents à la sécurité interne de son site et pour fournir un accusé de réception à son client, le tiers archiveur est amené à signer lui-même à la fois l'ensemble du lot (*101\_ens\_lot*), son n° d'ordre de réception (*102\_ore\_lot*) et sa date de réception (*102\_hre\_lot*) pour obtenir un sceau appelé *102\_scl\_ens*. Le scellement ainsi effectué ou le sceau ainsi calculé a pour but de garantir l'intégrité des données archivées. Il ne concerne pas l'intégrité des données au cours du transport des données.

Les opérations suivantes se succèdent :

I.2.a Contrôle d'intégrité au moyen de la sécurité de transport *101\_sec\_fic* sur l'ensemble télétransmis *101\_ens\_lot* : la sécurité *101\_sec\_fic* est conservée avec l'ensemble télétransmis *101\_ens\_lot* afin de ménager un contrôle ultérieur

I.2.b Affectation du n° d'ordre réception *102\_ore\_lot*

I.2.c Ajout de la date de réception *102\_hre\_lot*

I.2.d Scellement pour obtenir un sceau appelé *102\_scl\_ens* : ce sceau est envoyé avec l'accusé de réception ; il sert également au tiers archiveur dans un but de vérification lorsqu'il régénère ses fichiers dans la gestion de ses archives électroniques

I.2.e Mise à jour de la table de gestion des archives détenues par le tiers archiveur du *102\_arc\_blc* à archiver (*102\_ore\_lot*, *102\_hre\_lot*, *101\_ens\_lot*, *102\_scl\_ens*)

I.2.f Archivage du *102\_arc\_blc*

I.2.g Transmission d'un accusé de réception (*102\_are\_blc*) au donneur d'ordre comprenant le numéro d'ordre d'envoi initial (*101\_oen\_fic*), le n° d'ordre de réception (*102\_ore\_lot*), la date de réception (*102\_hre\_lot*), le sceau (*102\_scl\_ens*) et la sécurité transport (*102\_sec\_are*)

Les opérations I.2.a à c permettent de mettre à jour le "registre" des entrées-sorties des fichiers archivés par le tiers archiveur.

Le tiers archiveur doit accuser réception à l'émetteur de son message. L'accusé de réception *102\_are\_blc* n'est pas que formel, il se réfère également à une "image" du bloc qui a été réellement archivé. Le donneur d'ordre est ainsi en mesure, à la réception de l'accusé de réception, de vérifier ce qui est réellement archivé.

L'"image" du bloc n'a cependant pas besoin de se présenter comme une reproduction intégrale de ce bloc. Un condensé (ou sceau) signé permet de vérifier l'authentification du tiers archiveur et l'intégrité du bloc.

Le niveau de sécurité voulu déterminera le type d'horodatage : horodatage interne, horodatage effectué par un tiers horodateur qui peut être différent le cas échéant du tiers archiveur.

### 513. TRAITEMENT 3 (sur l'initiative du donneur d'ordre)

Pour se résumer, les opérations suivantes se succèdent :

I.3.a Contrôle d'intégrité au moyen de la sécurité de transport *102\_sec\_are* sur l'accusé de réception *102\_are\_blc*

I.3.b Vérification éventuelle de la concordance entre les informations de l'accusé de réception *102\_are\_blc* et les éléments à archiver *101\_lot\_fic* : recalcul du sceau *102\_scl\_ens* à l'aide de certains renseignements figurant en clair dans l'accusé de réception *102\_are\_blc* (n° d'ordre de réception *102\_ore\_lot* et date de réception *102\_hre\_lot*) et de l'ensemble à archiver *101\_ens\_lot* toujours détenu par le donneur d'ordre

I.3.c Mise à jour de la table de gestion des archives avec les renseignements suivants : sceau *102\_scl\_ens*, n° d'ordre et date de réception (*102\_ore\_lot* et *102\_hre\_lot*)

I.3.d En cas de concordance, destruction éventuelle de l'ensemble archivé (*101\_lot\_fic*)

I.3.e En cas de concordance, sauf besoin particulier ou permanent de vérification, destruction éventuelle des éléments de sécurité de transport *102\_sec\_are*.

### 52. Scénario III : télétransmission des demandes d'archives

Action	Données de service	Données	Sécurité
TRAITEMENT 1 (chez le donneur d'ordre) – voir ci-dessous			
Demande de restitution des archives <i>301_dde_req</i>	N° d'ordre envoi <i>301_oen_req</i> Date d'envoi de la requête <i>301_hen_req</i>	“ REQUETE ” : n° d'ordre envoi des archives <i>101_oen_fic</i> ou n° d'ordre archiveur <i>102_ore_lot</i>	Sécurité transport (intégrité) <i>301_sec_req</i>
TRAITEMENT 2 (chez le tiers archiveur) - voir ci-dessous			
Envoi d'un accusé de	N° d'ordre envoi	délai estimé	Sécurité transport

réception de la requête <b>302_are_req</b>	N° d'ordre réception <b>301_oen_req</b> Date de réception <b>302_ore_req</b> <b>302_hre_req</b>		(intégrité) <b>302_sec_are</b>
<b>TRAITEMENT 3 (chez le tiers archiveur) - voir ci-dessous</b>			
Archives restituées <b>303_res_blc</b>	N° d'ordre envoi <b>301_oen_req</b> N° d'ordre réponse <b>303_ore_blc</b> Date de réponse <b>303_hre_blc</b>	bloc envoi <b>102_arc_blc</b>	Sécurité transport (intégrité) <b>303_sec_blc</b>
<b>TRAITEMENT 4 (chez le donneur d'ordre) - voir ci-dessous</b>			
Vérification de la concordance des archives Transmission d'un accusé de réception <b>304_are_blc</b>	N° d'ordre envoi <b>301_oen_req</b> N° d'ordre réponse <b>304_ore_blc</b> Date de réponse <b>304_hre_blc</b>	indication du type de demande : communication ou restitution	Sécurité transport (intégrité) <b>304_sec_blc</b>
<b>TRAITEMENT 5 (chez le tiers archiveur) - voir ci-dessous</b>			
Mise à jour de la table Destruction archives	Date communication ou destruction <b>304_are_blc</b> N° d'ordre communication / destruction <b>305_ore_blc</b> Date communication / destruction <b>305_hre_blc</b>		

## 521. TRAITEMENT 1 (sur l'initiative du donneur d'ordre)

Le donneur d'ordre prépare une demande d'archives pouvant être aussi bien une demande de communication (pour consultation ou vérification d'une clé par exemple) qu'une demande de restitution. Dans ce dernier cas, le tiers archiveur peut être amené à détruire, suivant l'accord contractuel, les archives qu'il détenait pour le compte du donneur d'ordre.

III.1.a Le donneur d'ordre prépare sa demande d'archives (**301\_dde\_req**) en y précisant soit le n° d'ordre d'envoi (**101\_oen\_fic**), soit le n° d'ordre de réception du fichier (**102\_ore\_lot**).

III.1.b Ensuite, il y a transmission de la requête (**301\_dde\_req**) avec une sécurité de transport (**301\_sec\_req**).

III.1.c Il est également procédé à la mise à jour de la table des archives en y indiquant le n° d'ordre de la requête (**301\_oen\_req**) et la date de la demande (**301\_hen\_req**).

Le niveau de sécurité voulu déterminera le type d'horodatage : horodatage interne, horodatage effectué par un tiers horodateur qui peut être différent le cas échéant du tiers archiveur.

## 522. TRAITEMENT 2 (étape facultative sur l'initiative du tiers archiveur)

Les opérations suivantes se succèdent :

- III.2.a Contrôle d'intégrité au moyen de la sécurité de transport *301\_sec\_req* sur l'ensemble télétransmis *301\_dde\_req* : la sécurité *301\_sec\_req* est conservée avec l'ensemble télétransmis *301\_dde\_req* afin de ménager un contrôle ultérieur
- III.2.b Affectation du n° d'ordre réception *302\_ore\_req*
- III.2.c Ajout de la date de réception *302\_hre\_req*
- III.2.d Mise à jour de la table de gestion des archives détenues par le tiers archiveur des requêtes *301\_req* (*301\_oen\_req*, *302\_ore\_req*, *302\_hre\_req*, *301\_dde\_req*)
- III.2.e Estimation du délai de restitution
- III.2.f Transmission d'un accusé de réception (*302\_are\_req*) au donneur d'ordre comprenant le numéro d'ordre d'envoi initial (*301\_oen\_req*), le n° d'ordre de réception (*302\_ore\_req*), la date de réception (*302\_hre\_req*), le délai estimé pour la demande et la sécurité transport (*302\_sec\_are*)

Le niveau de sécurité voulu déterminera le type d'horodatage : horodatage interne, horodatage effectué par un tiers horodateur qui peut être différent le cas échéant du tiers archiveur.

### **523. TRAITEMENT 3 (sur l'initiative du tiers archiveur)**

Après l'envoi de l'accusé de réception *302\_are\_req*, le tiers archiveur procède aux opérations suivantes :

- III.3.a Extraction, vérification préalable de la qualité des fichiers et constitution du bloc à émettre *102\_arc\_blc* à l'exception du sceau *102\_scl\_ens*
- III.3.b Affectation du n° d'ordre réponse *303\_ore\_blc*
- III.3.c Ajout de la date de réponse *303\_hre\_blc*
- III.3.d Sécurisation du transport (*303\_sec\_blc*)
- III.3.e Mise à jour de la table de gestion des archives détenues par le tiers archiveur de l'envoi *303\_res\_blc* et des renseignements suivants : *303\_ore\_blc*, *303\_hre\_blc*, *303\_sec\_blc*

Le niveau de sécurité voulu déterminera le type d'horodatage : horodatage interne, horodatage effectué par un tiers horodateur qui peut être différent le cas échéant du tiers archiveur.

### **524. TRAITEMENT 4 (sur l'initiative du donneur d'ordre)**

Pour se résumer, les opérations suivantes se succèdent :

- III.4.a Contrôle d'intégrité de la sécurité de transport *303\_sec\_blc* sur les archives restituées *303\_res\_blc*
- III.4.b Vérification éventuelle de la concordance entre les informations des archives restituées *303\_res\_blc* et les éléments conservés par le donneur d'ordre : rapprochement des données (dates d'envoi et de réception, heures d'envoi et de réception, sceaux) et recalcul du sceau *102\_scl\_ens* à l'aide des renseignements figurant dans la table de gestion des archives du donneur d'ordre, notamment n° d'ordre de réception *102\_ore\_lot*, date de réception *102\_hre\_lot* et de l'ensemble à archiver *101\_ens\_lot* transmis au donneur d'ordre par le tiers archiveur,
- III.4.c Mise à jour de la table de gestion des archives avec les renseignements suivants : n° d'ordre et date de réponse (*303\_ore\_blc* et *303\_hre\_blc*)
- III.4.d En cas de concordance exacte, destruction éventuelle de la sécurité transport (*303\_sec\_blc*)
- III.4.e Transmission d'un accusé de réception (*304\_are\_blc*) au tiers archiveur comprenant le numéro d'ordre (*301\_oen\_req*), le n° d'ordre de réception (*304\_ore\_blc*) et la sécurité de

transport (*304\_sec\_are*), la date de réception (*304\_hre\_blc*). Cet accusé de réception précise s'il s'agit d'une communication ou d'une restitution.

## **525. TRAITEMENT 5 (sur l'initiative du tiers archiveur)**

Les opérations suivantes se succèdent :

- III.5.a Contrôle d'intégrité du transport (*304\_sec\_are*)
- III.5.b Destruction des archives (*101\_ens\_lot*) par le tiers archiveur selon l'indication du type de demande formulée par le donneur d'ordre,
- III.5.c Mise à jour de la table de gestion des archives soit après communication, soit après destruction des archives, (*304\_are\_blc*, *305\_ore\_blc* et *305\_hre\_blc*). Le tiers archiveur n'envoie pas de certificat de destruction.

## 6. Les archives restent confiées au donneur d'ordre

**Objectif :** Les archives sont conservées par l'entreprise. Elles peuvent être conservées et consultées par une ou plusieurs entités (personnes, services) . De plus, lors de la consultation, la vérification qui doit être possible est le test d'intégrité des fichiers. La politique de gestion des archives détermine le besoin de vérification de l'intégrité.

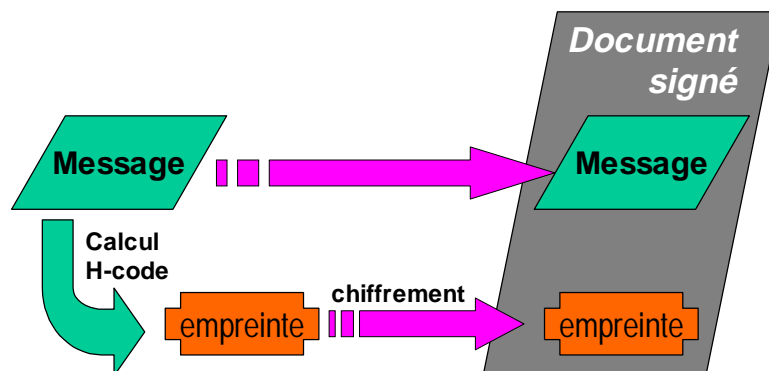
Le principe qui a prévalu aux scénarii I et III est reconduit dans les scénarii II et IV :

- les données sont archivées, personne ne doit pouvoir, dans un but probatoire, en modifier le contenu,
- le sceau chiffré des archives est envoyé au tiers archiveur assurant de ce fait un blocage de l'état des fichiers.

Comme dans les scénarii du chapitre 4 : chaque partie effectue sa gestion des documents grâce à une table de contrôle.

Le présent chapitre détermine les actions et procédures pour effectuer un "bon archivage".

Remarque préliminaire : empreinte – sceau



Une empreinte est une chaîne de caractères représentative d'un message, calculée par un algorithme de scellement du type "H-code". L'empreinte permet de garantir l'intégrité du message.

Une empreinte qui fait l'objet d'un chiffrement permet de garantir outre l'intégrité, l'authentification du donneur d'ordre.

Du fait de la conservation des archives en interne, les fichiers restent accessibles aux divers services. Il faut donc prévoir un mécanisme permettant de prouver à tout moment la correspondance entre le fichier restitué et le fichier au moment de l'archivage. On trouve ici un autre aspect du contrôle d'intégrité. Pour obtenir une assurance de la validité de ce contrôle, on fait appel à un tiers archiveur qui conserve les sceaux chiffrés associés aux fichiers.

Si ce sceau chiffré est également présent dans l'entreprise, tout service habilité peut à tout moment effectuer un contrôle d'intégrité. Et, en cas de contrôle administratif, le recours au sceau chiffré conservé chez le tiers archiveur permet d'assurer la validité du contrôle d'intégrité. De plus, tout accès au sceau chiffré du tiers archiveur entraîne une trace dans les tables de gestion et permet donc un suivi, un historique. En revanche, si le sceau chiffré est également présent dans l'entreprise, il n'y aura aucune trace chez le tiers archiveur lors des contrôles d'intégrité effectués en interne.

Cette opération de tiers archivage des clés est validant en cas de preuve car aucune des parties ne peut modifier ce qu'il possède sans détruire la réciprocité (la réplique) des documents.

## 61. Scénario II : télétransmission du sceau des archives (du moyen de contrôle de l'intégrité des archives)

Le scénario II décrit l'opération suivante : un donneur d'ordre (une entreprise ou un cabinet) télétransmet les sceaux de ses archives nouvelles à un tiers archiveur.

La clé est attachée soit à un lot de fichiers, soit à un seul fichier suivant le mode d'organisation prévu par le donneur d'ordre.

Action	Données de service	Données	Sécurité
TRAITEMENT 1 (chez le donneur d'ordre) - voir ci-dessous			
Envoi d'une empreinte à archiver <b>201_ens_lot</b>	N° d'ordre envoi <b>201_oen_fic</b>	Eléments à archiver ( <b>201_emp_fic</b> )	Sécurité transport (intégrité) <b>201_sec_fic</b>
	Date d'envoi <b>201_hen_fic</b>		
Envoi d'un lot à archiver en interne <b>201_don_blc</b>	N° d'ordre envoi interne <b>201_nar_fic</b>	Eléments à archiver ( <b>101_lot_fic</b> )	
	Date d'envoi <b>201_har_fic</b>		
TRAITEMENT 2 (chez le tiers archiveur) - voir ci-dessous			
Envoi d'un accusé de réception <b>202_are_blc</b>	N° d'ordre envoi <b>201_oen_fic</b>	Sceau chiffré <b>202_scc_are</b> de : <b>201_emp_fic</b> Clé publique : <b>202_cpu_are</b>	Sécurité transport (intégrité) <b>202_sec_are</b>
	N° d'ordre réception <b>202_ore_lot</b>		
	Date de réception <b>202_hre_lot</b>		
TRAITEMENT 3 (chez le donneur d'ordre) - voir ci-dessous			
Vérification de la concordance des sceaux chiffrés			

### 611. TRAITEMENT 1 (sur l'initiative du donneur d'ordre)

Cette phase de traitement concerne la préparation du lot à archiver.

II.1.a Il s'agit de procéder à l'archivage des fichiers électroniques en interne et de transmettre chez un tiers archiveur un élément permettant lors des "désarchivages" de contrôler l'intégrité des données. Il convient de prendre en considération :

- l'émetteur se trouve face à de nombreux fichiers à archiver et qu'il doit gérer globalement son archivage (**101\_lot\_fic**),
- certaines législations peuvent lui imposer un système de contrôle ou de suivi de l'archivage (ex.: la législation sur la dématérialisation de la facture impose pour l'échange électronique de ces documents une liste récapitulative et un fichier des partenaires),

- en matière de gestion des archives, il convient de dater les envois de fichiers vers le service interne d'archivage *201\_har\_fic* et de les numéroter *201\_nar\_fic*.

Cet ensemble d'informations prend pour nom *201\_don\_blc* (*201\_har\_fic*, *201\_nar\_fic*, *101\_lot\_fic*) (C'est le bloc qui reste chez le donneur d'ordre).

II.1.b Il faut également préparer l'envoi vers le tiers archiveur. Il suffit d'envoyer l'empreinte de *101\_lot\_fic* (*201\_emp\_fic*).

Cet ensemble d'informations prend pour nom *201\_ens\_lot* (*201\_oen\_fic*, *201\_hen\_fic*, *201\_emp\_fic*, *201\_sec\_fic*).

Il convient de préciser par ailleurs, qu'en matière de gestion des archives, le donneur d'ordre doit créer (ou mettre à jour) une table de gestion des archives et de gérer les liens qui seraient nécessaires entre fichiers (message et certificat par exemple). C'est à cette occasion qu'il met à jour cette table.

Le niveau de sécurité voulu déterminera le type d'horodatage : horodatage interne, horodatage effectué par un tiers horodateur qui peut être différent le cas échéant du tiers archiveur. Toutefois, l'indépendance des acteurs (tiers archiveur et donneur d'ordre) et la concordance normale des horodatations (envoi/réception) peuvent permettre de ne pas avoir recours à un tiers horodateur.

## 612. TRAITEMENT 2 (sur l'initiative du tiers archiveur)

Lorsque le tiers archiveur reçoit l'ensemble du lot (*201\_ens\_lot*) du donneur d'ordre, il doit :

- affecter son propre numéro d'ordre à l'ensemble entrant *202\_ore\_lot*,
- dater l'ensemble entrant *202\_hre\_lot*.

Pour fournir un accusé de réception à son client et permettre un contrôle a posteriori, le tiers archiveur est amené à chiffrer l'empreinte avec sa clé privée pour obtenir un sceau chiffré appelé *202\_scc\_are*.

Les opérations suivantes se succèdent :

- II.2.a Contrôle d'intégrité de la sécurité de transport *201\_sec\_fic* sur l'ensemble télétransmis *201\_ens\_lot* : la sécurité *201\_sec\_fic* est conservée avec l'ensemble télétransmis *201\_ens\_lot* afin de ménager un contrôle ultérieur,
- II.2.b Affectation du n° d'ordre réception *202\_ore\_lot*,
- II.2.c Ajout de la date de réception *202\_hre\_lot*,
- II.2.d Chiffrement du sceau appelé *202\_scc\_are* : ce sceau chiffré sera envoyé en II.2.g dans l'accusé de réception accompagné de la clé publique tiers archiveur (*202\_cpu\_are*),
- II.2.e Mise à jour de la table de gestion des archives détenues par le tiers archiveur du *202\_arc\_blc* à archiver (*202\_ore\_lot*, *202\_hre\_lot*, *202\_cpu\_are*, *202\_scc\_are*),
- II.2.f Archivage du *202\_arc\_blc*,
- II.2.g Transmission d'un accusé de réception (*202\_are\_blc*) au donneur d'ordre comprenant le numéro d'ordre d'envoi initial (*201\_oen\_fic*), le n° d'ordre de réception (*202\_ore\_lot*), la date de réception (*202\_hre\_lot*), le sceau chiffré (*202\_scc\_are*), la clé publique (*202\_cpu\_are*) et la sécurité transport (*202\_sec\_are*),
- II.2.h Destruction de l'empreinte (*201\_emp\_fic*).

Les opérations II.2.b et II.2.c permettent de mettre à jour la table des entrées-sorties des fichiers ar-

chivés par le tiers archiveur.

### 613. TRAITEMENT 3 (sur l'initiative du donneur d'ordre)

Pour se résumer, les opérations suivantes se succèdent :

- II.3.a Contrôle d'intégrité de la sécurité de transport *202\_sec\_are* sur l'accusé de réception *202\_are\_blc*,
- II.3.b Vérification éventuelle de la concordance entre les informations de l'accusé de réception : déchiffrement du sceau chiffré (*202\_scc\_are*) avec la clé publique du tiers archiveur (*202\_cpu\_are*). Comparaison entre l'empreinte issue du déchiffrement (*201\_emp\_fic'*) et celle recalculée de l'archive (*201\_emp\_fic*), le fichier x' est destiné à être identique à x,
- II.3.c Mise à jour de la table de gestion des archives avec les renseignements suivants : sceau chiffré *202\_scc\_are*, n° d'ordre et date de réception (*202\_ore\_lot* et *202\_hre\_lot*),
- II.3.d En cas de concordance, sauf besoin particulier ou permanent de vérification, destruction éventuelle des éléments de sécurité de transport *202\_sec\_are*.

Remarques :

- a) Le donneur d'ordre doit conserver et mettre à disposition la clé publique du tiers archiveur,
- b) Si le donneur d'ordre archive le sceau chiffré, les divers utilisateurs peuvent vérifier à tout moment l'intégrité des archives, mais il n'y a aucun moyen de contrôle opposable de traçabilité,
- c) Si le donneur d'ordre archive le sceau chiffré, pour vérifier l'intégrité et assurer l'opposabilité de la traçabilité des opérations, il demande le sceau chiffré correspondant au tiers archiveur, et compare les sceaux chiffrés,
- d) Si le donneur d'ordre ne conserve pas le sceau chiffré, chaque fois qu'il veut vérifier l'intégrité des données, il fait la demande du sceau chiffré au tiers archiveur et procède à la vérification en :
  - calculant l'empreinte de l'archive,
  - déchiffrant le sceau chiffré avec la clé publique,
  - en comparant les deux empreintes obtenues.

### 62. Scénario IV : restitution du sceau chiffré des archives

Le scénario IV décrit l'opération suivante : un donneur d'ordre (une entreprise ou un cabinet) désire vérifier l'intégrité de ses archives et demande le sceau chiffré correspondant.

Action	Données de service	Données	Sécurité
<b>TRAITEMENT 1 (chez le donneur d'ordre) – voir ci-dessous</b>			
Demande de restitution des archives <i>401_dde_req</i>	N° d'ordre envoi <i>401_oen_req</i> Date d'envoi de la requête <i>401_hen_req</i>	“ REQUETE ” : n° d'ordre envoi des archives <i>201_oen_fic</i> ou n° d'ordre archiveur <i>202_ore_lot</i>	Sécurité transport (intégrité) <i>401_sec_req</i>
<b>TRAITEMENT 2 (chez le tiers archiveur ) - voir ci-dessous</b>			
Envoi d'un accusé de réception de la requête <i>402_are_req</i>	N° d'ordre envoi <i>401_oen_req</i> N° d'ordre réception <i>402_ore_req</i>	délai estimé	Sécurité transport (intégrité) <i>402_sec_are</i>

	Date de réception <b>402_hre_req</b>		
<b>TRAITEMENT 3 (chez le tiers archiveur) - voir ci-dessous</b>			
Restitution du sceau chiffré <b>403_res_blc</b>	N° d'ordre envoi <b>401_oen_req</b> N° d'ordre réponse <b>403_ore_blc</b> Date de réponse <b>403_hre_blc</b>	bloc envoi <b>202_arc_blc</b>	Sécurité transport (intégrité) <b>403_sec_blc</b>
<b>TRAITEMENT 4 (chez le donneur d'ordre) - voir ci-dessous</b>			
Vérification de la concordance des sceaux			

## 621. TRAITEMENT 1 (sur l'initiative du donneur d'ordre)

Les opérations suivantes se succèdent :

- IV.1.a Préparation de la demande de restitution (**401\_dde\_req**) par le donneur d'ordre en y rappelant soit le n° d'ordre d'envoi (**201\_oen\_fic**), soit le n° d'ordre de réception du fichier (**202\_ore\_lot**),
- IV.1.b Transmission de la requête (**401\_dde\_req**) avec une sécurité de transport (**401\_sec\_req**),
- IV.1.c Mise à jour de la table des archives en y indiquant le n° d'ordre de la requête (**401\_oen\_req**) et la date de la demande (**401\_hen\_req**).

Le niveau de sécurité voulu déterminera le type d'horodatage : horodatage interne, horodatage effectué par un tiers horodateur qui peut être différent le cas échéant du tiers archiveur.

## 622. TRAITEMENT 2 (étape facultative sur l'initiative du tiers archiveur)

Les opérations suivantes se succèdent :

- IV.2.a Contrôle d'intégrité de la sécurité de transport **401\_sec\_req** sur l'ensemble télétransmis **401\_dde\_req** : la sécurité **401\_sec\_req** est conservée avec l'ensemble télétransmis **401\_dde\_req** afin de ménager un contrôle ultérieur,
- IV.2.b Affectation du n° d'ordre réception **402\_ore\_req**,
- IV.2.c Ajout de la date de réception **402\_hre\_req**,
- IV.2.d Mise à jour de la table de gestion des archives détenues par le tiers archiveur des requêtes **401\_dde\_req** (**401\_oen\_req**, **402\_ore\_req**, **402\_hre\_req**, **401\_dde\_req**),
- IV.2.e Estimation du délai de restitution,
- IV.2.f Transmission d'un accusé de réception (**402\_are\_req**) au donneur d'ordre comprenant le numéro d'ordre d'envoi initial (**401\_oen\_req**), le n° d'ordre de réception (**402\_ore\_req**), la date de réception (**402\_hre\_req**), le délai estimé pour la restitution et la sécurité transport (**402\_sec\_are**).

Le niveau de sécurité voulu déterminera le type d'horodatage : horodatage interne, horodatage effectué par un tiers horodateur qui peut être différent le cas échéant du tiers archiveur.

### **623. TRAITEMENT 3 (sur l'initiative du tiers archiveur)**

Après l'envoi de l'accusé de réception *402\_are\_req*, le tiers archiveur procède aux opérations suivantes :

- IV.3.a Extraction, et constitution du bloc à émettre *202\_arc\_blc* contenant notamment *202\_cpu\_are* et *202\_scc\_are*,
- IV.3.b N° d'ordre d'envoi de la demande *401\_oen\_req*,
- IV.3.c Affectation du n° d'ordre réponse *403\_ore\_blc*,
- IV.3.d Ajout de la date de réponse *403\_hre\_blc*,
- IV.3.e Mise à jour de la table de gestion des archives détenues par le tiers archiveur de la restitution *403\_res\_blc*,
- IV.3.f Sécurisation du transport (*403\_sec\_blc*).

Le niveau de sécurité voulu déterminera le type d'horodatage : horodatage interne, horodatage effectué par un tiers horodateur qui peut être différent le cas échéant du tiers archiveur.

### **624. TRAITEMENT 4 (sur l'initiative du donneur d'ordre)**

Pour se résumer, les opérations suivantes se succèdent :

- IV.4.a Contrôle d'intégrité de la sécurité de transport *403\_sec\_blc*,
- IV.4.b Déchiffrement du sceau chiffré avec la clé publique du tiers archiveur. Comparaison entre l'empreinte issue du déchiffrement (*201\_emp\_fic'*) et celle recalculée de l'archive (*201\_emp\_fic*), le fichier x' est destiné à être identique à x,
- IV.4.c Mise à jour de la table de gestion des archives avec les renseignements issus de *403\_res\_blc* (*403\_ore\_blc*, *403\_hre\_blc*).

## **7. Relations avec les autres tiers**

A côté du donneur d'ordre et du tiers archiveur, d'autres personnes peuvent être amenées à intervenir dans le scénario d'archivage afin de renforcer les questions de preuve en cas de litige et de garantir la sécurité des échanges électroniques.

Les personnes, à ce jour, identifiées, qui tiennent leur pouvoir de l'une et de l'autre ou seulement de l'une des parties à l'échange électronique, sont :

- le tiers horodateur,
- le tiers certificateur,
- les autres tiers archiveurs.

### **71. Rôle et fonction de ces autres tiers**

#### **711. Le tiers horodateur**

Dans les différents scénarii étudiés, il a été envisagé la mise en place d'un système d'horodatation réalisé soit en interne soit par un tiers horodateur indépendant, selon le niveau de sécurité souhaité.

L'horodatation qui repose sur un ensemble de techniques permet de s'assurer qu'un document électronique a été créé, signé, demandé ou consulté à une certaine date et heure.

Dans la mesure où le système d'horodatation mis en place doit pouvoir servir de preuve en cas de litige, il est nécessaire que la datation des messages échangés soit fiable, précise, protégée et reconnue par les partenaires à l'échange.

La mission comme l'étendue de la responsabilité du tiers horodateur sont définies dans un contrat de prestation de services qui le lie au donneur d'ordre et au tiers archiveur.

#### **712. Le tiers certificateur**

Comme le tiers horodateur, le tiers certificateur tient son pouvoir des parties et non de la loi.

En sa qualité d'intermédiaire choisi par les parties pour sa neutralité et son indépendance, le tiers certificateur a pour mission de contrôler et garantir la sécurité des échanges électroniques et de fournir des preuves en cas de litige.

A ce titre, il doit être en mesure de proposer aux parties, dans le cadre d'un contrat de prestation de services qui le liera à ces derniers, des services assurant au minimum :

- une identification fiable de l'émetteur et du destinataire,
- l'intégrité du contenu des messages échangés entre l'émetteur et le destinataire,
- la non répudiation par l'émetteur et le destinataire des messages échangés.

#### **713. Autres tiers archiveurs**

Afin d'assurer, dans un souci de sécurité, une dualité de conservation des archives qui lui seraient

télétransmises par un donneur d'ordre, le tiers archiveur peut être conduit à confier à un autre tiers archiveur la réplique des dites archives (contrat de back up).

Il peut être également envisagé que pour faire face à une réserve insuffisante en capacité de stockage, le tiers archiveur conclut avec un autre tiers archiveur un contrat de partenariat afin d'assurer sans discontinuité la prise en charge des éléments électroniques arrivants (contrat de partenariat).

Dans la mesure où le donneur d'ordre n'est pas le plus souvent, partie à ces contrats de back up et de partenariat, il sera nécessaire que le tiers archiveur lié contractuellement à son donneur d'ordre, l'en informe régulièrement soit par une clause de leur contrat réservant au tiers archiveur la possibilité de recourir aux services d'un autre tiers archiveur soit par une autorisation expresse du donneur d'ordre si une telle possibilité n'est pas envisagée contractuellement.

En tout état de cause, le tiers archiveur doit être particulièrement attentif dans ses relations avec ces autres tiers archiveurs, puisqu'il est seul responsable à l'égard de son donneur d'ordre des fautes commises par ces derniers, en l'absence de liens contractuels entre le donneur d'ordre et les autres tiers archiveurs.

## **72. Cumul des fonctions**

Si le recours à un tiers, indépendant des parties, semble en effet le meilleur moyen de renforcer la validité des échanges électroniques et donc la sécurité juridique des parties en cas de litige, il convient néanmoins de s'interroger sur la faisabilité ou non du cumul de ces fonctions.

- Tiers archiveur/Tiers horodateur

Il peut être envisagé que le tiers archiveur puisse également assurer les fonctions de tiers horodateur. Cependant, la présence d'un tiers indépendant des parties principales dans un scénario d'archivage, que sont le donneur d'ordre et le tiers archiveur, renforce l'efficacité des preuves en cas de litige ;

- Tiers archiveur/Tiers certificateur

Le tiers certificateur ayant notamment pour mission de garantir la sécurité des échanges électroniques, il apparaît que celui-ci doit être totalement indépendant des parties à ces échanges et ne peut donc cumuler ses fonctions avec celle de tiers archiveur ;

- Tiers horodateur/Tiers certificateur

En revanche, il n'existe pas d'obstacle majeur à ce qu'un tiers certificateur assure également les fonctions de tiers horodateur ;

- Autres tiers archiveurs

Bien que, le plus souvent, non lié contractuellement avec le donneur d'ordre, ces autres tiers archiveurs le sont avec le tiers archiveur. L'intervention d'un tiers indépendant des parties, permettant de renforcer l'efficacité des preuves en cas de litige, il n'apparaît donc pas souhaitable que ces autres tiers archiveurs, pour les raisons ci-dessus indiquées, puissent cumuler leurs fonctions avec celle de tiers certificateur ou de tiers horodateur.

### **73. Fin du contrat ou cessation d'activité du tiers**

Une distinction semble devoir être effectuée entre les Tiers horodateur/Tiers certificateur d'une part et les autres Tiers archiveurs d'autre part.

Cette distinction repose sur le fait que :

- le tiers horodateur et/ou le tiers certificateur sont, en général, contractuellement liés avec le donneur d'ordre et le tiers archiveur ;
- les autres tiers archiveurs, le plus souvent, avec le tiers archiveur exclusivement.

Comme le tiers archiveur dans ses relations avec le donneur d'ordre, il convient de s'assurer, en fin de contrat ou en cours de cessation d'activité, que les tiers en cause s'engagent, dans les délais prévus contractuellement, à remettre l'ensemble des éléments électroniques correspondant à leur prestation à la disposition :

- du ou des nouveaux tiers désignés par le donneur d'ordre et le tiers archiveur, s'agissant du tiers horodateur et du tiers certificateur ;
- du tiers archiveur ou de toute personne désignée par celui-ci, s'agissant des autres tiers archiveurs.



## **8. Traitements chez le donneur d'ordre et le tiers archiveur**

Dans l'entreprise comme chez le tiers archiveur, des traitements spécifiques sont à prévoir en fonction des contraintes du donneur d'ordre et du système informatique du tiers archiveur.

### **81. Traitements**

#### **811. Traitements de constitution des objets à archiver chez le donneur d'ordre**

L'entreprise donneur d'ordre a établi un plan d'archivage qui comprend :

- la description des objets à archiver (fichiers de données, états informatiques, etc.),
- les procédures permettant la constitution des objets à archiver,
- les contrôles de constitution des archives (en particulier les contrôles de contenu, la vérification de l'intégrité des objets et la conformité technique),
- la description des opérations à exécuter pour l'archivage, c'est-à-dire le transfert vers le site d'archivage (interne ou externe),
- le calendrier d'exécution des procédures d'archivage,
- la récupération des archives.

Ce plan doit nécessairement être mis à jour à chaque modification du système d'information, par exemple :

- ajout d'une nouvelle application informatique,
- modification substantielle d'une application,
- changement de système d'exploitation ou de système de gestion des bases de données,
- changement de prestataire d'exploitation informatique.

Les traitements sont détaillés aux chapitres 5 et 6.

#### **812. Traitements d'acquisition d'archives chez le tiers archiveur**

Le plan d'archivage doit prévoir des tests réguliers de ré-utilisation des archives. Chez le tiers archiveur, les traitements reposent principalement sur la gestion des archives électroniques qui lui sont confiées par le donneur d'ordre. Ils imposent le respect du code de bonne conduite du tiers archiveur, garantie pour le donneur d'ordre que ses archives seront récupérables telles qu'elles ont été déposées et ceci sur une longue période. Suivant le système informatique retenu par le tiers archiveur, ce dernier s'impose à respecter la norme AFNOR Z 42-013.

Les traitements sont détaillés aux chapitres 5 et 6.

### **82. Gestion des tables**

Aussi bien pour le donneur d'ordre que pour le tiers archiveur, une table de gestion des archives doit être tenue afin de suivre les entrées, sorties et demandes d'archives ou d'empreintes.

Le contenu de chaque table est défini au chapitre 32.

## 83. Organisation de la profession de tiers archiver

### 831. Au niveau du tiers archiver

#### 8311. Rôle, fonctions et organisation

Le tiers archiver a pour fonction de recevoir, d'archiver et de restituer tous éléments électroniques envoyés par ses clients donneurs d'ordre, entreprises ou mandataires des entreprises. Sa mission est définie par un contrat de prestation de services. Il assure notamment les fonctions suivantes :

- la réception et la gestion des éléments électroniques dont les délais de conservation sont précisés par le donneur d'ordre ;
- la réception et la mise en place de tout contrôle d'intégrité attaché à chaque ensemble de fichiers émis ; le calcul du chiffre-clé et son contrôle doivent être effectifs à chaque manipulation du fichier (réception du fichier, régénération des supports magnétiques, transfert sur cédérom, etc.) ;
- la tenue et la conservation d'une liste récapitulative des éléments électroniques reçus sachant que :
  1. la liste récapitulative peut être établie sur support informatique et doit être conservée pendant le délai de conservation précisé par le donneur d'ordre et ce, même en cas de rupture de contrat quelle qu'en soit la raison ; cette liste doit comporter au moins les mentions suivantes :
    - la date d'édition de la liste,
    - la version du logiciel utilisé,
    - la date de création et les références de l'élément électronique chez le donneur d'ordre,
    - la date et l'heure de réception ou d'émission de l'élément électronique,
    - la taille de l'élément électronique,
    - le propriétaire du fichier (donneur d'ordre, mandataire, etc.),
    - un numéro de réception,
    - les identifiants de l'émetteur et du récepteur donnés par le système de télétransmission ;
  2. la liste récapitulative doit indiquer de façon claire et précise les anomalies éventuelles intervenues lors de chaque transmission ;
  3. la liste récapitulative doit mentionner de façon claire et précise les dates de destruction ou de restitution des éléments électroniques;
  4. la liste doit pouvoir être éditée séquentiellement dans l'ordre d'arrivée ou d'émission des éléments électroniques.

#### 8312. Obligations

Le tiers archiver doit respecter strictement le contrat pour tout ce qui touche les flux d'informations avec ses donneurs d'ordre. Il s'engage à ne pas restituer les éléments électroniques à une autre personne que son donneur d'ordre ou les personnes mandatées par ce dernier, sauf obligations légales.

Le tiers archiver remplit les obligations minimales suivantes :

- disposer d'une réserve suffisante en capacité de stockage pour assurer sans discontinuité la prise en charge des éléments électroniques arrivants ;
- mettre en place des normes minimales de sécurité ;
- définir des contrôles adaptés ;
- créer et mettre à jour la table de gestion des éléments électroniques ;
- conserver l'intégralité des éléments électroniques reçus et non seulement les mentions obligatoires de la liste récapitulative visées ci-dessus ;
- prendre toutes les dispositions pour assurer la sécurité de l'archivage des éléments électroniques qui lui ont été confiés pendant toute la durée déterminée par le donneur d'ordre ; prendre toute disposition matérielle permettant d'assurer la continuité du service ;
- pendant la durée de son engagement et postérieurement à sa résiliation, n'adresser les éléments électroniques qu'aux seuls destinataires indiqués dans le contrat, sauf obligations légales ;
- protéger les données personnelles collectées pour l'enregistrement des entités ayant recours à ses services (obligation d'information, droit d'accès et de rectification aux informations pour les intéressés, etc., conformément à la loi du 26 janvier 1978 et à la directive européenne 95/46 du 24 octobre 1995) ;
- interdire l'utilisation à des fins personnelles ou professionnelles des programmes informatiques qui sont confiés par son donneur d'ordre et qui sont nécessaires à l'exploitation des éléments électroniques ;
- informer les donneurs d'ordre de la perte de la qualification de tiers archiveur ;
- restituer les éléments électroniques sous une forme convenue contractuellement avec le donneur d'ordre ;
- accepter des audits de vérification des dispositions qu'il a prises pour garantir le service ;
- prendre une assurance couvrant les risques liés à l'exécution du service et pendant toute la durée de sa mission ;
- en fin de contrat ou en cas de cessation d'activité, suivant les délais prévus contractuellement :
  - mettre à la disposition du donneur d'ordre ou de son nouveau prestataire d'archivage, les éléments électroniques qui lui avaient été confiés,
  - s'assurer auprès du donneur d'ordre de la capacité de ce dernier à exploiter les éléments électroniques,
  - détruire les éléments électroniques sur demande écrite du donneur d'ordre et fournir à celui-ci une attestation de destruction dont un double est conservé par le tiers archiveur,
  - assurer la réversibilité du service, c'est-à-dire le transfert du service vers un autre archiveur ou directement chez le donneur d'ordre.

Le tiers archiveur n'est en aucun cas responsable du contenu des éléments électroniques à archiver transmis par le donneur d'ordre.

### *8313. Responsabilités*

Le tiers archiveur est responsable :

- du respect de ses engagements contractuels vis-à-vis du donneur d'ordre ;
- de tout manquement à son obligation de confidentialité, et ce, notamment au regard des données personnelles que le donneur d'ordre lui a transmises ;
- des préjudices causés au donneur d'ordre en cas d'inexécution du contrat par le tiers archiveur ; des préjudices causés par son personnel dans le cadre des prestations de service offertes et définies dans le contrat ;

- des préjudices subis par le donneur d'ordre et résultant de dysfonctionnement du matériel utilisé par le tiers archiveur ;
- de la précision et de l'intégrité des données qu'il délivre et manipule ;
- de l'information du donneur d'ordre de toute évolution technique pouvant modifier le mode d'échange et de conservation des éléments électroniques ;
- de la lisibilité ultérieure des supports électroniques utilisés en tenant compte notamment des évolutions technologiques.

## **832. Au niveau de la profession de tiers archiveur**

### *8321. Rôle, fonctions et organisation*

L'ensemble des tiers archiveurs constitue un groupement de professionnels dont l'intérêt est de se rassembler et de respecter des règles communes, afin d'offrir aux donneurs d'ordre un service de confiance, et de garantir une interopérabilité entre ses membres.

Ce groupement doit :

- être structuré et disposer d'une instance représentative ;
- définir et appliquer une procédure de qualification des postulants au titre de tiers archiveur ;
- garantir collectivement la qualité du service en définissant les conditions de transfert et de sortie exceptionnelle de contrat.

### *8322. Obligations*

Le groupement professionnel des tiers archiveurs doit :

- établir un règlement intérieur de la structure interprofessionnelle mise en place et notamment, sa composition, sa gestion organisationnelle et financière, etc. ;
- définir une charte présentant l'éthique, les services et engagements minima que doivent respecter les tiers archiveurs membres du groupement et qui sera tenue à disposition de tout donneur d'ordre ;
- mutualiser les risques par la mise en place d'un système de solidarité entre les membres du groupement professionnel ;
- organiser le bon fonctionnement de la profession en attribuant des missions à d'autres tiers archiveurs du groupement en cas de carence, de cessation d'activité ou d'impossibilité de respecter les engagements contractuels par un tiers archiveur membre, après accord du donneur d'ordre ;
- élaborer un dispositif de contrôle de la qualité des prestations fournies par les tiers archiveurs, afin d'apprécier le respect de la charte ;
- former les professionnels et développer les compétences du groupement.

### *8323. Responsabilités*

Le groupement des tiers archiveurs ne peut être tenu responsable que des manquements à ses seules obligations.

### *8324. Garanties*

Le groupement des tiers archiveurs apporte des garanties au niveau collectif :

- mise en place d'un fonds de péréquation,
- souscription d'une assurance de groupe,

pour couvrir les défaillances de l'un de ses membres.

### **833. Au niveau du donneur d'ordre**

#### *8331. Rôle, fonctions et organisation*

Le donneur d'ordre a pour fonction d'envoyer au tiers archiveur les éléments électroniques à archiver.

Il accomplit les actions suivantes :

- la préparation et l'envoi des éléments électroniques à archiver ;
- les demandes de restitution des éléments électroniques archivés ;
- les autorisations de destruction des éléments électroniques archivés périmés.

#### *8332. Obligations*

Le donneur d'ordre doit remplir les obligations suivantes :

- préparation et envoi des éléments électroniques en conformité avec les dispositions techniques contractuelles, en particulier calcul d'un chiffre-clé de contrôle d'intégrité pour chaque élément électronique;
- gestion du cycle de vie des éléments électroniques et détermination de leur durée de conservation minimale ;
- information sans délai du tiers archiveur en cas de variation importante par rapport au flux habituel des échanges.

#### *8333. Responsabilités*

Le donneur d'ordre assume les responsabilités suivantes :

- respect des obligations légales quant au délai de conservation des archives ;
- respect des engagements contractuels vis-à-vis du tiers archiveur ;
- licéité des éléments électroniques archivés ;
- respect de la réglementation sur la cryptologie.

En effet, bien que le tiers archiveur n'ait pas à connaître du contenu des données à archiver, il est nécessaire d'insérer une clause de responsabilité qui stipule que le donneur d'ordre ne doit pas archiver des données qui mettent en péril l'ordre public et les bonnes mœurs. Ainsi, le donneur d'ordre doit respecter la législation en vigueur et les dispositions prévues par le code civil, le code pénal et celui de la propriété industrielle.

Une liste des textes applicables en l'espèce est présentée à titre indicatif en annexe 6.

#### *8334. Garanties*

Etant seul en mesure d'estimer le préjudice en cas de perte d'archives et par conséquent le montant

de la garantie y afférente, le donneur d'ordre doit éventuellement souscrire une police d'assurance auprès de la compagnie de son choix.

## **84. Exigences juridiques préalables**

Un certain nombre de documents ayant un caractère juridique doivent être rédigés. Ils touchent les tiers archiveurs, les donneurs d'ordre et conjointement les deux.

### **841. Exigences juridiques préalables au niveau de la profession de tiers archiveur**

Afin de garantir aux donneurs d'ordre un service de confiance, notamment ce qui concerne la qualité des prestations, la continuité du service et la conformité des systèmes aux normes applicables, les tiers archiveurs ont intérêt à constituer entre eux un groupement professionnel.

Ce groupement aurait pour mission de définir les conditions d'un service de confiance, d'établir les modalités de mise en œuvre de ces conditions, de les adapter si besoin pour rester en adéquation avec l'évolution des activités de l'archivage électronique et de veiller à leur respect par tous ses membres.

Pour remplir pleinement l'objectif fixé, un cadre juridique et organisationnel s'impose. Il comprend :

- un code de bonne conduite des tiers archiveurs (voir ci-dessous),
- un règlement intérieur venant compléter le code de bonne conduite, règlement qui définit de façon plus détaillées le fonctionnement du groupement, la définition de ses instances et de leur rôle, les modalités pratiques de mise en œuvre des dispositions de la charte : contrôle, continuité de service, garanties financières, contrats d'assurance, etc.

Dans le cadre de cette fonction, et afin de définir les cadres de référence pour l'exercice de leurs activités, les documents suivants sont établis :

- contrat type avec les tiers horodateurs,
- contrat type avec les tiers certificateurs,
- contrat(s) type entre les membres du groupement pour la mise en œuvre de modalités spécifiques liées à leur activité : regroupement de plusieurs tiers archiveurs derrière un chef de file pour répondre au besoin d'un même donneur d'ordre, dispositifs de secours, systèmes de sécurité, etc.
- déclaration à la CNIL,
- etc.

Il appartient aux membres de ce groupement de décider si les dispositions qui permettent de garantir au donneur d'ordre la continuité du service d'archivage doivent être prévues dans une convention spécifique entre membres ou être incluses dans un contrat type de partenariat entre membres.

Outre ces dispositions contractuelles, le groupement peut étudier l'opportunité d'un système d'assurance mutuelle (ou de caution mutuelle) en complément de dispositions techniques et contractuelles entre les membres pour compléter les garanties données aux donneurs d'ordre.

Le code de bonne conduite des tiers archiveurs est un document qui permet de définir une discipline destinée à mettre en œuvre l'activité de service de tiers archivage conforme à des engagements pré-définis et dont le but est de qualifier ledit service proposé par les prestataires informatiques à leurs clients entreprises ou organisation.

Ce code doit aborder les points suivants :

- la définition et le périmètre du service de tiers archivage ;
- la définition des responsabilités en cas de répartition, de modification ou de création de services ;
- les engagements sur la construction du service :
  - sur le service apporté,
  - sur la fourniture du service,
  - sur les composants du système informatique et leur intégration,
  - sur la sécurité : sauvegarde, restauration, information des donneurs d'ordre, confidentialité, télémaintenance du système, sensibilisation du donneur d'ordre, etc.
  - sur les fonctions d'échanges de données,
  - sur la documentation d'utilisation et d'exploitation (par exemple manuel),
  - sur la maintenabilité et l'évolutivité : documentation technique et gestion de configuration, etc.
  - sur les prestations de services : mise en service de la prestation, support au démarrage, assistance téléphonique, service après-vente, dépannage, maintenance logicielle et suivi, maintenance matérielle, etc.
  - sur le respect des règles de bonne conduite : lettre d'engagement, audit périodique du système informatique mis en place, etc. ;
- les engagements sur la commercialisation du service :
  - sur les pratiques commerciales : présentation du service et démonstration, règles de bonnes pratiques du donneur d'ordre, formation du personnel commercial, liste des responsables du tiers archiveur, catalogue des produits et des prestations de services, conditions préférentielles, référence à des labels ou des agréments, présentation des offres du tiers archiveur,
  - sur le ou les contrat(s) Tiers Archiveur/Donneur d'ordre ;
- les engagements sur la réalisation du service :
  - sur les relations après-vente entre le donneur d'ordre et le tiers archiveur : compétence du personnel en contact avec le donneur d'ordre, suivi des clients donneurs d'ordre, contenu du dossier de suivi, information des donneurs d'ordre,
  - sur les prestations : mesure de la satisfaction des donneurs d'ordre, démarche d'amélioration de la qualité du service.

## **842. Exigences juridiques préalables entre tiers archiveur et donneur d'ordre**

### *8421. Clause "Objet/Description du service"*

Cette clause décrit le service proposé au donneur d'ordre avec, le cas échéant, des options additionnelles disponibles.

Cette description d'ordre général peut être complétée d'une description technique renvoyée en annexe du contrat (taux de disponibilité/performance du service/délai et restitution).

L'ensemble des dispositions techniques et juridiques définit le périmètre de la prestation.

Il s'agit également de définir les modalités du service en termes :

- d'abonnement (prise de commande, acceptation en ligne, signature électronique),
- d'accès au service (transfert, retrait et consultation des fichiers, configuration matérielle minimale requise),
- de sécurité (code d'identifiant, mot de passe, signature électronique),
- de disponibilités (horaires, période de maintenance, espace disque alloué, serveur dédié ou partagé).

#### 8422. Clause "*Obligation du tiers archiveur*"

Cette clause rappelle, de manière exhaustive, les obligations du tiers archiveur telles que décrites au paragraphe 8312 et notamment l'obligation de :

- conserver l'intégralité des fichiers reçus,
- prendre toutes les dispositions pour assurer la pérennité de ces fichiers,
- n'adresser les fichiers conservés qu'aux seuls destinataires habilités par le donneur d'ordre sous sa responsabilité au titre du contrat (sous réserve des obligations légales),
- ne pas utiliser à des fins personnelles ou professionnelles les fichiers ou programmes informatiques confiés par le donneur d'ordre,
- restituer les fichiers dans leur forme originale, c'est à dire dans leur forme ou format de réception par le tiers archiveur .

#### 8423. Clause "*Obligation du donneur d'ordre*"

Cette clause expose l'ensemble des obligations du donneur d'ordre telles que décrites au paragraphe 8332 (à compléter en fonction des observations) et notamment concernant :

- les conditions d'utilisation du service conformément aux instructions fournies (respect des protocoles d'envoi)
- le signalement de tout défaut constaté,
- les autorisations légales, réglementaires ou administratives nécessaires,
- la connexion de son serveur au Centre Serveur du tiers archiveur,
- la prise en charge le coût des communications téléphoniques,
- la conformité des messages émis ou reçus,
- la mise à disposition de toutes informations et documentations nécessaires ou utiles pour la bonne exécution du service.

#### 8424. Clause "*Responsabilité*"

L'objet de cette clause est de rappeler que :

- le tiers archiveur ne peut être soumis qu'à une obligation de moyens dans le cadre de l'exécution du contrat,
- sa responsabilité ne peut être engagée qu'en cas de défaillance de sa part et sur faute prouvée par le donneur d'ordre,
- le tiers archiveur ne saurait être tenu pour responsable des manquements à des obligations qui ne relèvent pas de sa négligence ou qui auraient pour cause des éléments sur lesquels il n'a aucune

maîtrise.

Il convient également de prévoir une limitation de responsabilité et/ou de réparation, clause valable uniquement entre professionnels et destinée à limiter la responsabilité du tiers archiveur à un plafond financier déterminé au moment de la conclusion du contrat.

En outre, il peut être envisagé une préqualification des dommages indirects pouvant être réclamés par le donneur d'ordre en cas de litige.

#### *8425. Clause "Garanties"*

Cette clause précise les garanties données tant par le donneur d'ordre que par le tiers archiveur, telles que décrites au paragraphe 8314 et 8334.

#### *8426. Clause "Réversibilité"*

Le tiers archiveur s'engage à assurer la réversibilité du service, et donc le transfert des fichiers archivés sur un autre serveur connecté au réseau Internet, et désigné par le donneur d'ordre.

A la demande du donneur d'ordre, le tiers archiveur apporte son assistance au donneur d'ordre ou à tout autre prestataire désigné par celui-ci, pour faciliter le transfert des fichiers et donc la réversibilité du service.

Ces prestations d'assistance peuvent être, le cas échéant, valorisées au tarif standard du prestataire, en vigueur au moment du transfert, à défaut de meilleur accord entre les parties.

#### *8427. Clause "Autorisations"*

Cette clause indique les autorisations dont bénéficie le tiers archiveur au regard de la prestation de services qu'il assure (autorisations légales, administratives, réglementaires, professionnelles).

#### *8428. Clause "Conditions financières"*

Cette clause prévoit l'ensemble des conditions financières applicables au service (abonnement, tarifs, modification des tarifs, révision du prix, indices, modes de paiement et de facturation, réclamations, pénalités).

#### *8429. Clause "Durée"*

La durée du service est définie en considération des besoins du client et selon les formules de services proposés par le tiers archiveur (abonnement) avec des possibilités de dénonciation du contrat avant chaque période de reconduction du contrat.

#### *84210. Clause "Convention sur la preuve"*

Cette clause indique que le tiers archiveur et le donneur d'ordre entendent, dans le cadre de l'exécution du service, donner aux messages électroniques échangés la valeur de preuve entre elles des transmissions, des commandes de prestations et des paiements intervenus ; la portée de la preuve étant celle accordée au titre des dispositions de la loi du 13 mars 2000 réformant le Code civil et portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Ces dispositions ne seront toutefois pas applicables aux données et informations contenues dans les fichiers transmis et faisant l'objet du service.

#### *84211. Clauses génériques*

Les dispositions particulières visées ci-dessus sont à compléter par des dispositions habituelles afférentes à ce type de contrat de prestations de services (force majeure, résiliation, cession, titre, non renonciation, loi, compétence, etc.).

### **843. Exigences juridiques préalables au niveau du donneur d'ordre**

Dans certains cas, le donneur d'ordre fait appel à un tiers pour opérer sa propre gestion des archives. Un mandat doit donc être établi entre donneur d'ordre et mandataire afin de répartir les responsabilités entre les parties.

Par ailleurs, il n'y a pas spécifiquement d'exigences juridiques à respecter pour l'entreprise donneur d'ordre en ce qui concerne toute autorité nationale, communautaire ou internationale, qui détient le pouvoir d'effectuer des contrôles et/ou des investigations de par ses statuts ou ensuite d'une décision judiciaire opposable à tout tiers, telle que les autorités douanières, fiscales, policières, de sécurité sociale (URSSAF, etc.), le Conseil de la Concurrence, la Commission des Opérations de Bourse, la Commission de la Concurrence de l'Union Européenne et les services douaniers de cette dernière, les Ordres nationaux de certaines branches, les commissaires aux comptes, un expert judiciaire commis, sans que cette liste soit limitative.

Le tiers archiveur doit informer le donneur d'ordre immédiatement de tout événement lié à ces contrôles et investigations, quels que soient l'heure et le jour en cause.

## 9. Services ajoutés par les tiers archiveurs

On entend par services à valeur ajoutée, des prestations que le tiers archiveur est susceptible d'offrir au donneur d'ordre, en sus des services de base définis supra.

L'objet de ces services est de contribuer à la continuité de la chaîne de l'archivage (préparation, prise en charge, archivage, gestion de l'archivage, restitution, assistance, formation).

Ces services se déclinent en services amont et services aval. Ils visent à couvrir des travaux qui sont du ressort du donneur d'ordre.

Les principaux services amont qui peuvent être rendus sont les suivants :

- conditionnement et formatage des données et des documents à archiver : mise en œuvre de formats pivot, traduction et transcodification, contrôles de validité, constitution des lots d'archivage ;
- prise en charge et transfert des données à archiver : services de télécommunications, services « terrestres » (enlèvement des supports) ;
- contrôle de la chaîne d'acquisition des éléments à archiver : scellement, sécurité ;
- formation ;
- information et conseil pour le choix des autres tiers (horodateur, certificateur, autre archiveur) ;
- le cas échéant conseil pour la conservation des archives chez le donneur d'ordre et, éventuellement, fourniture du système d'archivage installé chez le donneur d'ordre.

Les principaux services en aval qui peuvent être offerts sont :

- la conservation "active" des documents confiés, c'est-à-dire la mise en œuvre de l'ensemble des dispositions de suivi et d'adaptation aux versions successives des progiciels, des logiciels et des navigateurs et du matériel (lecteurs, processeurs, etc.) dans le but de la sauvegarde des archives et du maintien de leur lisibilité ; ces dispositions doivent garantir la conservation de l'intégrité et de l'imputabilité du document archivé ;
- dans le cas de la conservation "passive" des documents confiés, fonction de veille pour le compte du donneur d'ordre qui peut décider cas par cas de mettre en œuvre les évolutions constatées ;
- l'accès direct en consultation des archives ;
- l'assistance aux contrôles réglementaires.

Cet ensemble de services s'inscrit dans des clauses de confidentialité et de respect du secret professionnel.



## Annexe 1 - Récapitulation des codes utilisés

NB - Le glossaire des abréviations utilisées dans cette récapitulation figure en annexe 2.

### Classement par variable

<i>102_arc_blc</i> :	ensemble du bloc archivé par le tiers archiveur comprenant <i>102_ore_lot</i> , <i>102_hre_lot</i> , <i>101_ens_lot</i> , <i>102_scl_ens</i>
<i>202_arc_blc</i> :	ensemble du bloc archivé par le tiers archiveur comprenant <i>202_ore_lot</i> , <i>202_hre_lot</i> , <i>202_cpu_are</i> , <i>202_scc_are</i>
<i>102_are_blc</i> :	accusé de réception de <i>101_ens_lot</i> donné par le tiers archiveur
<i>202_are_blc</i> :	accusé de réception de <i>201_ens_lot</i> donné par le tiers archiveur
<i>302_are_req</i> :	accusé de réception de la <i>301_dde_req</i> donné par le tiers archiveur
<i>402_are_req</i> :	accusé de réception de la <i>401_dde_req</i> donné par le tiers archiveur
<i>304_are_blc</i> :	accusé de réception des archives demandées
<i>202_cpu_are</i> :	clé publique du tiers archiveur
<i>301_dde_req</i> :	demande d'archives effectuée par le donneur d'ordre
<i>401_dde_req</i> :	demande d'empreinte effectué par le donneur d'ordre
<i>201_don_blc</i> :	lot à archivé en interne par le donneur d'ordre comprenant <i>201_har_fic</i> , <i>201_nar_fic</i> et <i>101_lot_fic</i>
<i>201_emp_fic</i> :	empreinte de l'élément à archiver <i>101_lot_fic</i>
<i>101_ens_lot</i> :	ensemble comprenant <i>101_oen_fic</i> , <i>101_hen_fic</i> , <i>101_lot_fic</i> , <i>101_sec_fic</i>
<i>201_ens_lot</i> :	ensemble comprenant <i>201_oen_fic</i> , <i>201_hen_fic</i> , <i>201_sec_fic</i> , <i>201_empr_fic</i>
<i>201_har_fic</i> :	date d'envoi du <i>101_lot_fic</i> donnée par le donneur d'ordre en interne
<i>101_hen_fic</i> :	date d'envoi du <i>101_lot_fic</i> donnée par le donneur d'ordre
<i>201_hen_fic</i> :	date d'envoi du sceau du <i>101_lot_fic</i> donnée par le donneur d'ordre
<i>301_hen_req</i> :	date d'envoi de la requête d'archives par le donneur d'ordre
<i>401_hen_req</i> :	date d'envoi de la requête d'empreinte par le donneur d'ordre
<i>102_hre_lot</i> :	date de réception par le tiers archiveur de l'ensemble <i>101_ens_lot</i>
<i>202_hre_lot</i> :	date de réception par le tiers archiveur du sceau de l'ensemble <i>101_ens_lot</i>
<i>302_hre_req</i> :	date de la réponse à la requête <i>301_dde_req</i> donnée par le tiers archiveur
<i>402_hre_req</i> :	date de la réponse à la requête <i>401_dde_req</i> donnée par le tiers archiveur
<i>303_hre_blc</i> :	date de la réponse des archives restituées donnée par le tiers archiveur
<i>403_hre_blc</i> :	date de la réponse de l'empreinte restituée donnée par le tiers archiveur
<i>304_hre_blc</i> :	date de l'accusé de réception des archives restituées donnée par le donneur d'ordre
<i>305_hre_blc</i> :	date de communication/restitution des archives demandées
<i>101_lot_fic</i> :	ensemble du lot à archiver
<i>201_nar_fic</i> :	n° d'ordre interne d'envoi du <i>101_lot_fic</i> donné par le donneur d'ordre
<i>101_oen_fic</i> :	n° d'ordre d'envoi du <i>101_lot_fic</i> donné par le donneur d'ordre
<i>201_oen_fic</i> :	n° d'ordre d'envoi du sceau du <i>101_lot_fic</i> donné par le donneur d'ordre
<i>301_oen_req</i> :	n° d'ordre de la requête d'archives par le donneur d'ordre
<i>401_oen_req</i> :	n° d'ordre de la requête d'empreinte par le donneur d'ordre
<i>102_ore_lot</i> :	n° d'ordre de réception par le tiers archiveur de l'ensemble <i>101_ens_lot</i>
<i>202_ore_lot</i> :	n° d'ordre de réception par le tiers archiveur du sceau de l'ensemble <i>101_ens_lot</i>
<i>302_ore_req</i> :	n° d'ordre de la réponse à la requête <i>301_dde_req</i> donné par le tiers archiveur
<i>402_ore_req</i> :	n° d'ordre de la réponse à la requête <i>401_dde_req</i> donné par le tiers archiveur
<i>303_ore_blc</i> :	n° d'ordre des archives restituées donné par le tiers archiveur

<b>403_ore_blc</b> :	n° d'ordre de l'empreinte restituée donné par le tiers archiver
<b>304_ore_blc</b> :	n° d'ordre de l'accusé de réception des archives restituées donné par le donneur d'ordre
<b>305_ore_blc</b> :	n° d'ordre de communication/restitution des archives demandées
<b>301_dde_req</b> :	informations concernant la demande de requête elle-même comprenant <b>101_oen_fic</b> ou <b>102_ore_lot</b> ,
<b>303_res_blc</b> :	archives restituées par le tiers archiver
<b>403_res_blc</b> :	empreinte restituée par le tiers archiver
<b>202_scc_are</b> :	sceau chiffré de l'empreinte <b>201_emp_fic</b>
<b>102_scl_ens</b> :	sceau de l'ensemble <b>101_ens_lot</b> , <b>102_ore_lot</b> , <b>102_hre_lot</b>
<b>101_sec_fic</b> :	sécurité transport du <b>101_ens_lot</b> effectuée par le donneur d'ordre
<b>201_sec_fic</b> :	sécurité transport du sceau du <b>101_ens_lot</b> effectuée par le donneur d'ordre
<b>102_sec_are</b> :	sécurité transport du <b>102_are_blc</b> effectuée par le tiers archiver
<b>202_sec_are</b> :	sécurité transport du <b>202_are_blc</b> effectuée par le tiers archiver
<b>301_sec_req</b> :	sécurité transport de la <b>301_dde_req</b> effectuée par le donneur d'ordre
<b>401_sec_req</b> :	sécurité transport de la <b>401_dde_req</b> effectuée par le donneur d'ordre
<b>302_sec_are</b> :	sécurité transport de l'accusé de réception <b>302_are_req</b> effectuée par le tiers archiver en réponse à une requête
<b>402_sec_are</b> :	sécurité transport de l'accusé de réception <b>402_are_req</b> effectuée par le tiers archiver en réponse à une requête
<b>303_sec_blc</b> :	sécurité transport de la restitution des archives <b>303_res_blc</b> effectuée par le tiers archiver en réponse à une requête
<b>403_sec_blc</b> :	sécurité transport de la restitution de l'empreinte <b>403_res_blc</b> effectuée par le tiers archiver en réponse à une requête
<b>304_sec_blc</b> :	sécurité transport du <b>304_are_blc</b> effectuée par le donneur d'ordre

### **Classement par n° de traitement**

<b>101_ens_lot</b> :	ensemble comprenant <b>101_oen_fic</b> , <b>101_hen_fic</b> , <b>101_lot_fic</b> , <b>101_sec_fic</b>
<b>101_hen_fic</b> :	date d'envoi du <b>101_lot_fic</b> donnée par le donneur d'ordre
<b>101_lot_fic</b> :	ensemble du lot à archiver
<b>101_oen_fic</b> :	n° d'ordre d'envoi du <b>101_lot_fic</b> donné par le donneur d'ordre
<b>101_sec_fic</b> :	sécurité transport du <b>101_ens_lot</b> effectuée par le donneur d'ordre
<b>102_arc_blc</b> :	ensemble du bloc archivé par le tiers archiver comprenant <b>102_ore_lot</b> , <b>102_hre_lot</b> , <b>101_ens_lot</b> , <b>102_scl_ens</b>
<b>102_are_blc</b> :	accusé de réception de <b>101_ens_lot</b> donné par le tiers archiver
<b>102_hre_lot</b> :	date de réception par le tiers archiver de l'ensemble <b>101_ens_lot</b>
<b>102_ore_lot</b> :	n° d'ordre de réception par le tiers archiver de l'ensemble <b>101_ens_lot</b>
<b>102_scl_ens</b> :	sceau de l'ensemble <b>101_ens_lot</b> , <b>102_ore_lot</b> , <b>102_hre_lot</b>
<b>102_sec_are</b> :	sécurité transport du <b>102_are_blc</b> effectuée par le tiers archiver
<b>201_don_blc</b> :	lot à archivé en interne par le donneur d'ordre comprenant <b>201_har_fic</b> , <b>201_nar_fic</b> et <b>101_lot_fic</b>
<b>201_emp_fic</b> :	empreinte de l'élément à archiver <b>101_lot_fic</b>
<b>201_ens_lot</b> :	ensemble comprenant <b>201_oen_fic</b> , <b>201_hen_fic</b> , <b>201_sec_fic</b> , <b>201_empr_fic</b>
<b>201_har_fic</b> :	date d'envoi du <b>101_lot_fic</b> donnée par le donneur d'ordre en interne
<b>201_hen_fic</b> :	date d'envoi du sceau du <b>101_lot_fic</b> donnée par le donneur d'ordre
<b>301_hen_req</b> :	date d'envoi de la requête d'archives par le donneur d'ordre
<b>201_nar_fic</b> :	n° d'ordre interne d'envoi du <b>101_lot_fic</b> donné par le donneur d'ordre
<b>201_oen_fic</b> :	n° d'ordre d'envoi du sceau du <b>101_lot_fic</b> donné par le donneur d'ordre

**201\_sec\_fic** : sécurité transport du sceau du **101\_ens\_lot** effectuée par le donneur d'ordre  
**202\_arc\_blc** : ensemble du bloc archivé par le tiers archiver comprenant **202\_ore\_lot**, **202\_hre\_lot**, **202\_cpu\_are**, **202\_scc\_are**  
**202\_are\_blc** : accusé de réception de **201\_ens\_lot** donné par le tiers archiver  
**202\_cpu\_are** : clé publique du tiers archiver  
**202\_hre\_lot** : date de réception par le tiers archiver du sceau de l'ensemble **101\_ens\_lot**  
**202\_ore\_lot** : n° d'ordre de réception par le tiers archiver du sceau de l'ensemble **101\_ens\_lot**  
**202\_scc\_are** : sceau chiffré de l'empreinte **201\_emp\_fic**  
**202\_sec\_are** : sécurité transport du **202\_are\_blc** effectuée par le tiers archiver  
**301\_dde\_req** : informations concernant la demande de requête elle-même comprenant **101\_oen\_fic** ou **102\_ore\_lot**,  
**301\_dde\_req** : demande d'archives effectuée par le donneur d'ordre  
**301\_oen\_req** : n° d'ordre de la requête d'archives par le donneur d'ordre  
**301\_sec\_req** : sécurité transport de la **301\_dde\_req** effectuée par le donneur d'ordre  
**302\_are\_req** : accusé de réception de la **301\_dde\_req** donné par le tiers archiver  
**302\_hre\_req** : date de la réponse à la requête **301\_dde\_req** donnée par le tiers archiver  
**302\_ore\_req** : n° d'ordre de la réponse à la requête **301\_dde\_req** donné par le tiers archiver  
**302\_sec\_are** : sécurité transport de l'accusé de réception **302\_are\_req** effectuée par le tiers archiver en réponse à une requête  
**303\_hre\_blc** : date de la réponse des archives restituées donnée par le tiers archiver  
**303\_ore\_blc** : n° d'ordre des archives restituées donné par le tiers archiver  
**303\_res\_blc** : archives restituées par le tiers archiver  
**303\_sec\_blc** : sécurité transport de la restitution des archives **303\_res\_blc** effectuée par le tiers archiver en réponse à une requête  
**304\_are\_blc** : accusé de réception des archives demandées  
**304\_hre\_blc** : date de l'accusé de réception des archives restituées donnée par le donneur d'ordre  
**304\_ore\_blc** : n° d'ordre de l'accusé de réception des archives restituées donné par le donneur d'ordre  
**304\_sec\_blc** : sécurité transport du **304\_are\_blc** effectuée par le donneur d'ordre  
**305\_hre\_blc** : date de communication/restitution des archives demandées  
**305\_ore\_blc** : n° d'ordre de communication/restitution des archives demandées  
**401\_dde\_req** : demande d'empreinte effectué par le donneur d'ordre  
**401\_hen\_req** : date d'envoi de la requête d'empreinte par le donneur d'ordre  
**401\_oen\_req** : n° d'ordre de la requête d'empreinte par le donneur d'ordre  
**401\_sec\_req** : sécurité transport de la **401\_dde\_req** effectuée par le donneur d'ordre  
**402\_are\_req** : accusé de réception de la **401\_dde\_req** donné par le tiers archiver  
**402\_hre\_req** : date de la réponse à la requête **401\_dde\_req** donnée par le tiers archiver  
**402\_ore\_req** : n° d'ordre de la réponse à la requête **401\_dde\_req** donné par le tiers archiver  
**402\_sec\_are** : sécurité transport de l'accusé de réception **402\_are\_req** effectuée par le tiers archiver en réponse à une requête  
**403\_hre\_blc** : date de la réponse de l'empreinte restituée donnée par le tiers archiver  
**403\_ore\_blc** : n° d'ordre de l'empreinte restituée donné par le tiers archiver  
**403\_res\_blc** : empreinte restituée par le tiers archiver  
**403\_sec\_blc** : sécurité transport de la restitution de l'empreinte **403\_res\_blc** effectuée par le tiers archiver en réponse à une requête



## Annexe 2 - Glossaire des abréviations

### Sémantique attachée à une variable

<i>arc</i> :	à archiver
<i>are</i> :	accusé de réception
<i>cpu</i> :	clé publique
<i>dde</i> :	demande
<i>don</i> :	donneur d'ordre
<i>emp</i> :	empreinte
<i>har</i> :	heure et date de l'accusé de réception
<i>hen</i> :	heure et date d'envoi
<i>hre</i> :	heure et date de réception
<i>lot</i> :	mise en lot
<i>oen</i> :	n° d'ordre d'envoi
<i>ore</i> :	n° d'ordre de réception
<i>nar</i> :	n° d'ordre d'accusé de réception
<i>res</i> :	restitution
<i>scl</i> :	sceau
<i>sec</i> :	sécurité de transport

### Objet de l'application de la variable

<i>are</i> :	accusé de réception
<i>blc</i> :	bloc
<i>ens</i> :	ensemble
<i>fic</i> :	fichier
<i>lot</i> :	lot
<i>req</i> :	requête



## Annexe 3 - Glossaire

NB –Les définitions proposées ne concernent que le présent document.

### Présentation :

Le terme français est indiqué en **gras**.

Le terme anglais correspondant est indiqué à la suite en *gras –italique*.

L'origine des définitions est indiquée en *italique* entre crochets.

Lorsque cela est jugé nécessaire, une explication est donnée dans un paragraphe en retrait.

**Accusé de réception (*acknowledgement of receipt*)** : Message permettant d'informer l'émetteur de la prise en compte, de la mise en suspens ou du rejet de ses opérations et de la détection d'éventuelles anomalies.

**Algorithme (*algorithmics*)** : Etude de la résolution de problèmes par la mise en œuvre de suites d'opérations élémentaires selon un processus défini aboutissant à une solution. Dans le domaine de la sécurité, l'algorithme qualifie principalement une procédure de calcul de clé, de code secret ou de mot de passe.

**Archives (*archives*)** : Les archives en phase de constitution ou de traitements sont un ensemble de documents, rassemblés et classés à des fins historiques ou juridiques. L'archivage est une fonction en soi, qu'il ne faut pas confondre ni avec la sauvegarde ni avec la GED. Les données archivées nécessitent un support adapté, fiable, résistant au temps et suffisamment sécurisé.

**ASP (*Application Service Provider*)** : La location d'applications consiste, pour une entreprise, à payer pour utiliser à distance une application hébergée chez un prestataire de services. L'entreprise règle un loyer mensuel pour une ressource standard (matériel, logiciel et réseaux), en fonction du nombre d'utilisateurs, voire d'indicateurs d'usage (nombre de comptes gérés, de colis transportés, etc.). Le concept s'apparente à l'ancien service bureau, mais à la mode Internet.

**Authentification (*authentication*)** : Processus visant à établir de manière formelle et intangible l'identification des parties à un échange ou une transaction électronique. Ce processus implique que les parties confirment et valident leur identification par des moyens techniques, tels que mot ou phrase de passe, un code secret, une réponse à un défi ou encore une sécurisation numérique. [ISO] En cas d'authentification mutuelle, chaque partie doit authentifier l'autre.

**Authentification de message (*message authentication*)** : Action de vérifier qu'un message a été transmis intact par l'émetteur supposé au destinataire prévu.

**Authentification des données (*data authentication*)** : Processus servant à vérifier l'intégrité des données transmises, tout particulièrement dans un message.

**Authentification réciproque (*reciprocal authentication*)** : Garantie pour chacun des deux partenaires que l'autre est bien celui qui a été identifié. Le système central est assuré que l'utilisateur du terminal est bien celui qui s'est annoncé, mais également que cet utilisateur est certain que le système central est bien celui sur lequel il veut se connecter.

**Autorité de certification (*AC, Certification Authority, CA*)** : Organisme ayant la confiance d'une ou plusieurs autres entités pour créer, attribuer et révoquer ou suspendre des certificats de clés publiques.

**Bi-clé asymétrique** : Ensemble des paramètres utilisés dans un algorithme cryptographique asymétrique. Une bi-clé asymétrique est composé d'un ensemble de paramètres rendus publics, globalement appelés la clé publique, et d'un ensemble de paramètres conservés secrets par de vers le propriétaire de la bi-clé, et appelés la clé privée. Les deux ensembles de clés ont la propriété que, connaissant la clé publique, il est impossible par le calcul d'en déduire la clé privée.

**Certificat (*certificate*)** : De façon générique c'est un objet informatique logique qui permet de lier de façon intangible une identité d'entité à certaines caractéristiques de cette entité. Lorsqu'une des caractéristiques est une clé publique, on parlera de certificat de clé publique. Si ce n'est pas le cas on parlera de certificat d'attributs. Le lien est créé par la sécu-

risation de l'ensemble des données du certificat par la clé privée de l'autorité qui émet le certificat. [ISO]

Par extension on comprend que le certificat est l'ensemble formé par les données et par la sécurisation de l'autorité sur ces données. La finalité première d'un certificat est de permettre à un utilisateur de vérifier l'authenticité (identité, caractéristique du propriétaire) de la clé publique qu'il va utiliser pour vérifier la sécurisation produite par le signataire, en se basant sur la garantie apportée par l'autorité de certification.

**Chiffre (cipher)** : Principe de codage utilisant la substitution d'un caractère par un autre ou éventuellement par plusieurs autres en se servant d'un algorithme de transformation de complexité variable.

**Chiffrement (ciphering, encryption)** : Procédé visant à transformer, à l'aide de conventions secrètes, des informations ou des signaux clairs en informations ou signaux inintelligibles pour des tiers. Le procédé peut également permettre de réaliser l'opération inverse, grâce à des matériels ou logiciels conçus à cet effet (art. 28 de la loi du 29 décembre 1990). Ce processus utilise généralement des algorithmes cryptographiques. " [recommandation n°901/DISSI/SCSSI]

Le terme chiffrement devrait être réservé au mécanisme visant à rendre le service de sécurité de confidentialité (voir ISO7498-2). L'opération inverse est alors le déchiffrement. Le décryptage est une opération effectuée par le cryptanalyste qui ne connaît pas la clé de déchiffrement visant à rétablir le clair ou retrouver la clé ayant servi à chiffrer.

**Clé (key)** : Série de symboles commandant les opérations de chiffrement et de déchiffrement. Ce paramètre est impossible à déduire des données d'entrée et de sortie.

**Clé privée (private key)** : Partie du bi-clé asymétrique qui n'est connue que de son propriétaire. [ISO]

Cette définition doit être scrupuleusement respectée lorsque le bi-clé est utilisé pour la sécurisation numérique, et d'autant plus que le service de non répudiation doit être assuré.

Il faut noter cependant que cette définition devient fausse dès lors que le bi-clé est utilisé dans le cadre du chiffrement de données (directement ou indirectement par enveloppe numérique) et que le système cryptographique permet le recouvrement des clés au titre de la loi française de 1996 sur la cryptologie.

**Clé publique (public key)** : Partie du bi-clé qui est communiquée aux utilisateurs pour vérifier ou chiffrer. [ISO]

Cette clé n'est donc pas secrète, ce qui ne veut pas dire qu'elle doit être publiée, il suffit qu'elle soit communicable ou communiquée aux entités qui en ont besoin.

L'intégrité et l'authenticité de la clé publique sont essentiels et peuvent être assurées par un processus de certification.

**Confidentialité (confidentiality)** : Caractère de ce qui est confidentiel. Nécessité liée à la sécurité des informations, visant à interdire l'accès de certaines données aux personnes ou aux entités non autorisées.

**Confidentialité des données (data confidentiality)** : Données dont la connaissance par des employés ou des tiers pourrait causer un préjudice à l'entreprise. Par exemple, il peut s'agir des marges, du salaire des employés, des commissions versées pour l'acquisition de marchés, de prix d'achats, de secrets de fabrication, etc.

**Contrôle (check)** : Vérification d'une donnée, d'un travail ou d'un équipement permettant d'examiner la bonne exécution d'un processus.

**Contrôle de cohérence (analytical review)** : Contrôle tendant à vérifier si les données associées sont compatibles entre elles.

**Contrôle de vraisemblance (test of reasonableness)** : Contrôle tendant à vérifier si les valeurs de certaines données obéissent à des critères habituels prédéterminés.

**Copie de sauvegarde, copie de sécurité (backup copy)** : Copie de programme ou de fichier à laquelle on peut se référer si l'original est perdu ou endommagé, ou encore, copie effectuée avant un travail pour conserver les données susceptibles d'être modifiées pendant le travail.

**Cryptographie (cryptography)** : Discipline qui englobe les principes, moyens et méthodes permettant la transformation de données, dans le but d'assurer, ensemble ou séparément, les services de confidentialité de leur contenu, de détection de leur modification, et/ou d'empêcher leur utilisation non autorisée. [recommandation n°901/DISSI/SCSSI]

Le chiffrement n'est qu'un des mécanismes cryptographiques visant à rendre le service de confidentialité.

**Déchiffrement (decryption)** : Action de déchiffrer un message précédemment chiffré pour en retrouver la signification, par une opération inverse du chiffrement. On remarquera que le déchiffrement suppose la méthode de chiffrement connue, alors que le décryptage indique qu'on ignore la clé utilisée et qu'on cherche à la découvrir. En conséquence, le terme "cryptage" n'existe pas.

**Déclaration relative aux Pratiques de certification ( )** : voir DPC.

**Décryptage (*decryption*)** : Recherche de la signification d'un message chiffré dont on ne connaît pas la clé de déchiffrement.

**De secours (*back up*)** : Qualifie les procédures et les matériels destinés à être utilisés dans certains cas d'anomalie de fonctionnement.

**DES (*data encryption system*)** : Système de codage cryptographique mis au point par IBM.

**Document (*document*)** : Ensemble d'un support et des données enregistrées sur celui-ci, sous une forme en général permanente et lisible par l'homme ou par une machine.

**Donnée (*data*)** : Représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement.

**DPC (*Déclaration des Pratiques de certification*)** : Document décrivant les pratiques qu'une autorité de certification emploie pour l'émission des certificats.

**Empreinte (*Print*)** : Résultat d'une fonction mathématique qui fait correspondre à des valeurs de longueur quelconque d'un domaine très grand, des valeurs d'une longueur fixe dans un domaine fini. La fonction de prise d'empreinte associée permet de réduire un très long message à une empreinte de longueur fixe qui est suffisamment compacte pour être introduite dans un algorithme de signature. Une bonne fonction de prise d'empreinte doit être sans collision, c'est-à-dire qu'il est impossible par le calcul de déterminer une seconde entrée pouvant correspondre à l'empreinte d'une entrée donnée.

**Fiabilité (*reliability*)** : Qualifie la faculté d'un système quelconque à résister aux attaques dont il peut faire l'objet.

**Fichier (*data set, file*)** : Ensemble organisé d'articles ou d'enregistrements de même nature, susceptibles de faire l'objet de traitements par les mêmes programmes ou issus de tels traitements.

**Format (*format*)** : Agencement structuré d'un support de données ; disposition des données elles-mêmes ; dérivés : formater, formatage.

**ICP (*PKI, Public Key Infrastructure*)** : Ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de certificats utilisés par les services de sécurité basés sur de la cryptographie à clé publique.

**Identification (*identification*)** : Opération par laquelle l'identité d'un utilisateur est connue par le système.

**IETF (*Internet Engineering Task Force*)** : Ensemble de groupes de travail qui développent les nouveaux standards pour l'Internet.

**Information (*information*)** : Élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué. Note - l'information est ainsi considérée comme le contenu sémantique d'une donnée ; toutefois, le terme est souvent employé à la place de donnée comme par exemple dans l'expression *support d'information*.

**Infrastructure à clés publiques (*Public Key Infrastructure*)** : voir ICP.

**Intégrité (*integrity*)** : Propriété assurant que des données n'ont pas été modifiées, insérées ou détruites de façon non autorisée.

**Intégrité des données (*data integrity*)** : Garantie que les données n'ont pas été altérées ou détruites, accidentellement ou intentionnellement.

**Liste d'habilitation** : voir Profil d'accès.

**Méthode objet (*object procedure*)** : Conception orientée par les objets, née de la constatation d'un certain nombre d'inconvénients et de manques inhérents aux méthodes de conception classique : manque de cohérence entre le vocabulaire de l'utilisateur et sa traduction en termes informatiques, manque de souplesse face aux modifications fonctionnelles, etc. La méthode objet utilise un formalisme graphique qui établit la visibilité, donc les liens entre les objets, l'interface, les attributs, les liens entre les objets.

**Méthode UML (*UML procedure*)** : Une méthode est une des implémentations possibles d'une opération.

**Modèle UML (*UML template*)** : Un modèle est une représentation sémantiquement complète d'un système.

**Objet (*object*)** : Un objet est la représentation d'une entité abstraite ou une abstraction d'un objet physique du monde réel. Le terme d'objet est parfois utilisé comme synonyme de classe, parfois comme synonyme d'instance.

**PC (*Certification policy*)** : Ensemble de règles qui décrit la façon dont un certificat est applicable à un domaine particulier et/ou une classe d'applications ayant des exigences de sécurité communes. Par exemple, une politique d'usage de certificats particulière pourrait indiquer l'applicabilité d'un type de certificat à l'authentification de transactions EDI pour le commerce de biens dans une gamme de prix donnée. La politique d'usage de certificats devrait être utilisée par l'utilisateur d'un certificat pour décider s'il peut accepter ou non les conditions et les justificatifs sur lesquels le lien entre l'identité du propriétaire du certificat et la clé publique a été effectué. Un sous ensemble de composants du cadre de politique d'usage de certificats donne des valeurs concrètes pour définir celle-ci. La politique d'usage de certificats est représentée par un identifiant d'objet enregistré dans le certificat X.509 Version 4. Le propriétaire enregistre également une description textuelle de la politique et la rend disponible aux entités en relation.

**Politique de certification** : voir **PC**.

**Prestataires de Services de Certification** : voir **PSC**.

**Profil d'accès / liste d'habilitation (*capability list*)** : liste associée à un sujet et qui identifie tous les types d'accès de ce sujet pour tous les objets.

**Profil de document (*document profile*)** : ensemble d'attributs qui définissent les caractéristiques de la totalité d'un document, telles que son type et son format.

**Profil d'utilisateur (*user profile*)** : description des droits et limites attribués à l'opérateur de terminal (l'utilisateur) à l'égard de la connaissance des fichiers ainsi que de l'introduction, de la manipulation et de l'extraction de l'information. Description d'un utilisateur comprenant des données telles que l'identificateur d'utilisateur, le nom de l'utilisateur, le mot de passe, les droits d'accès et d'autres attributs.

**PSC (*Certification Service Provider*)** : toute personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques.

**Reprise (*restart*)** : continuation de l'exécution d'un programme arrêté au cours de son déroulement ; une reprise n'est possible qu'à partir d'un point de contrôle ou d'un point d'arrêt.

**Reprise en secours, de sécurité, de réserve (*back-up*)** : se dit des moyens gardés en réserve en prévision d'une interruption anormale du fonctionnement des installations.

**Requête (*request*)** : Demande effectuée pour obtenir quelque chose : demande destinée à lancer une recherche dans une base de données, dans un fichier. Expression formalisée d'une demande.

**RSA (*Rivest, Shamir, Adleman*)** : sigle désignant un algorithme de cryptage à double clé mis au point au MIT de Stanford.

**Sauvegarde (*backup*)** : Transfert sur un support distinct d'informations en mémoire en vue de les protéger ou de les mettre en sécurité.

**Sceau numérique (*digital seal*)** : Valeur associée à un message pour s'assurer de son intégrité. Le sceau est obtenu par une transformation univoque du message. Toute modification du message entraînera un résultat différent, révélateur de la modification par comparaison des sceaux..

**Scellement numérique (*digital sealing*)** : Fonction mathématique permettant d'obtenir le sceau (ou empreinte) à partir d'un message de façon à en garantir l'intégrité. Synonymes : hachage/condensation/scellement

**Scénario (*scenario*)** : Séquence spécifique d'actions qui illustre des comportements. Un scénario peut être utilisé pour illustrer une interaction. Une interaction est une spécification de comportement qui comprend un ensemble de messages échangés entre un ensemble d'objets dans un contexte particulier dans le but d'accomplir une tâche particulière. Une

interaction peut être illustrée par un ou plusieurs scénarii. Un comportement correspond aux effets observables d'une opération ou d'un événement y compris les résultats produits."

**Scénario UML (*UML scenario*)** : Un scénario est un exemple particulier d'exécution d'un cas d'utilisation, depuis son début jusqu'à sa fin. Un scénario est décrit textuellement par un paragraphe descriptif, et peut être traduit graphiquement par un ou plusieurs diagrammes de séquence. Pour représenter tous les cas de figure, il faut écrire différents scénarios, obtenus en faisant varier les entrées et les sorties du système et l'ordre d'apparition des événements.

**Sécurité de transport (*Transport layer security*)** : Ensemble de mesures prises pour protéger une fonction de communication assurant l'acheminement complet des informations entre deux points terminaux d'un réseau, contre toute destruction, dégradation, divulgation, malveillance, etc.

**Signature (*electronic seal*)** : Méthode de contrôle permettant de s'assurer qu'un message émane bien de l'expéditeur prévu.

**Signature électronique (*electronic non handwritten signature*)** : Donnée ajoutée à une donnée ou à un ensemble de données et garantissant l'origine de cette ou de ces données, c'est-à-dire certifiant l'authenticité de l'émetteur.

**Sécurisation électronique (*electronic signature*)** : Action de chiffrer, à l'aide de la clé privée d'une bi-clé, afin de garantir l'authenticité, l'intégrité et la non répudiation d'un document électronique.

**Tiers archiveur (*independent archiver*)** : Personne physique ou morale qui se charge pour le compte de tiers, d'assurer et de garantir la conservation et l'intégrité de documents électroniques.

**Tiers certificateur (*Trusted Third party*)** : Autorité de certification et de notarisation des échanges électroniques. Elle est conventionnellement désignée par les parties à un échange de données informatisé, généralement dans le cadre d'un accord d'interchange ; sa mission consiste à contrôler et garantir la sécurisation d'un échange ou d'une transaction électronique (intégrité du contenu du message, identification de l'expéditeur et du destinataire, date d'émission, etc.).

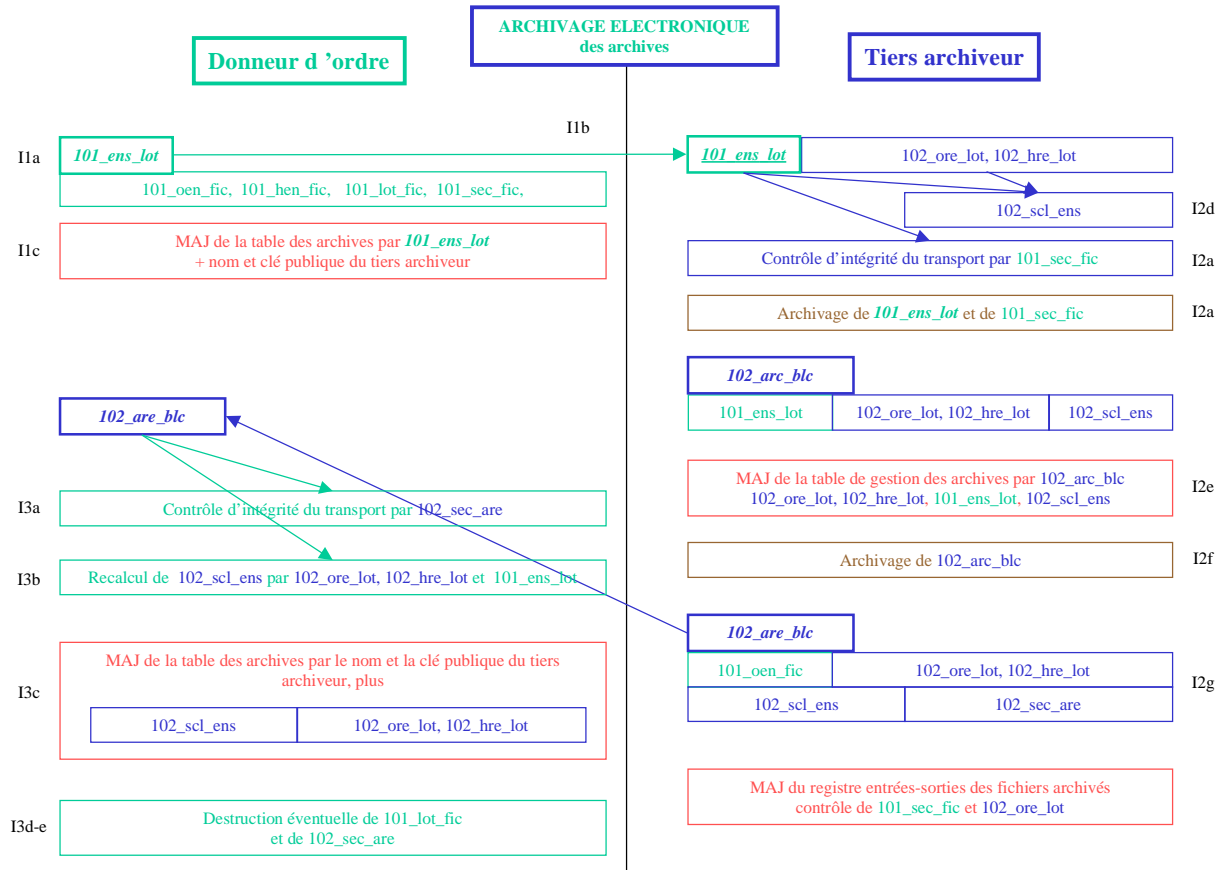
**Tiers horodateur (*Time Stamping Authority*)** : L'horodatation est un ensemble de techniques utilisant des algorithmes cryptographiques permettant de s'assurer si un document électronique a été créé ou signé à (ou avant) une certaine date. En pratique, la plupart des systèmes d'horodatation font appel à un tiers de confiance appelé Autorité d'horodatation (TSA, Time-Stamping Authority). Une horodatation est une attestation électronique émanant d'un TSA qui identifie qu'un document électronique a été présenté à un TSA à une certaine date.

**Sources** : Arrêtés ministériels du 22 décembre 1981, 30 décembre 1983, 30 mars 1987 et du 27 juin 1989 sur l'enrichissement du vocabulaire informatique ; dictionnaire informatique Masson, 1987 ; dictionnaire de l'informatique Larousse, 1986 ; dictionnaire de la comptabilité, ICCA, OEC, 1994 ; Progiciels de comptabilité, ECM, 1990 ; groupe "terminologie" du Comité français d'organisation et de normalisation bancaires ; L'archivage électronique, ECM, 1998 ; Glossaire de l'informatique et des réseaux, Le Moniteur, 1995 ; Livre blanc Tiers de confiance, IALTA, 1998 ; documents ISO ; Dictionnaire de l'EDI et du Commerce électronique, Edifrance, Paris, 2000 ;

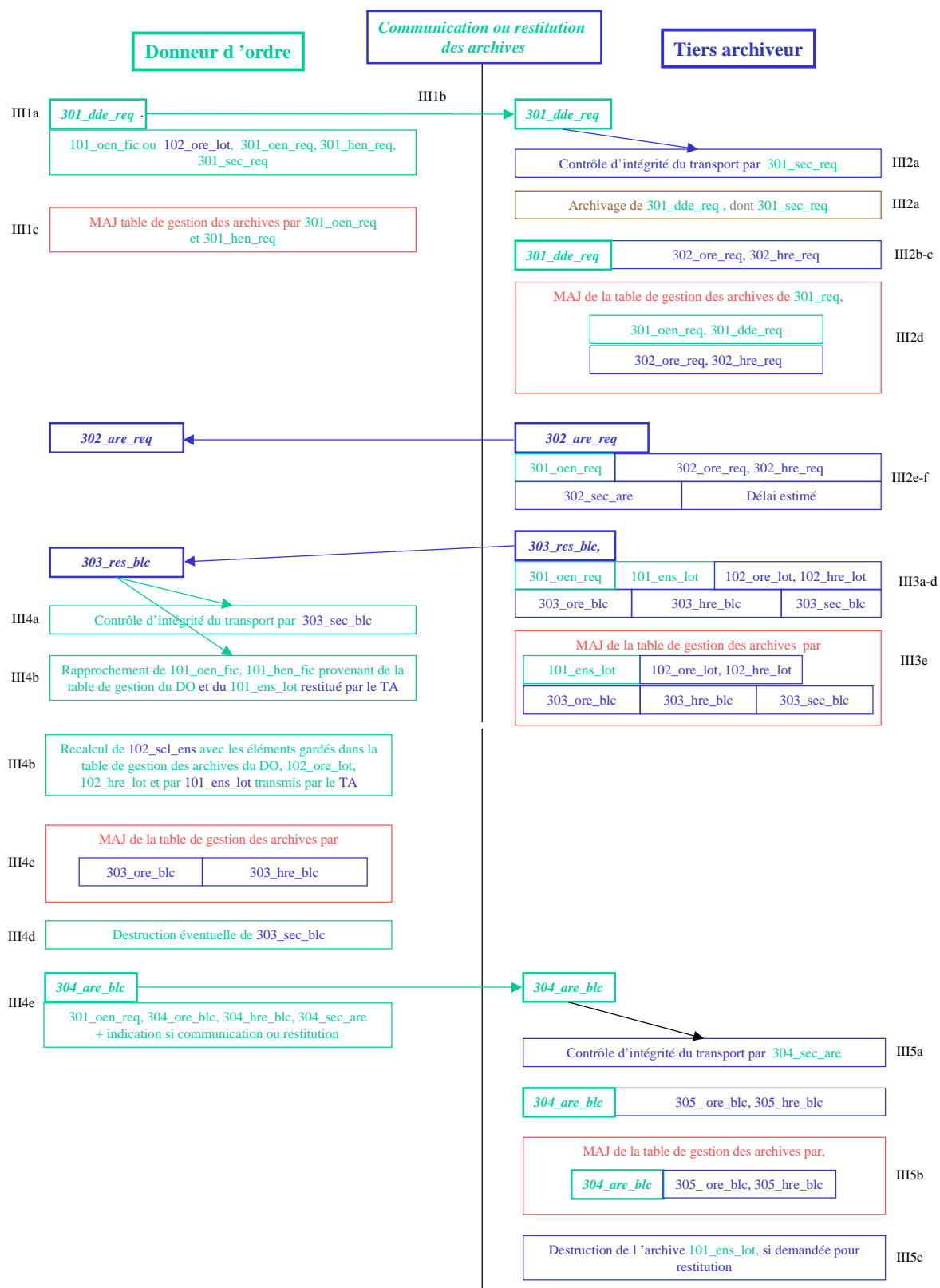


## Annexe 4 - Scénarii d'échanges

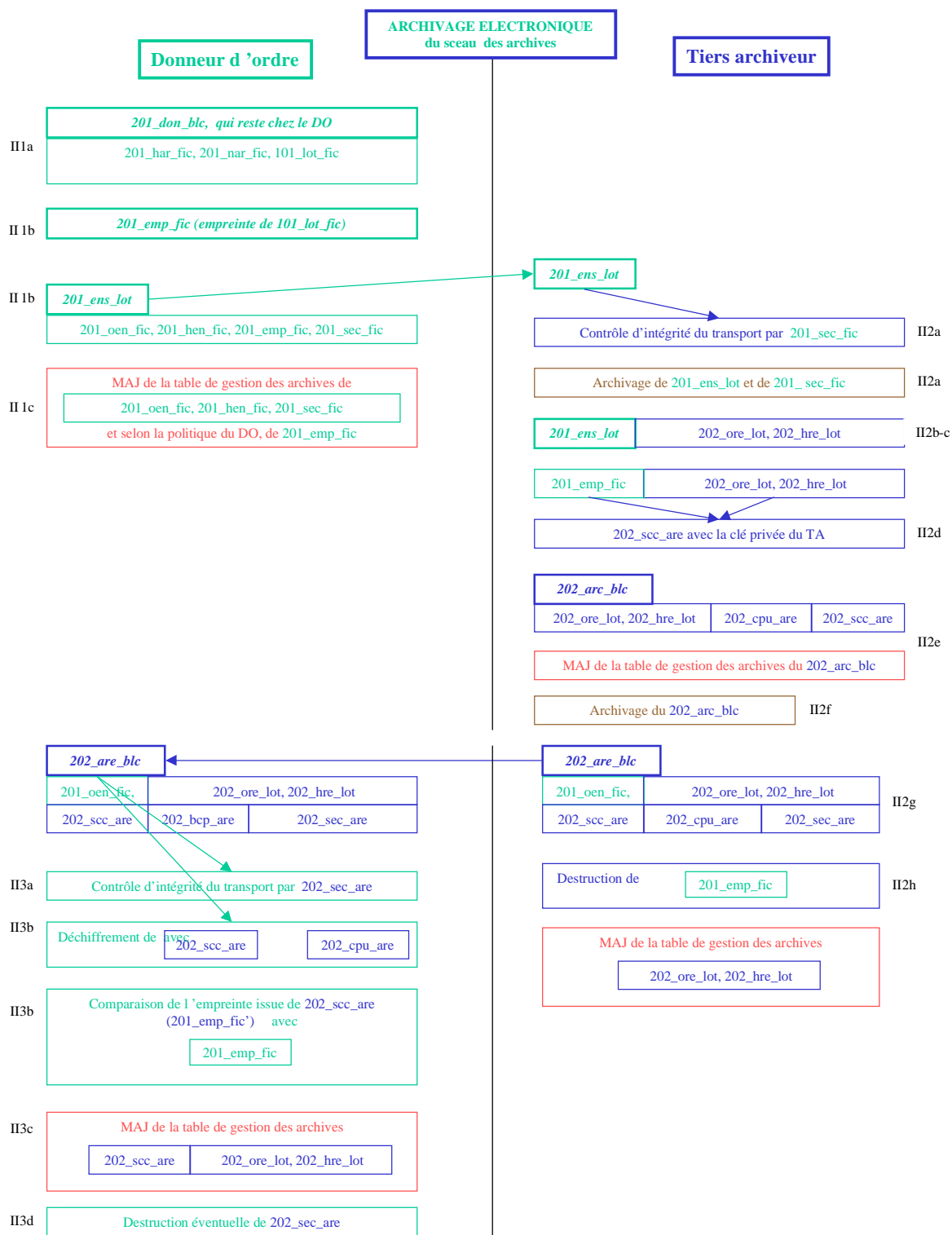
### Scénario I



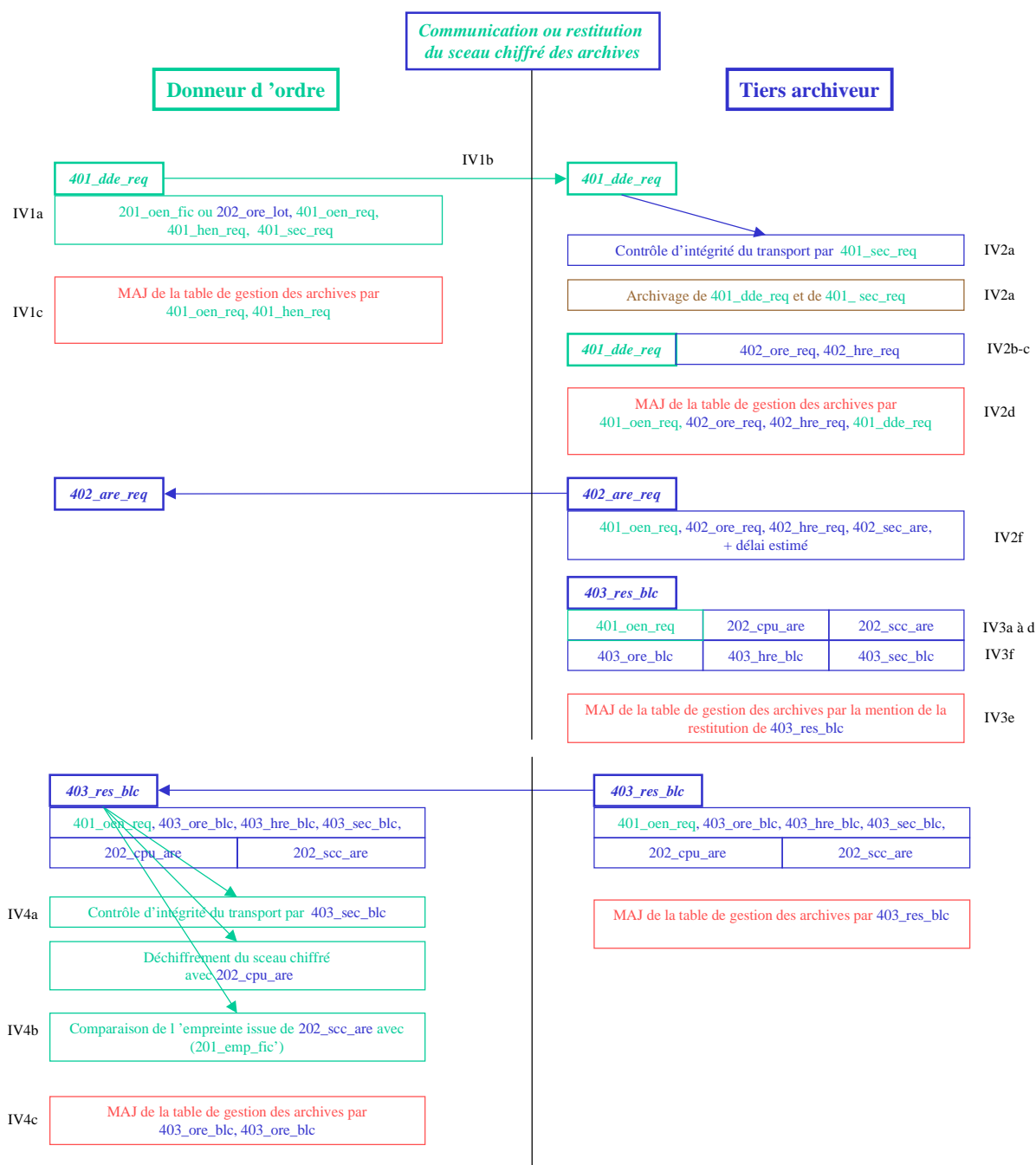
## Scénario III



## Scénario II



# Scénarii IV



## **Annexe 5 - Bibliographie**

**L'Archivage électronique.** Ordre des experts-comptables. Expert-comptable Média. Paris. 1999.

**Variations sur le thème du droit de l'archivage dans le commerce électronique,** E.A. Caprioli, Les petites affiches, n°164, 18 août 1999, p.4 s. (première partie), Les petites affiches, n°165, 19 août 1999, p.7 s. (deuxième partie).

**L'Archivage électronique des documents.** Guide Juridique Alain Bensoussan. Hermès. 1992.

**Echanges Electroniques - Certification et sécurité.** Thierry Piette Coudol. Editions LITEC. 2000.

**Norme AFNOR Z 42 013 :** Recommandations relatives à la conception et à la gestion des systèmes informatiques destinés à l'enregistrement de documents sous forme numérique sur disque optique de type WORM.

**Politique de certification type.** Version 2.0. 20 décembre 1999. Ministère de l'Economie, des Finances et de l'Industrie.

**Informatique et Telecoms.** Alain Bensoussan. Editions Francis Lefebvre. 1997-1999.

**Cryptologie et signature électronique, aspects juridiques.** Alain Bensoussan, Yves Leroux. Editions Hermès. 1999.



## Annexe 6 – Principaux textes applicables au 30 juin 2000

### Textes généraux :

- Loi n° 230-2000 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique,
- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et les articles 226-16 et suivants du code pénal,
- Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données du 24 octobre 1995,
- Loi n° 78-753 du 17 juillet 1978 modifiée portant diverses mesures d'amélioration des relations entre l'administration et le public,
- Loi n° 79-18 du 3 janvier 1979 modifiée sur les archives,
- Loi du 29 juillet 1881 sur la liberté de la presse (Art. 23 et suivants : provocation aux crimes et délits) ;

### • Code civil :

- Respect de la vie privée (Art. 9),
- Du dépôt et du séquestre (Art. 1915 et suivants) :
  - Etre en capacité de contracter,
  - Etre propriétaire de la chose déposée ou avoir donné son consentement exprès ou tacite,
  - Ne pas avoir volé ou détourné frauduleusement la chose,
  - Respecter l'entier paiement de ce qui est dû à raison du dépôt avant de pouvoir en obtenir restitution ;

### • Code pénal :

- Atteinte à la vie privée (Art. 226-1 et 226-2),
- Atteinte aux mineurs (Art. 227-23 et 227-24),
- Du vol (Art. 311-1 et suivants du code pénal),
- Des destructions, dégradations et détériorations (Art. 322-2 et 322-3 du code pénal),
- Des atteintes aux systèmes de traitement automatisé de données (Art. 323-1 et suivants du code pénal),
- De la livraison d'informations à une puissance étrangère (Art. 411-7 et 411-8),
- Du sabotage (Art. 411-9),
- Des atteintes au secret de la défense nationale (Art. 413-9 et suivants),
- Du terrorisme (Art. 421-1 et suivants) ;

### • Code de la propriété intellectuelle :

- Protection des logiciels (Art. L. 112-1 et L. 112-2),
- Droit d'auteur (Art. L. 113-1 et L. 113-9),
- Droits moraux (Art. L. 121-1 et suivants),
- Droits patrimoniaux (Art. L. 122-1 et suivants),

- Contrefaçon d'un logiciel (Art. L. 335-2 et suivants),
- Atteinte aux droits du producteur d'une base de données (Art. L. 341-1 et suivants),
- Contrefaçon d'un dessin ou d'un modèle (Art. L. 521-4 et suivants),
- Contrefaçon d'une marque (Art. L. 716-9 et suivants).

En outre, en matière de chiffrement, il convient de respecter les dispositions prévues par l'article 28 de la loi n° 90-1170 modifiée du 29 décembre 1990 sur la réglementation des télécommunications, et de ses décrets et arrêtés d'application de février et mars 1998 et de mars 1999.

