CFONB

Niveaux de services d'archivage électronique

Groupe de travail « Archivage électronique » - Groupe « Pratiques d'archivage »
- Année 2009-

Informations sur le document

Nom du document	GTPA-DEFINITION DES NIVEAUX DE SERVICES-T1.9.DOC

Versions

Version	Date	Auteur	Nature des modifications
T1.0	21/05/2008	Groupe de travail archivage	Version initiale
T1.1	12/06/2008	Groupe de travail archivage	Ajout des remarques de la réunion du 29/05/2008 : +§ Attestation +§ contrôles récurrents
T1.2	25/06/08	Groupe de travail archivage	Ajout des remarques de la réunion du 18/06/2008
T1.3	22/09/08	Groupe de travail archivage	Ajout introduction
T1.4	28/10/2008	Groupe de travail archivage	Ajout de la partie Horodatage
T1.5	20/11/2008	Groupe de travail archivage	Ajout de la définition de WORM cryptographique
T1.6	02/02/2009	Groupe de travail archivage	Prise en compte des remarques du GT
T1.7	26/03/2009	Groupe de travail archivage	Prise en compte de la version publiée de la Norme NF Z42-013
T1.8	27/04/2009	Groupe de travail archivage	Harmonisation du document avec le Sous-Groupe ID
T1.9	08/07/2009	Groupe de travail archivage	Prise en compte des remarques inter-bancaire
V1.1	25/01/2010	Groupe de travail archivage	Version validée

PLAN

1 Introduction

La démarche adoptée par le Groupe de Travail « Archivage Électronique » du CFONB a été définie en prenant en considération deux points de vue potentiellement antagonistes mais qui correspondent à deux préoccupations légitimes :

- la conformité à l'esprit et la lettre de la Loi,
- la mise en œuvre de moyens techniques, économiques et humains raisonnables.

Naturellement, cette double filiation s'est traduite par la constitution de deux sous-groupes : « Typologie documentaire » chargé de déterminer, pour les grandes familles d'Opérations bancaires, quels sont les documents concernés et, pour chacun d'eux, quelle « type de politique » doit lui être appliquée.
« Pratique d'archivage » chargé de déterminer les caractéristiques de différentes offres répondant à des besoins regroupés de manière cohérente en « niveaux de services».
Au final, la synthèse des travaux des deux sous-groupes est assurée par la mise en correspondances des « types de politique » et des « niveaux de services ».

Le sous-groupe de travail « Pratique d'archivage » s'est appuyé sur la norme NF Z 42-013 de Mars 2009 afin d'en dégager les principes directeurs à prendre en considération pour définir les différents « niveaux de services ». D'autre part, pour définir les niveaux, une approche en couches a été retenue, de sorte qu'une « couche supérieure » s'appuie totalement sur sa « couche inférieure » en apportant des fonctionnalités nouvelles plus contraignantes.

2 Définitions

Les extraits de norme figurant dans cet ouvrage sont reproduits avec l'accord d'AFNOR. Seul le texte original et complet de la norme telle que diffusée par AFNOR – accessible via le site Internet www.afnor.fr – a valeur normative.

Les citations de la Norme mentionnées dans ce document sont issues du texte de la Norme NF Z 42-013 de Mars 2009 – Indice de Classement Z 42-013 - ICS : 01.140.20 ; 35.240.30 homologué par décision du Directeur Général d'AFNOR le 4 février 2009 pour prendre effet le 4 mars 2009. Elle remplace la norme homologuée NF Z 42-013 de décembre 2001.

Autres définitions :

Objet
Un objet est constitué de
- L'archive (ex : document)
- Et de ses méta-données
  - Index
  - éléments de contexte (signature électronique, attestation, etc…)

Compte rendu
Le compte rendu est un rapport technique de la réalisation d'une action

Attestation
L'attestation, est un extrait des journaux, matérialisant des éléments de preuve.

WORM cryptographique
Il s'agit de supports réinscriptibles protégés par des moyens cryptographiques tels que l'objet soit infalsifiable : garantie d'intégrité.

Empreinte
« Ensemble de bits caractéristique d'un document numérique. L'empreinte est obtenue par une fonction de hachage. Toute modification du document numérique entraînera une empreinte différente qui révélera la modification par comparaison avec la première empreinte. » ([1])

Fonction de hachage
« Fonction qui fait subir une succession de traitements à une donnée quelconque fournie en entrée pour en produire une empreinte servant à identifier la donnée initiale. » ([2])

Unité de création d'attestations (UCA)
« Matériel et/ou logiciel permettant la délivrance d'attestations électroniques. Chaque attestation créée comporte l'identifiant de l'unité et du service d'archivage de l'organisme, ou de l'entreprise, ou du tiers archiveur. » ([3])

[1] *Selon terminologie retenue par la Norme NF Z 42-013 publiée en mars 2009 cf. page 9 – Chapitre 3 : Termes et définitions*
[2] *Selon terminologie retenue par la Norme NF Z 42-013 publiée en mars 2009 cf. page 10 – Chapitre 3 : Termes et définitions*
[3] *Selon terminologie retenue par la Norme NF Z 42-013 publiée en mars 2009 cf. page 11 – Chapitre 3 : Termes et définitions*

3 Principe général

Le principe est de présenter des niveaux de services d'archivage électronique, répondant chacun à des exigences en matière de sécurité. Le groupe de travail a opté pour quatre niveaux, numérotés de 0 à 3.

Niveau 0 : Pas encore de l'archivage à proprement parler, i.e. ***Conservation***.
Niveau 1 : Ce niveau apporte un premier niveau d'exigence en matière de ***traçabilité***
Niveau 2 : Ce niveau complète le niveau 1, en apportant des garanties d'***intégrité***
Niveau 3 : Ce niveau complète le niveau 2, en apportant des garanties d'***authenticité***

Les niveaux sont déclinés uniquement sur des fonctions discriminantes entre ceux-ci.
Toutes les applications remettantes devront être identifiées par le système d'archivage, et ce, dès le niveau 0.
Les autres fonctions, non précisées dans ce document, sont conformes aux dispositions préconisées dans la Norme N F Z42-013 Mars 2009.

4 Journalisation

4.1 La journalisation ([4])

« Un enregistrement doit être réalisé pour chaque événement lié à l'exploitation du système ou au cycle de vie des archives. Celui-ci doit être créé automatiquement par le système, horodaté en utilisant le temps UTC et enregistré de façon exhaustive et séquentielle dans les journaux correspondants.
Il doit être possible de lire les journaux de façon simple et leur exploitation doit être détaillée dans le dossier de description technique du système.
Les journaux doivent être archivés selon une périodicité et des conditions définies par la politique d'archivage dans des volumes de stockage assurant au moins la même pérennité et intégrité que les documents auxquels ils se rapportent.
Le journal des évènements ne doit pas être accessible aux opérateurs en temps normal, seul un responsable dûment habilité doit avoir accès à la gestion de ces journaux.
La journalisation conduit à la production d'attestations. Celles-ci doivent être archivées dans les mêmes conditions de conservation que les documents qu'elles concernent.

Selon le contexte d'exploitation du système d'archivage, WORM physique ou logique ou supports réinscriptibles protégés par des moyens cryptographiques, les journaux doivent permettre de démontrer la continuité de l'enregistrement des évènements soit par utilisation de supports WORM physique ou logique, soit par l'utilisation de supports réinscriptibles protégés par des moyens cryptographiques.

Les journaux doivent être conservés au même titre que les documents »

<u>Principes applicables à tous les niveaux de services</u>

- Le journal est créé automatiquement par le système
- Le journal est enregistré de façon séquentielle dans les journaux correspondants
- Il doit être possible de lire les journaux de façon simple et leur exploitation doit être détaillée dans le dossier de description technique du système
- Les journaux doivent être archivés selon une périodicité et des conditions définies par la politique d'archivage dans des volumes de stockage assurant au moins la même pérennité et intégrité que les documents auxquels ils se rapportent.
- Les journaux ne doivent pas être accessibles aux opérateurs en temps normal, seul un responsable dûment habilité doit avoir accès à la gestion de ces journaux.
- La journalisation conduit à la production d'attestations. Celles-ci doivent être archivées dans les mêmes conditions de conservation que les documents qu'elles concernent

[4] *Selon terminologie retenue par la Norme NF Z 42-013 publiée en mars 2009 cf. page 19 – Chapitre 5.6 : Journalisation*

4.2 Le journal du cycle de vie

4.2.1 Extrait de la Norme NF Z 42-013 ([5])

« Le journal de cycle de vie des archives peut être global ou spécifique par entité gérée.
Le journal de cycle de vie des archives comprend les attestations électroniques suivantes :

1. *attestation de prise en compte initiale d'un dépôt ;*
2. *attestation de prise en compte d'une modification de la durée d'un dépôt, le cas échéant ;*
3. *attestation de destruction anticipée ou à terme d'un dépôt, le cas échéant ;*
4. *attestation de restitution d'un dépôt, le cas échéant ;*
5. *attestation pour toute création, modification ou suppression d'un profil d'archivage.*

Le journal de cycle de vie des archives doit être mis à jour dès qu'une trace de création, modification ou suppression d'un profil d'archivage est générée ou qu'une nouvelle attestation électronique est générée.
Le journal du cycle de vie des archives doit pouvoir être consulté partiellement ou dans son intégralité par toute personne habilitée à effectuer une opération au titre d'un profil d'archivage.
Le service d'archivage d'un organisme, ou d'une entreprise, ou le tiers archiveur, doit fournir à toute personne habilitée à effectuer une opération au titre d'un profil d'archivage, les moyens lui permettant de vérifier l'intégrité et l'origine de toute partie ou de l'ensemble de ce journal.
Lors de chaque mise à jour, le service d'archivage d'un organisme, ou d'une entreprise, ou le tiers archiveur, doit mettre à disposition une donnée permettant aux personnes habilitées de vérifier l'intégrité de toute partie ou de l'ensemble de ce journal. »

4.2.2 Journal du cycle de vie par niveau de service

4.2.2.1 Journal du cycle de vie - Niveau 0

Ce niveau de journalisation permet de suivre le <u>bon fonctionnement du système d'archivage électronique</u>

4.2.2.1.1 Contenu

Dans ce niveau, seules des traces techniques sont écrites dans le journal.
Il s'agit des opérations techniques nécessaires au suivi de l'application (pilotage), et qui permettent de détecter d'éventuels dysfonctionnements, l'acquittement des traitements d'archivage, et la suppression d'archives.
Le niveau de détail de ces traces est variable, selon les établissements.

4.2.2.1.2 Sécurisation

Pas de condition particulière de conservation.
Le journal doit faire l'objet d'une sauvegarde selon la politique de sauvegarde du système d'archivage électronique.

[5] *Selon terminologie retenue par la Norme NF Z 42-013 publiée en mars 2009 cf. page 20 – Chapitre 5.6.2 : Journalisation du cycle de vie des archives*

4.2.2.1.3 Conditions de conservation

La **conservation de ces traces** peut-être limitée dans le temps, inférieure à la durée de l'archive.
Le choix du **support de conservation** de ces traces est laissé à l'appréciation des établissements.

4.2.2.2 Journal du cycle de vie - Niveau 1

Ce niveau de journalisation permet d'enregistrer les traces applicatives
Le niveau 1 apporte de nouvelles exigences par rapport au niveau 0.

4.2.2.2.1 Contenu

Le journal du cycle de vie de niveau 1 rend compte des opérations de :

- Création d'archive / **Dépôt**
- **Suppression** d'archive
- **Changement** de durée (prolongement) de l'archive
- **Restitution** d'une archive
- **Contrôles** correspondant à ceux du niveau de services.

Les consultations ne sont pas tracées.

Un évènement sur le cycle de vie, doit faire l'objet d'une trace dans le journal
Pour le niveau 1, chaque ligne du journal doit comporter au minimum :

- Une date fiable
- L'identifiant unique de l'archive
- Le type d'évènement

Lors de l'opération de dépôt, l'empreinte de l'objet archivé doit être consignée dans le journal si le support de stockage n'est pas de type WORM, elle servira notamment à vérifier l'intégrité de l'objet lors de sa consultation, ou de sa restitution.
En cas de stockage sur un support WORM, l'intégrité est assurée par le support : pas de dispositif particulier au niveau du journal.

4.2.2.2.2 Sécurisation

Pas de sécurisation particulière en dehors des dispositifs pris par la politique de sécurité des établissements.

4.2.2.2.3 Conditions de conservation

Sa durée de conservation est compatible avec celle des archives.

4.2.2.3 Journal du cycle de vie - Niveau 2

Le niveau 2 reprend les dispositions du niveau 1, en offrant de meilleures garanties en matière **d'intégrité**.

4.2.2.3.1 Contenu

Idem 4.2.2.2.1 +

- Si le document à archiver a une empreinte associée, alors le document et l'empreinte doivent être archivés.
- Si le document n'a pas d'empreinte associée, alors le système d'archivage doit calculer cette empreinte et archiver cette dernière avec le document
- L'empreinte de l'objet archivé doit être consignée systématiquement dans le journal, elle servira notamment à vérifier l'intégrité de l'objet lors de sa consultation, ou de sa restitution.
- En cas de contestation, le système doit permettre la comparaison entre l'empreinte archivée, l'empreinte calculée au moment de la restitution et l'empreinte consignée dans les journaux au moment de l'archivage.

Dans ce niveau de journalisation, les consultations sont tracées.

4.2.2.3.2 Sécurisation

Une empreinte (hash) est calculée par journal, elle forme la première ligne du journal (principe du chaînage des journaux). La fin d'un journal doit comprendre la date de clôture de ce dernier.

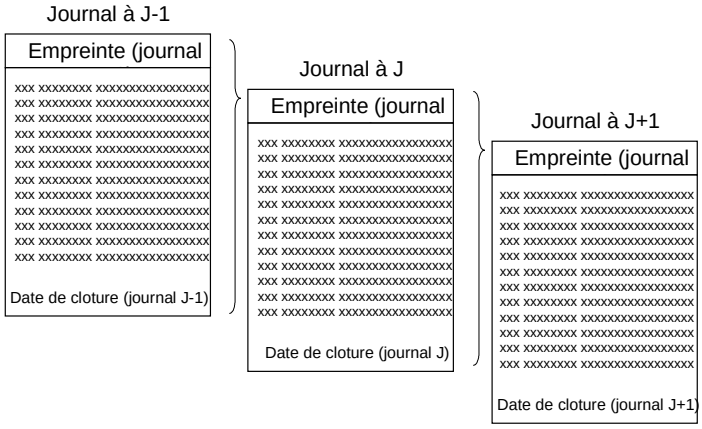


Figure 1: Principe de chaînage des journaux

4.2.2.3.3 Conditions de conservation

Chaque journal ainsi constitué sera archivé dans les mêmes conditions que les archives auxquelles il se rapporte.
Sa durée de conservation est égale au minimum à la durée maximum de la durée de conservation la plus longue de l'archive.
La conservation de ces journaux pourra aller au delà de la durée fixée, à des fin de traçabilité, dès lors que ces derniers ne permettent pas l'identification, la récupération ou la reconstitution de données personnelles définitivement effacées (ou devenues inaccessibles en cas d'archives historiques).

4.2.2.4 Journal du cycle de vie - Niveau 3

Le niveau 3 reprend les dispositions du niveau 2, en y apportant des garanties **d'authenticité**.

4.2.2.4.1 Contenu

Idem 4.2.2.3.1
+ *« Chaque attestation enregistrée dans le journal de cycle de vie des archives doit être signée par une UCA du système d'archivage de l'organisme, ou de l'entreprise, ou bien du tiers archiveur, au moyen d'une signature électronique. »* ([6])

- Les informations permettant de vérifier la signature électronique ne font pas partie de ce journal, et font l'objet d'une politique de conservation à part. « *Le service d'archivage de l'organisme, ou de l'entreprise, ou bien le tiers archiveur, doit indiquer, pour chaque politique d'archivage, la ou les politiques de signatures applicables aux ordres signés électroniquement par les personnes habilitées à effectuer des opérations au titre d'un profil d'archivage.»* ([7])

4.2.2.4.2 Sécurisation

Correspond au niveau de sécurisation le plus élevé, tel que spécifié dans la Norme NF Z 42-013 Mars 2009

4.2.2.4.3 Conditions de conservation

Les éléments permettant de vérifier les signatures électroniques devront être archivés en dehors du journal ; dans un système tiers, à l'intérieur ou à l'extérieur de l'établissement (tiers archiveur ou tiers de confiance)

---

[6] *Selon terminologie retenue par la Norme NF Z 42-013 publiée en mars 2009 cf. page 24 – Chapitre 9.2 : Niveau de sécurisation renforcé*
[7] *Selon terminologie retenue par la Norme NF Z 42-013 publiée en mars 2009 cf. page 24 – Chapitre 9.3 : Niveau de sécurisation avancé*

4.3 Le journal des évènements

4.3.1 Journal des évènements ([8])

« Le journal des évènements est unique par système et doit permettre de consigner qui a utilisé celui-ci (utilisateur humain ou système automatique), à quel moment, ce qui a été fait sur le système et quels en ont été les résultats. Les traces permettent ainsi de détecter qui a accédé au système, si le personnel a bien suivi les procédures ou si l'une des actions effectuées est susceptible d'être accidentelle, frauduleuse, malveillante ou non autorisée.

Ce journal se décompose en trois parties :

- *une partie pour les évènements relatifs à l'application d'archivage ;*
- *une partie pour les évènements relatifs à la sécurité ;*
- *une partie pour les évènements relatifs au système ;*

Le journal des évènements sert d'abord à des fins de contrôle interne et permet d'auditer l'ensemble des informations, messages d'erreur et autres avertissements générés durant le fonctionnement, comme les échecs ou au contraire le succès des opérations effectuées.

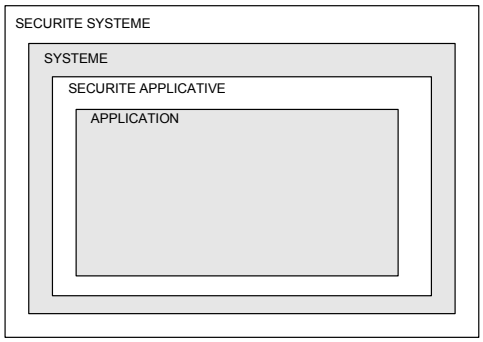
Pour les systèmes utilisant des supports de stockage de type WORM physique ou logique le journal des évènements doit consigner la création et la clôture de chaque support En cas de recopie d'un support sur un autre, le journal des évènements doit consigner cette opération de recopie

Les traces fournissent des moyens de confirmation du respect des procédures spécifiées et doivent comporter au minimum les informations suivantes pour chaque évènement significatif :

- *les dates et heures de l'opération conforme à la norme ISO 8601 ;*
- *l'opération effectuée ;*
- *l'identification du système technique qui a été utilisé ;*
- *le nom du processus en cause et l'indication de sa version ;*
- *le cas échéant, l'identification de l'opérateur. »*

Préambule

Nous distinguons la sécurité du système et de l'application selon le schéma suivant :



[8] *Selon terminologie retenue par la Norme NF Z 42-013 publiée en mars 2009 cf. page 20 – Chapitre 5.6.3 : Journal des évènements*

Périmètre des journaux d'évènements par niveau de service

Journal des évènements		NIVEAUX DE SERVICES D'ARCHIVAGE			
		0	1	2	3
APP (applicatif)		NON	**OUI**	**OUI**	**OUI**
SEC (Sécurité)	APP	NON	NON	**OUI**	**OUI**
	SYS	NON	NON	**OUI**	**OUI**
SYS (système)		NON	NON	NON	**OUI**

4.3.2 Journal des évènements par niveau de service

4.3.2.1 Journal des évènements - Niveau 0

Pas de journal des évènements au niveau 0.

4.3.2.1.1 Contenu

Non applicable

4.3.2.1.2 Sécurisation

Non applicable

4.3.2.1.3 Conditions de conservation

Non applicable

4.3.2.2 Journal des évènements - Niveau 1

Le journal des évènements n'enregistre les évènements **qu'au niveau applicatif**.

4.3.2.2.1 Contenu

- les dates et heures de l'opération conforme à la norme ISO 8601 ;
- l'opération effectuée ;
- l'identification du système technique qui a été utilisé ;
- le nom du processus en cause et l'indication de sa version ;

4.3.2.2.2 Sécurisation

Accès au journal soumis à autorisation conformément à la politique de sécurité en vigueur dans l'établissement.

4.3.2.2.3 Conditions de conservation

Idem 4.2.2.2.3 Journal du cycle de vie -Niveau 1.

4.3.2.3 Journal des évènements - Niveau 2

4.3.2.3.1 Contenu

Le journal des évènements enregistre les évènements **au niveau applicatif et au niveau sécurité (APP+SYS)**
De plus, il consigne les évènements liés à l'initialisation/ clôture du journal de cycle de vie, en faisant apparaître son empreinte.

4.3.2.3.2 Sécurisation

Idem 4.2.2.3.2.
Accès au journal soumis à autorisation conformément à la politique de sécurité en vigueur dans l'établissement.

4.3.2.3.3 Conditions de conservation

Idem niveau 2 du journal du cycle de vie (4.2.2.3.3)

4.3.2.4 Journal des évènements - Niveau 3

Le journal des évènements enregistre les évènements **sur tous les niveaux**.

4.3.2.4.1 Contenu

Idem 4.3.2.3.1, journal des évènements – Niveau 2.
+ Le journal des évènements enregistre les évènements :

- **au niveau applicatif (APP)**
- **au niveau sécurité (APP+SYS)**
- **au niveau système (SYS)**

4.3.2.4.2 Sécurisation

Accès au journal soumis à autorisation conformément à la politique de sécurité en vigueur dans l'établissement.

4.3.2.4.3 Conditions de conservation

Le journal est conservé dans les mêmes conditions que les archives auxquelles il se rapporte. Sa durée de conservation est égale au minimum à celle de l'archive, elle pourra aller bien au delà selon les contraintes réglementaires en vigueur.

4.4 Les attestations

Nota Bene : Une attestation peut revêtir un double sens :

- Un sens technique : compte rendu d'exécution, accusé de réception,…
- Un sens plus fonctionnel : Ensemble d'éléments justifiant de la qualité d'une archive, et qui en assure sa fiabilité

On ne traite ici que les attestations dans ce deuxième sens, la description des attestations techniques est propre à chaque établissement.

4.4.1 Les attestations de niveau 0

Pas d'attestation

4.4.2 Les attestations de niveau 1

L'attestation doit fournir à ce niveau de service, tous les éléments permettant de vérifier la traçabilité de l'archive (entre son dépôt, et la date de l'attestation).

L'attestation est un extrait du journal de cycle de vie de l'archive de niveau 1, avec toutes les informations disponibles dans ce niveau de journal.

L'attestation peut prendre différente forme selon les établissements.

4.4.3 Les attestations de niveau 2

L'attestation doit fournir à ce niveau de service, tous les éléments permettant de vérifier l'intégrité, la traçabilité de l'archive

L'attestation est un extrait du journal de cycle de vie de l'archive de niveau 2 avec toutes les informations disponibles dans ce niveau de journal.

L'attestation peut prendre différentes formes selon les établissements

4.4.4 Les attestations de niveau 3

L'attestation doit fournir à ce niveau de service, tous les éléments permettant de vérifier l'intégrité, la traçabilité, et l'authenticité de l'archive

L'attestation est un extrait du journal de cycle de vie de l'archive de niveau 3 avec toutes les informations disponibles dans ce niveau de journal.

L'attestation peut prendre différentes formes selon les établissements

5 Contrôles

Préambule
Les contrôles sont tracés systématiquement dans leur journal correspondant (cycle de vie ou journal des évènements)

5.1 Les contrôles sur évènement

5.1.1 Sur dépôt d'un objet à archiver

5.1.1.1 Niveau 0

APPLICATION DU CONTROLE	**Non applicable**
DEFINITION DU CONTROLE	**Non applicable**
EXEMPLE	**Non applicable**
ENREGISTREMENT	**Non applicable**

Détails :
Pas de détail.

5.1.1.2 Niveau 1

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	Le format de l'objet à archiver est un format pérenne et reconnu, les méta-données sont documentées, les spécifications du flux sont accessibles pour les audits (cf. paragraphe 5.2)
EXEMPLE	Formats pdf, TIFF, xml
ENREGISTREMENT	Le contrôle n'est pas tracé

Détails :
Le choix du format doit permettre de garantir que l'archive sera exploitable arrivé au terme de sa durée de conservation. Ce choix est fait en phase de spécification du flux à archiver.

5.1.1.3 Niveau 2

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	IDEM Niv. 1 + Contrôle de la conformité du format de l'objet à archiver par échantillonnage + Contrôle par échantillonnage de l'intégrité de l'objet à archiver + Contrôle systématique de l'exhaustivité du traitement d'un lot (le cas échéant)
EXEMPLE	Intégrité : comparaison entre l'empreinte calculée et l'empreinte transmise avec le flux
ENREGISTREMENT	Journal du cycle de vie de Niv. 2

Détails :
La méthode d'échantillonnage est définie dans la documentation applicative
L'empreinte de l'objet à archiver est réceptionnée par le SAE en même temps que l'objet à archiver
N.B : En cas d'utilisation de WORM cryptographique, ce contrôle est systématique

5.1.1.4 Niveau 3

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	IDEM Niv.2 + Contrôle systématique de la conformité du format de l'objet à archiver + Contrôle systématique de l'intégrité de l'objet à archiver + Contrôle de l'authenticité de l'objet à archiver
EXEMPLE	authenticité : Vérifier la signature électronique de l'ordre et de l'objet à archiver
ENREGISTREMENT	Journal du cycle de vie de Niv. 3

Détails :
Pas de détail.

5.1.2 Sur écriture d'une archive

5.1.2.1 Niveau 0

APPLICATION DU CONTROLE	**Non applicable**
DEFINITION DU CONTROLE	
EXEMPLE	
ENREGISTREMENT	

Détails :
Pas de détail.

5.1.2.2 Niveau 1

APPLICATION DU CONTROLE	**Applicable, journalisation uniquement**
DEFINITION DU CONTROLE	**Non applicable**
EXEMPLE	**Non applicable**
ENREGISTREMENT	Journal du cycle de vie de Niv.1

Détails :
Pas de détail.

5.1.2.3 Niveau 2

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	Comparaison par échantillonnage de l'empreinte de l'objet archivé avec l'empreinte reçue
EXEMPLE	Appliquer ce contrôle tous les 100 archives
ENREGISTREMENT	Journal du cycle de vie de Niv.2

Détails :

L'empreinte de l'archive est réceptionnée par le SAE en même temps que l'objet à archiver, il s'agit de vérifier par ce contrôle l'égalité des 2 empreintes.
La méthode d'échantillonnage est définie dans la documentation applicative
N.B : En cas d'utilisation de WORM cryptographique, ce contrôle est systématique

5.1.2.4 Niveau 3

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	Idem Niv.2
EXEMPLE	
ENREGISTREMENT	Journal du cycle de vie de Niv.3

Détails :

Pas de détail

5.1.3 Sur lecture d'une archive

5.1.3.1 Niveau 0

APPLICATION DU CONTROLE	**Non Applicable**
DEFINITION DU CONTROLE	
EXEMPLE	
ENREGISTREMENT	

Détails :

Pas de détail

5.1.3.2 Niveau 1

APPLICATION DU CONTROLE	**Non Applicable**
DEFINITION DU CONTROLE	
EXEMPLE	
ENREGISTREMENT	

Détails :

Pas de détail

5.1.3.3 Niveau 2

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	L'intégrité de l'objet archivé est vérifiée lors de la lecture, par comparaison de son empreinte au moment de la lecture avec l'empreinte reçue au moment de son archivage ; ce contrôle est appliqué par échantillonnage
EXEMPLE	
ENREGISTREMENT	Journal du cycle de vie de Niv.2

Détails :
En cas d'utilisation de WORM cryptographique, ce contrôle est systématique

5.1.3.4 Niveau 3

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	Idem Niv.2
EXEMPLE	
ENREGISTREMENT	Journal du cycle de vie de Niv.3

Détails :
Pas de détail.

5.1.4 Sur suppression d'une archive

La suppression d'une archive est appliqué quand :

- Un contrat est réalisé entre le déposant et l'archiveur, mentionnant explicitement dans quel cas et à quel moment la suppression d'une archive sera faite.
- Un ordre explicite de suppression est donné à l'archiveur

Le donneur d'ordre est clairement identifié et dûment habilité.
Ex : Son nom et son rôle sont mentionnés dans le contrat entre les parties

5.1.4.1 Niveau 0

APPLICATION DU CONTROLE	**Non applicable**
DEFINITION DU CONTROLE	
EXEMPLE	
ENREGISTREMENT	

Détails :

Pas de contrôle, mais la demande de suppression fait l'objet d'un support écrit :

- Formulaire,
- Mèl,
- Contrat de service entre le remettant et l'archiveur
- La date de suppression est une méta-donnée de l'archive

Cet écrit n'est nécessairement conservé.

5.1.4.2 Niveau 1

APPLICATION DU CONTROLE	**Applicable, journalisation uniquement**
DEFINITION DU CONTROLE	
EXEMPLE	
ENREGISTREMENT	Journal de cycle de vie de Niv.1

Détails :

Idem Niv.0
+ Cet écrit est conservé pour une durée égale au minimum à celle de l'archive concernée et dans des conditions de conservation compatibles avec les objets archivés.

5.1.4.3 Niveau 2

APPLICATION DU CONTROLE	**Applicable, journalisation uniquement**
DEFINITION DU CONTROLE	
EXEMPLE	
ENREGISTREMENT	Journal de cycle de vie de Niv.2

Détails :

Idem Niv.1

5.1.4.4 Niveau 3

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	L'ordre de suppression est authentifié par vérification de sa signature électronique. La vérification est tracée.
EXEMPLE	
ENREGISTREMENT	Journal de cycle de vie de Niv.3

5.1.5 Sur restitution d'une archive

5.1.5.1 Niveau 0

APPLICATION DU CONTROLE	**Non applicable**
DEFINITION DU CONTROLE	
EXEMPLE	
ENREGISTREMENT	

Détails :
Pas de détail.

5.1.5.2 Niveau 1

APPLICATION DU CONTROLE	**Applicable, journalisation uniquement**
DEFINITION DU CONTROLE	
EXEMPLE	
ENREGISTREMENT	Journal de cycle de vie de Niv.1

Détails :
La restitution est tracée dans le journal correspondant

5.1.5.3 Niveau 2

APPLICATION DU CONTROLE	**Applicable, journalisation uniquement**
DEFINITION DU CONTROLE	
EXEMPLE	
ENREGISTREMENT	Journal de cycle de vie de Niv.2

Détails :
La restitution est tracée dans le journal correspondant

5.1.5.4 Niveau 3

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	L'ordre de restitution est authentifié par la vérification de sa signature électronique
EXEMPLE	
ENREGISTREMENT	Journal de cycle de vie de Niv.3

Détails :
La restitution et la vérification de son authenticité sont tracées dans le journal correspondant.

5.1.6 Sur migration d'une archive

5.1.6.1 Niveau 0

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	Vérification de l'exhaustivité de la migration
EXEMPLE	xxxx archives dans le SAE avant migration = xxxx archives dans le nouveau SAE après migration.
ENREGISTREMENT	Journal de cycle de vie de Niv.0

Détails :
Pas de détail.

5.1.6.2 Niveau 1

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	Calcul de l'empreinte avant et après migration pour chaque objet archivé + génération et archivage d'un rapport de migration dans les mêmes conditions que les archives et pour une durée égale à la durée de vie de l'application
EXEMPLE	
ENREGISTREMENT	Journal de cycle de vie de Niv.1

Détails :
Pas de détail.

5.1.6.3 Niveau 2

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	Idem Niv.1
EXEMPLE	
ENREGISTREMENT	Journal de cycle de vie de Niv.2

Détails :
Pas de détail.

5.1.6.4 Niveau 3

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	Idem Niv.2
EXEMPLE	
ENREGISTREMENT	Journal de cycle de vie de Niv.3

Détails :
Pas de détail.

5.1.7 Sur création, modification, suppression d'un profil d'archivage

Seules les personnes dûment habilitées conformément à la politique de sécurité de l'établissement peuvent créer, modifier, ou supprimer un profil d'archivage.

Chacune de ces actions doit faire l'objet d'une journalisation dans le journal des évènements du niveau de service correspondant.

5.2 Les contrôles récurrents

5.2.1 Niveau 0

Pas de contrôle spécifique, les contrôles récurrents internes sont ceux pratiqués par les établissements conformément à leur politique.

Ex : Audit système à chaque montée de version logicielle, etc…

5.2.2 Niveau 1

L'établissement contrôle que les procédures définissant les niveaux de services sont respectés.

5.2.3 Niveau 2

Idem Niv.1

+

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	▪ Des audits **internes** sont pratiqués conformément aux dispositions de la Norme NF Z 42-013 Mars 2009 ▪ L'intégrité du stock est contrôlée par échantillonnage
EXEMPLE	
ENREGISTREMENT	Journal de cycle de vie de Niv.2

Détails :

La méthode d'échantillonnage est définie dans la documentation applicative

5.2.4 Niveau 3

APPLICATION DU CONTROLE	**Applicable**
DEFINITION DU CONTROLE	▪ Des audits internes sont pratiqués conformément à la Norme NF Z 42-013 Mars 2009 ▪ Des audits **externes** sont pratiqués conformément à la Norme NF Z 42-013 Mars 2009 ▪ L'intégrité du stock est contrôlée de façon exhaustive
EXEMPLE	
ENREGISTREMENT	Journal de cycle de vie de Niv.3

Détails :

Ex : Tous les mois, l'intégrité d'un douzième du stock d'archive est vérifiée. Ainsi, au bout d'un an, tout le stock sera contrôlé.

La périodicité des contrôles assurant la couverture complète peut varier selon les applications, notamment selon le volume des archives. Elle est fixée par l'établissement

6 Horodatage

Nota Bene : L'objet archivé peut contenir des éléments de preuve intrinsèquement.

La source de temps est considérée comme fiable à partir du niveau 0. Néanmoins, cette fiabilité est augmentée avec les niveaux de services, jusqu'à obtenir une preuve d'antériorité.

6.1 Niveau 0

Les dates et heures utilisées sont celles du **système**.
La fiabilité de l'horodatage est garantie par la politique interne de chaque établissement.

6.2 Niveau 1

Idem Niv.0

6.3 Niveau 2

Les dates et heures utilisées sont **certaines**, elles sont synchronisées avec une source de temps fiable, externe à l'application/système, et interne à l'entreprise.
Ex : Synchronisation avec un serveur de temps via le protocole NTP (Network Time Protocol)

6.4 Niveau 3

A ce niveau, l'horodatage est **sécurisé** par :

- Une signature électronique
- Une horloge fiable

} Jeton d'horodatage

Le mécanisme d'horodatage est différent du système d'archivage électronique.
Il est *a minima* interne à l'entreprise, et pourra selon les besoins être externe, i.e. « tiers horodateur ».
Les jetons d'horodatage doivent être conservés dans les mêmes conditions que les archives auxquelles ils se rapportent. Leur durée de conservation pourra excéder la durée prévue pour l'archive.

-FIN DU DOCUMENT-