LE
PRESIDENT

REFERENTIEL DEFINISSANT UN COFFRE-FORT ELECTRONIQUE POUR L'ARCHIVAGE A VOCATION PROBATOIRE D'OBJETS NUMERIQUES

Version 2010 / 11-6

Pour : Dominique Calmes
Diffusé le 5 novembre 2010 par la FNTC
La FNTC autorise le destinataire à utiliser cette copie exclusivement pour son usage personnel en vue d'une éventuelle candidature de son organisation à la labellisation FNTC-CFE

Sommaire

1. Suivi du document

Version	Date
V 1-0	10/01/2006
V2-0	15/01/2006
V2-1	26/01/2006
V3-0	16/02/2006
V4-0	03/02/2006
V5-0	10/02/2006
V6-0	11/06/2006
V7-0	25/10/2006
V7-1	28/10/2006
V7-2	07/11/2006
V7-3	07/12/2006
V7-4	26/12/2006
V8-0	20/03/2007
V9-1	20/05/2008
V9-2	23/05/2008
V9-3	20/06/2008
V9-4	19/07/2008
V10-1	25/10/2008
V10-2	28/10/2008
V10-3	19/11/2008
V11-1	16/12/2008
V11-2	14/01/2009
V11-3	05/02/2009
V 11-4	09/02/2009
V 11-5	11/02/2009
V 11-6	25/01/2010 (changement de logo et insertion *copyright*)

Le présent référentiel a été initialisé par un groupe de travail inter associations (FNTC, APROGED, FEDISA, ADAP).
La Fédération Nationale des Tiers de Confiance a finalisé ce référentiel en intégrant les apports de la norme NF Z42-013 : 2009.

2. Avant-propos

2.1. Les besoins en matière de conservation d'objets numériques

Le besoin de conservation des objets numériques, à plus ou moins long terme, c'est à dire de quelques heures à plusieurs centaines d'années, est lié à diverses considérations d'ordre réglementaire, juridique, patrimonial, historique. Parmi les objets numériques figurent notamment les données numériques et les documents dématérialisés ou nativement électroniques.

Dans ce contexte, la conservation doit prendre en compte trois besoins clés :

- L'authenticité ;
- L'intégrité ;
- La traçabilité.

Le Coffre-fort électronique a pour but de répondre à ces trois besoins clés.

2.2. Le concept de Coffre-fort électronique

Le Coffre-fort électronique est un composant fondamental qui permet d'assurer la conservation des objets numériques et leur valeur probatoire.

Un Coffre-fort électronique est un outil qui permet :

- Le contrôle de l'intégrité des objets numériques qu'il archive ;
- La tenue d'inventaire des objets numériques archivés ;
- Le contrôle des dépôts de ces objets, de leur lecture et de leur destruction ;
- La production et l'archivage sécurisé de journaux de l'ensemble de ces activités.

Le terme Coffre-fort électronique recouvre des outils ou des implémentations différentes. En effet, un Coffre-fort électronique peut être destiné à archiver des données pour quelques années (par exemple des documents comme les factures émises vers des clients ou les factures reçues des fournisseurs) ou plus de 100 ans (par exemple des données médicales).

L'implémentation d'un Coffre-fort électronique peut être très différente en matière de sécurisation des données dans le temps.

Par exemple, pour des enregistrements de télécommunication, il faut la combinaison d'une forte confidentialité et des délais de conservation courts (quelques mois). A contrario, les registres de brevets, le journal officiel ou le cadastre nécessitent une forte intégrité à long terme et une garantie de l'authenticité sans besoin de forte confidentialité.

Le but du présent référentiel est de définir des fonctions minimales garantissant la conservation sécurisée, l'intégrité et l'interopérabilité entre des Coffres-forts électroniques d'éditeurs différents.

Le référentiel permet la conception et l'exploitation de Coffres-forts électroniques adaptés aux différents contextes évoqués ci-dessus.

2.3. Définition du niveau de base

Le présent référentiel définit un niveau de base que tout Coffre-fort électronique doit posséder pour assurer les fonctions minimales qui sont nécessaires à la bonne conservation sécurisée d'objets numériques.

Toutes les fonctions spécifiées du § 7 « Exclusions » au § 17 « Statistiques d'utilisation » doivent être supportées par un Coffre-fort électronique qui se veut conforme au présent référentiel.

Les éditeurs de Coffres-forts électroniques peuvent proposer des fonctions complémentaires, qui ne sont pas comprises dans le présent référentiel, afin de fournir une valeur ajoutée qui leur est propre. L'implémentation de ces fonctions complémentaires est libre. Cependant ces fonctions ne doivent en aucun cas être incompatibles avec les fonctions définies dans le présent référentiel et nuire ou compromettre la conservation sécurisée des objets numériques. Si ces fonctions complémentaires sont journalisées, cette journalisation doit être conforme aux spécifications du § 12 « Enregistrement des actions dans le Coffre-fort électronique ».

2.4. Extensions futures du niveau de base

Dans le futur, il pourra bien évidemment exister de nouvelles versions du présent référentiel pour ajouter des fonctions au niveau de base défini ici. Ces futures versions comporteront obligatoirement :

- Une mesure d'impact sur les objets numériques qui sont stockés dans les précédentes versions du Coffre-fort électronique ;
- Un paragraphe précisant les évolutions de la nouvelle version par rapport à la précédente version ;
- Les mesures à prendre pour mettre en conformité les Coffres-forts électroniques en exploitation lors de la publication de la nouvelle version du référentiel.

3. Remerciements

Le présent référentiel s'inscrit dans la continuité des travaux menés depuis 2006 par un groupe inter-associations FNTC/Fedisa/Adap/Aproged notamment représenté par : Arnaud Belleil (Cecurity.com), Gabriel Gil (GLI Services), Christophe Godeau (Docubase), Jean-Louis Pascon (Henon Conseil).

La présente version est l'œuvre des membres actifs du groupe de travail Archivage de la Fédération Nationale des Tiers de Confiance.

Comité éditorial :

M.	Alain	Borghesi	Cecurity.com
M.	Denis	Bourdillon	Pitney Bowes Asterion
M.	Marc	Chédru	Marc Chédru Conseil
M.	Eric	Descours	Docubase
M.	Gabriel	Gil	GLI Services
M.	Jean-Jacques	Milhem	Atos Worldline
M.	Lucien	Poulain	ORSID Groupe La Poste
M.	Bruno	Ricci	Cecurity.com

4. Documents de référence

Le présent document fait référence aux documents suivants :

Référence	Titre
RFC 3174	Secure Hash Algorithm 1 (SHA-1)
FIPS 180-2	Secure Hash Algorithm 256 (SHA-256) Federal Information Processing Standards Publication 180-2
ISO 14721	Systèmes de transfert des informations et données spatiales - Système ouvert d'archivage de l'information (OAIS)
RFC 3161	Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)
RFC 2459	Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
NF EN 28601	Éléments de données et formats d'échange - Échange d'information - Représentation de la date et de l'heure
RFC 4998	Evidence Record Syntax (ERS)
ISO 8859-1	Traitement de l'information - Jeu de caractères graphiques codés sur un seul octet
ISO/CEI 10646	Technologies de l'information - Jeu universel de caractères codés sur plusieurs octets (JUC)
NF Z42-013 : 2009	Version 2009 de la norme française de l'archivage électronique de documents. Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes.

5. Vocabulaire

Le vocabulaire suivant est applicable au présent référentiel.

Nom	Définition
Objet	Train de bits numériques qui peut être stocké dans un Coffre-fort électronique
Document numérique	Ensemble composé d'un contenu, d'une structure logique, d'attributs de présentation permettant sa représentation, exploitable par une machine afin de restituer une version intelligible pour l'homme. Le document numérique peut être créé à l'état natif ou obtenu par un processus de transformation d'un document physique, on parle dans ce cas de document numérisé (définition norme AFNOR NF Z42-013 : 2009).
IDU	**Id**entification **U**nique d'un objet dans un Coffre-fort électronique
Dépôt	Fourniture au Coffre-fort électronique d'un objet numérique pour conservation sécurisée
Lecture (Mise à disposition)	Fourniture d'une copie conforme d'un objet contenu dans un Coffre-fort électronique, l'objet étant conservé dans le Coffre-fort électronique
Élimination (suppression)	Suppression complète d'un objet contenu dans un Coffre-fort électronique avec maintien obligatoire de toutes les traces relatives à cet objet dans le Coffre-fort électronique
Restitution	Lecture d'un objet suivie de l'Elimination de celui-ci dans un Coffre-fort électronique accompagné de ses éléments de preuve
Vidage	Restitution de la totalité des objets contenus dans un Coffre-fort électronique.
Intégrité	Invariabilité, au bit près, d'un objet numérique dans le temps
Inventaire	Liste exhaustive de tous les objets numériques contenus dans un Coffre-fort électronique
Empreinte	Séquence de bits, qui caractérise un objet numérique et dont la valeur est unique pour cet objet numérique. Cette séquence est produite par un algorithme de hachage standard. Toute modification du document numérique entraînera une empreinte différente qui révélera la modification par comparaison avec la première empreinte. **Nota** : à partir d'une empreinte donnée, il est impossible de reconstituer l'objet numérique qui lui est associé.

Dossier Technique du Système	Dossier regroupant tous les éléments permettant la compréhension du fonctionnement, les pré-requis pour son fonctionnement, le paramétrage et l'exploitation d'un Coffre-fort électronique
Déposant	Celui (personne ou système) qui réalise le dépôt d'un objet numérique dans un Coffre-fort électronique
Demandeur	Celui (personne ou système) qui souhaite obtenir, d'un objet contenu dans un Coffre-fort électronique, une Lecture, un Vidage, une Restitution ou une Elimination
Contremarque de temps	Donnée qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là (définition norme AFNOR NF Z42-013 : 2009).
Horodatage	Information permettant de démontrer qu'une donnée (par exemple, un document, un enregistrement d'audit ou une signature électronique) existait à un instant donné (définition norme AFNOR NF Z42-013 : 2009).
Métadonnée	Ensemble structuré d'informations techniques, de gestion et de description attaché à un document servant à décrire les caractéristiques de ce document en vue de faciliter son repérage, sa gestion, son usage ou sa préservation (définition norme AFNOR NF Z42-013 : 2009).
Scellement numérique	Procédé permettant de garantir, l'intégrité d'un document par l'utilisation conjointe de calculs d'empreintes, de signatures numériques et d'horodatage (définition norme AFNOR NF Z42-013 : 2009).
Traçabilité	Informations collectées et horodatées lors de chaque action réalisée dans un Coffre-fort électronique. Toute altération de ces informations doit être détectable.
Archivage électronique	Contexte et principe directeur de la pérennisation d'objets numériques
SIP	*Submission Information Package* (définition OAIS - ISO 14721)
AIP	*Archival Information Package* (définition OAIS)
DIP	*Dissemination Information Package* (définition OAIS)

6. Introduction

Le présent document a pour but de définir les fonctionnalités minimales que doit posséder un système de Coffre-fort électronique destiné à la conservation sécurisée d'objets numériques.

6.1. Architecture du Coffre-fort électronique

Au sens du présent référentiel, un Coffre-fort électronique peut être :

- Un progiciel exploité sur une ou plusieurs plate-forme(s) matérielle(s) ;
- Un ensemble progiciel et matériel exploité comme un tout.

6.2. Objets numériques

Au sens du présent document, un objet numérique est un train de bits.

Cet objet numérique peut être constitué d'un fichier simple ou d'un fichier agrégat.

A titre d'exemple, un objet numérique simple peut être constitué d'un fichier image au format TIFF ou d'une facture au format PDF intégrant sa signature électronique. Un agrégat peut être constitué d'un dossier d'étude comportant des plans, des cartes, des documents au format PDF, ou d'une facture accompagnée de sa signature électronique.

Par ailleurs, cet objet numérique peut contenir des métadonnées nécessaires à son indexation.

6.3. Fonctions du Coffre-fort électronique

Les principales fonctions d'un Coffre-fort électronique, au sens du présent référentiel, sont les suivantes :

- Les fonctions ayant trait à la gestion d'un objet numérique (Déposer, Lire et Éliminer) ;
- Les fonctions liées au contrôle de l'intégrité de chaque objet numérique qui est conservé au sein d'un Coffre-fort électronique ;
- Les fonctions ayant trait à l'administration globale du Coffre-fort électronique, comme la gestion et le contrôle des accès, la journalisation sécurisée des actions dans le Coffre-fort électronique relatives aux opérations sur les objets numériques qui y sont stockés.

6.4. OAIS

Le présent référentiel couvre les aspects suivants du modèle OAIS.

Domaines	Fonctions	Couverture
Preservation Planning	Suivre les développements technologiques et formuler des recommandations par rapport aux standards et à la politique d'archivage	Non
	Surveiller les efforts de recherche faits en matière d'archivage	Non
	Formulation de recommandations pour le maintien de la lisibilité de l'information stockée	Non
	Planification de migrations de données et de processus de copie	Non

Domaines	Fonctions	Couverture
Ingest	Prise en charge des SIP (Submission Information Packages) créés par le producteur	Oui
	Contrôle de l'intégralité et de l'intégrité	Oui
	Transformation des SIP en AIP (*Archival Information Packages*)	Oui L'AIP correspond à l'objet qui est conservé par le système d'archivage. Le format dans lequel cet objet est conservé peut être différent du format d'entrée ou de sortie et donc même si un Coffre-fort électronique doit restituer à l'identique les objets reçus il peut les conserver dans un format plus approprié.
	Extraction de l'information descriptive pour la base de données de recherche	Non
	Transmission des AIP à la mémoire d'archive	Oui
	Communication au Data Management	Oui
Data Management	Gère les informations descriptives (base de données) qui identifient les fonds d'archives et les documents, ainsi que d'autres données nécessaires à l'utilisation du matériau d'archives	Non
	Réception et traitement des demandes (queries)	Oui (mais uniquement sur l'IDU)
Archival Storage	Conservation et maintien des AIP	Oui
	Création de backup	Oui
	Contrôle régulier de l'intégrité des données	Oui
	Mécanismes automatiques de recréation d'objets numériques à partir de copies et/ou de backup	Oui
	Transmission des AIP à la fonction Access pour l'utilisation	Oui
Access	Interface utilisateur	Oui
	Permettre la recherche et générer des réponses contenant la description des AIP et des informations quant à leur disponibilité	Oui partiel (pas de recherche sur des métadonnées d'indexation propres à chaque objet numérique)

Domaines	Fonctions	Couverture
	Réception et traitement de demandes de données (requests) Transformation des AIP en DIP (Dissemination Information Packages) et livraison des DIP aux utilisateurs	Oui pour la réception et le traitement des requêtes. Oui pour la transformation des AIP en DIP (Voir le commentaire relatif aux « ingest » en début de tableau OAIS) Oui pour la livraison des DIP aux utilisateurs
	Garantie du respect des droits d'accès	Oui
Administration	Contrôle des processus globaux dans OAIS et de ses relations extérieures	Non
	Configuration du matériel et du logiciel	Non
	Attribution de droits d'accès	Oui

6.5. Norme française de l'archivage électronique NF Z42-013

Le présent référentiel s'appuie sur la norme française de l'archivage électronique dont le titre est : « Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes »

Extraits de l'introduction de la norme AFNOR Z42-013 : 2009 :

« La norme Z42-013 a été rédigée pour permettre aux organismes ainsi qu'aux entreprises de se référer à des principes et des procédés éprouvés et validés […] pour l'enregistrement, l'archivage et la communication de leurs documents numériques.
[…]
Elle définit les critères auxquels doit répondre la conception de ces systèmes et spécifie les procédures pour leur exploitation.

Ces spécifications visent à garantir que des documents numériques soient capturés, archivés, restitués et communiqués de façon à ce qu'il soit possible de s'assurer que le document archivé garde la même valeur que le document d'origine pendant toute la durée de conservation.
[…]
Pour les supports réinscriptibles, la garantie d'intégrité est assurée par des moyens cryptographiques caractérisés notamment par le calcul d'une empreinte, d'une contremarque de temps ou d'une signature électronique. »

Les moyens cryptographiques utilisés par les Coffres-forts électroniques devront être conformes à ceux de la norme.

7. Exclusions

7.1. Environnement et exploitation du Coffre-fort électronique

Le présent référentiel ne traite pas de l'environnement qui peut être nécessaire à l'exploitation du Coffre-fort électronique, comme les moyens de protection physique (système d'extinction des incendies, portes blindées, détecteurs de présence, etc.), les moyens de sécurisation de l'alimentation électrique (groupes électrogènes et onduleurs) ou encore les lignes de télécommunication.

Le présent référentiel ne traite pas non plus des procédures d'exploitation d'un Coffre-fort électronique, celles-ci sont de la responsabilité de l'exploitant de celui-ci.

7.2. Métadonnées

Les métadonnées associées aux objets numériques nécessaires à l'indexation de ceux-ci (métadonnées dites descriptives) n'entrent pas dans le champ du présent référentiel.

En conséquence, les aspects liés à la recherche des objets numériques contenus dans un Coffre-fort électronique ne sont pas inclus dans le présent référentiel, l'accès se faisant au minimum par un identifiant unique (IDU) que le Coffre-fort électronique attribue à chaque objet numériques lors du dépôt de cet objet.

L'utilisateur d'un Coffre-fort électronique conforme au présent référentiel doit mettre en œuvre des outils complémentaires (par exemple un logiciel de gestion électronique de documents) pour rechercher les objets numériques. La liaison entre le Coffre-fort électronique et l'outil d'indexation et de recherche est réalisée via l'IDU.

En revanche, le Coffre-fort électronique doit posséder au minimum des métadonnées techniques pour chaque objet numérique qui décrivent l'état de celui-ci au sein du Coffre-fort électronique comme la date de dépôt, la date de la dernière vérification d'intégrité, l'appartenance à une zone de stockage/service, etc.

7.3. Dépôts des objets numériques

Le présent référentiel ne définit pas :

- La constitution de l'objet numérique à conserver (le présent référentiel ne précise pas les opérations nécessaires à la constitution d'AIP à partir des SIP) ;
- L'exploitation de métadonnées d'indexation et leur éventuelle transmission vers un outil de gestion/indexation ;
- L'utilisation éventuelle de logiciels pour tester la validité des formats des objets numériques ;
- Les éventuelles conversions de formats des objets numériques avant leur dépôt.

7.4. Gestion des sauvegardes

La gestion de sauvegardes de sécurité d'un Coffre-fort électronique n'entre pas dans la couverture fonctionnelle du présent référentiel et plus précisément :

- La production de sauvegardes d'un Coffre-fort électronique ;
- La reconstitution partielle ou totale du contenu d'un Coffre-fort électronique à partir de ces sauvegardes.

Cependant, après reconstitution partielle ou totale du contenu d'un Coffre-fort électronique à partir de sauvegardes, le Coffre-fort électronique doit disposer d'outils qui permettent de s'assurer que l'intégrité des objets numériques a été préservée lors cette reconstitution.

7.5. Fourniture des objets numériques

La mise en forme des objets numériques lors de la Lecture ou de la Restitution ne fait pas partie de la couverture fonctionnelle du présent référentiel (au sens OAIS, pour un Coffre-fort électronique les DIP sont identiques aux AIP).

7.6. Contraintes

Toutes les exclusions précédentes ne doivent pas avoir d'incidences sur les objets numériques, l'intégrité de ceux-ci et la traçabilité des actions sur ceux-ci.

8. Modes de fonctionnement des dépôts

8.1. Définition

Un Coffre-fort électronique doit pouvoir fonctionner suivant deux modes :

- Mode "non contrôlé" : le déposant fournit l'objet numérique à stocker sans empreinte associée. Aucun contrôle d'intégrité n'est réalisé lors de la réception ;
- Mode "contrôlé" : le déposant fournit l'objet numérique à stocker accompagné d'une empreinte de ce dernier. Le système de réception vérifie la cohérence entre l'objet reçu et cette empreinte.

En conséquence, un Coffre-fort électronique doit pouvoir :

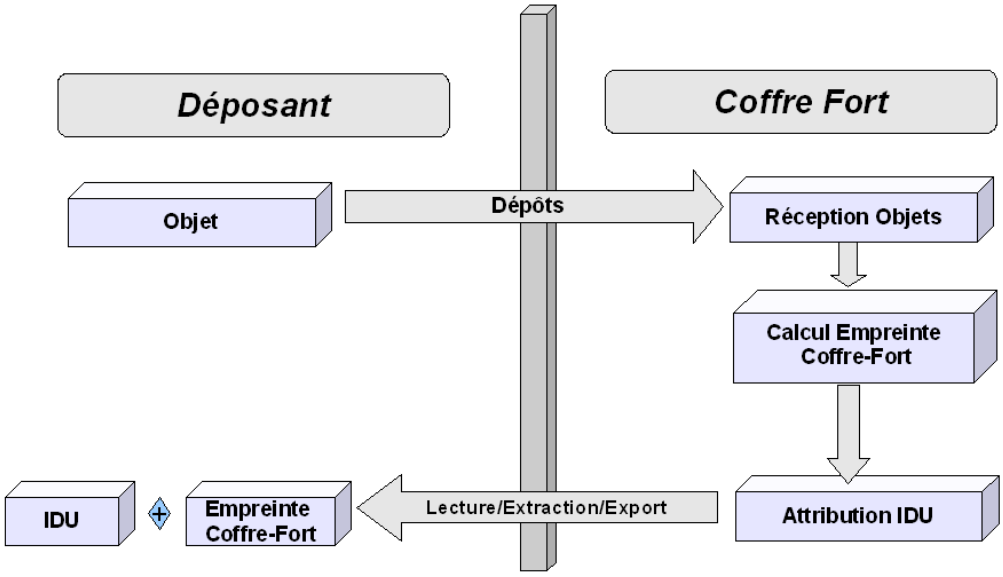
- Recevoir des objets numériques sans empreinte associée;
- Recevoir des objets numériques avec empreinte associée et effectuer un contrôle sur cette empreinte. La trace de ce contrôle doit être conservée.

8.2. Mode "non contrôlé"

Ce mode de fonctionnement correspond au dépôt d'un objet numérique par le déposant au Coffre-fort électronique sans que cet objet soit accompagné d'une empreinte calculée préalablement par le déposant.

A réception de l'objet numérique, le Coffre-fort électronique réalise les opérations suivantes :

- Calcul de l'empreinte interne correspondant à l'objet numérique reçu suivant un algorithme propre au Coffre-fort électronique ;
- Attribution à l'objet d'une IDU dans le Coffre-fort électronique ;
- Stockage de l'objet et de l'empreinte calculée par le Coffre-fort électronique ;
- Doublement du stockage de l'objet. Le Coffre-fort électronique doit disposer d'au moins une copie de sécurité ;
- Retour au déposant de l'IDU ;
- Retour au déposant de l'empreinte de l'objet numérique calculée par le Coffre-fort électronique dans le cas où le déposant souhaite obtenir cette donnée ;
- Retour au déposant d'une contremarque de temps calculée par le Coffre-fort électronique dans le cas où le déposant souhaite obtenir cette donnée ;
- L'ensemble des informations retournées au déposant devra faire l'objet d'un regroupement dans une attestation de dépôt pouvant être signée électroniquement par le Coffre-fort électronique selon un protocole normalisé.



8.3. Mode "contrôlé"

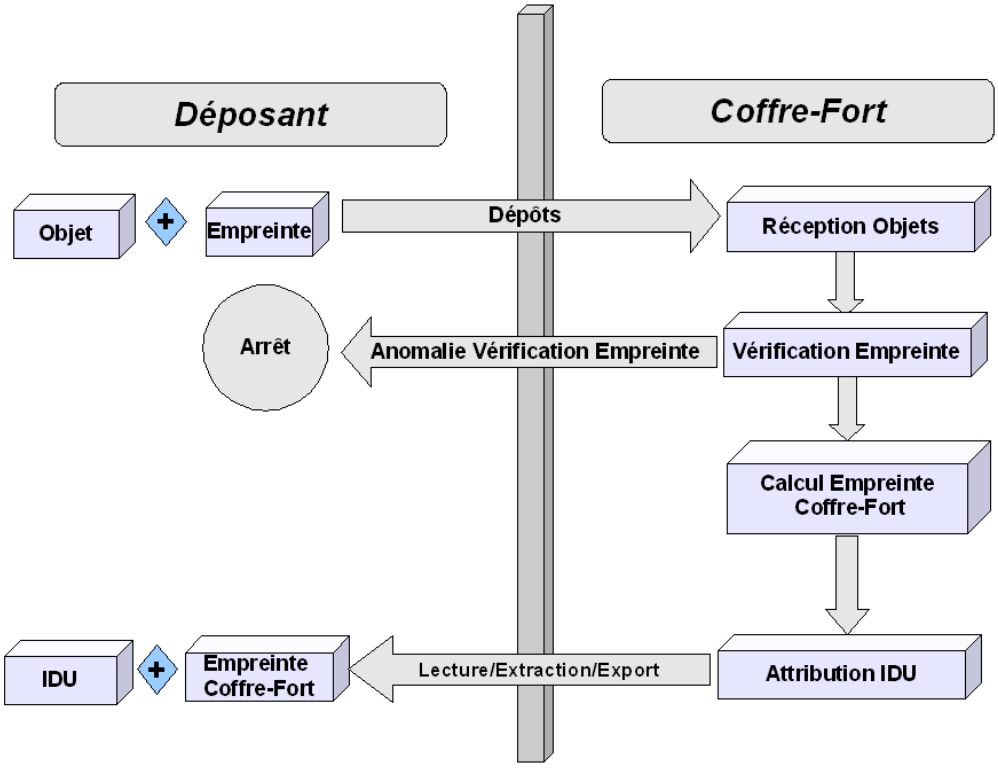
Ce second mode de fonctionnement correspond à des dépôts d'objets numériques accompagnés d'une empreinte calculée préalablement par le déposant.

A réception de l'objet numérique, le Coffre-fort électronique calcule une empreinte de l'objet reçu avec le même algorithme que celui utilisé par le déposant.

En cas de différence entre l'empreinte remise par le déposant et l'empreinte calculée par le Coffre-fort électronique, celui-ci émet en direction du déposant un message d'anomalie. Il n'y a pas alors de stockage de l'objet numérique.

Si les deux empreintes sont identiques, le Coffre-fort électronique réalise les opérations suivantes :

- Calcul de l'empreinte interne correspondant à l'objet numérique reçu suivant un algorithme propre au Coffre-fort électronique ;
- Attribution à l'objet d'une IDU dans le Coffre-fort électronique ;
- Stockage de l'objet et de l'empreinte calculée par le Coffre-fort électronique ;
- Doublement du stockage de l'objet. Le Coffre-fort électronique doit disposer d'au moins une copie de sécurité ;
- Retour au déposant de l'IDU ;
- Retour au déposant de l'empreinte de l'objet numérique calculée par le Coffre-fort électronique dans le cas où le déposant souhaite obtenir cette donnée ;
- Retour au déposant d'une contremarque de temps calculée par le Coffre-fort électronique dans le cas où le déposant souhaite obtenir cette donnée ;
- L'ensemble des informations retournées au déposant devra faire l'objet d'un regroupement dans une attestation de dépôt pouvant être signée électroniquement par le Coffre-fort électronique fort selon un protocole normalisé.



9. Dossier Technique

9.1. Définition du dossier technique

L'éditeur doit fournir un dossier technique permettant au Gestionnaire du Coffre-fort électronique de connaître le fonctionnement et toutes les possibilités de celui-ci.

La forme du dossier technique est libre mais il doit comporter obligatoirement les informations suivantes :

- L'architecture logicielle générale du Coffre-fort électronique et l'implémentation des fonctions ;
- Le besoin en éventuels composants nécessaires au bon fonctionnement du système (par exemple le SGBD support du Coffre-fort électronique) et la ou les versions compatibles de ces composants ;
- La description des flux des objets numériques depuis l'entrée dans le Coffre-fort électronique jusqu'à leur éventuelle élimination en passant par le stockage, la lecture et le vidage ;
- La description de tous les processus techniques garantissant l'intégrité des objets au sein du Coffre-fort électronique et notamment les algorithmes de production des empreintes des objets numériques et ceux de scellement numérique conformément à la norme NF Z42-013 : 2009 ;
- La nature et le format des informations retournées au déposant dans l'attestation de dépôt signée par le Coffre-fort électronique ;
- Les paramétrages, leur localisation et les moyens de les sauvegarder ;
- Les métadonnées techniques et d'intégrité liées aux objets numériques ;
- La définition des importations et des Restitutions d'objets numériques ;
- Les moyens employés pour assurer la réversibilité des objets ;
- Le référencement de chaque objet contenu dans le Coffre-fort électronique (constitution des IDU) ;
- Les moyens mis en œuvre pour les contrôles d'accès et la description des processus d'authentification ;
- Les outils utilisés pour l'horodatage des évènements (par exemple la définition d'une TSA, *Time Stamping Authority*) ;
- L'enregistrement des événements (journalisation) et la description des processus de conservation sécurisée des évènements afin de les rendre infalsifiables ;
- Les outils permettant les sauvegardes et les restaurations du Coffre-fort électronique ;
- La maintenance et le support technique.

9.2. Version du système

La version du Coffre-fort électronique doit être référencée de façon précise dans l'ensemble des livrables fournis aux utilisateurs de ce Coffre-fort électronique.

Lorsque le système est composé de sous-ensembles distincts et qui peuvent être installés de façon indépendante, ces sous-ensembles doivent être eux aussi décrits de façon précise en matière :

- De contenu de ces sous-ensembles ;
- De version de ces sous ensembles ;
- D'interface(s) avec les autres composants du Coffre-fort électronique.

9.3. L'environnement d'exploitation et de maintenance

L'environnement d'exploitation doit être décrit dans le dossier technique en précisant les matériels nécessaires, les conditions d'installation, d'exploitation et de maintenance nécessaires pour la bonne marche du Coffre-fort électronique.

Le dossier afférent doit comporter :

- L'architecture matérielle type définie avec précision (type de matériel, configuration, schéma de fonctionnement, …) :
  - Pour le serveur ;
  - Pour les postes des administrateurs du Coffre-fort électronique ;
  - Pour les postes des utilisateurs du Coffre-fort électronique.
- Les éléments descriptifs du doublement du stockage des objets et des empreintes ; les typologies des réseaux de communication supportés ;
- Le système d'exploitation et plus généralement tout l'environnement requis pour l'exploitation du système (système d'exploitation, gestionnaire de bases de données, serveur(s) HTTP(S), etc.) pour les serveurs et les postes des utilisateurs et des administrateurs ;
- Toute autre information jugée importante par l'éditeur et devant être portée à la connaissance de l'administrateur du Coffre-fort électronique pour le bon fonctionnement de celui-ci.

De plus, l'éditeur doit indiquer :

- Les principes de gestion des versions du Coffre-fort électronique ;
- L'impact sur les objets et les empreintes des changements de version ;
- Les conditions techniques de la maintenance (contrôles de reprise, contrôles d'intégrité, etc.) ;
- Les conséquences des incidents matériels ou des erreurs de fonctionnement du Coffre-fort électronique.

9.4. Plan d'Assurance Qualité

La conception et les développements du Coffre-fort électronique doivent reposer sur un Plan d'Assurance Qualité décrivant les procédures mises en œuvre pour :

- La conception du Coffre-fort électronique ;
- L'écriture des logiciels ;
- La production des équipements matériels lorsqu'ils existent ;
- La gestion des évolutions de celui-ci (notamment la gestion des versions) ;
- La gestion de la configuration ;
- Le signalement et le traitement des éventuels incidents relevés par les utilisateurs des Coffres-forts électroniques ;
- La gestion de la documentation.

9.5. Documentation

Outre le dossier technique, la documentation minimale qui doit être associée au système est la suivante :

- Manuel d'installation et de paramétrage ;
- Manuel d'administration et d'exploitation (notamment les procédures de sauvegardes et de restaurations à partir de ces sauvegardes) ;
- Manuel d'utilisation.

Ces manuels peuvent être regroupés en un seul ou fournis de façon indépendante et doivent être disponibles en français.

10. Horodatage

Le Coffre-fort électronique doit disposer d'une source de temps interne ou externe chargée de restituer une heure fiable selon l'usage requis.

Cette source de temps délivre au Coffre-fort électronique des Contremarques de temps.

Au minimum le Coffre-fort électronique effectue l'Horodatage des évènements suivants :

- Dépôts ;
- Eliminations (suppressions) ;
- Restitutions ;
- Vidages.

Dans le dossier technique, il doit être précisé tous les types d'horodatages supportés (interne ou externe).

Pour un horodatage externe la TSA (*Time Stamping Authority*) devra respecter le standard RFC3161.

Quel que soit l'horodatage appliqué, le dossier technique devra indiquer s'il utilise le standard RFC3161 ou bien décrire précisément son mécanisme d'Horodatage qui doit être auditable.

11. Enregistrement des actions dans le Coffre-fort électronique

11.1. Opérations journalisées

Un Coffre-fort électronique doit produire obligatoirement des enregistrements dans un journal de fonctionnement pour les fonctions suivantes :

- Dépôts ;
- Éliminations (suppressions) ;
- Restitutions ;
- Vidages ;
- Opérations de démarrage et d'arrêt du Coffre-fort électronique.

La journalisation des lectures n'est pas obligatoire mais un Coffre-fort électronique doit offrir cette possibilité :

- Soit de façon systématique ;
- Soit de façon optionnelle.

Dans le dossier technique, il doit être précisé :

- La possibilité de journaliser les lectures ;
- La méthode pour activer ou non cette possibilité si elle est optionnelle.

11.2. Implémentation du journal

11.2.1. Implémentation technique du journal

L'implémentation technique du journal est libre.

La description du journal, de sa forme et ses moyens de lecture et de contrôle doivent être précisés dans le dossier technique.

11.2.2. Éléments constitutifs du journal

Le journal doit contenir, a minima, les informations suivantes pour chaque action réalisée dans le Coffre-fort électronique, l'ordre des rubriques du journal n'étant pas imposé :

Rubrique	Obligatoire	Contenu	Exemple
Identifiant du Coffre-fort électronique	Oui	Identifiant du Coffre-fort électronique	PS_CFE_1234567890
Type Action	Oui	Actions possibles : ▪ Dépôt ▪ Elimination ▪ Restitution ▪ Vidage ▪ Lecture ▪ Vérification ▪ Administration	DEP
Identifiant Utilisateur	Oui	Identifiant unique de l'utilisateur qui exécute l'action par le Coffre-fort électronique	CLT-9987
Identification unique des objets attribuée par le Coffre-fort électronique lors du dépôt des objets (IDU)	Oui dans le cas d'une tache portant sur un objet géré par le Coffre-fort électronique. Facultatif pour les taches administratives de contrôle global, de	Identifiant unique à l'intérieur du Coffre-fort électronique	PS_CFE_1234567890_2008-05-12_008876

Rubrique	Obligatoire	Contenu	Exemple
	vidage, etc.		
Date de l'action	Oui	Format conforme à la norme NF EN 28601	2005/12/31
Heure de l'action	Oui	Format conforme à la norme NF EN 28601	23 :45 :17 :897
Time stamping	Oui	Le Coffre-fort électronique doit permettre un Horodatage : ▪ Soit conforme RFC 3161 ▪ Soit interne conforme à la norme Z42-013 : 2009	● Soit jeton RFC 3161 ● Soit jeton interne
Algorithme utilisé pour le calcul de l'empreinte lors du dépôt de l'objet	Oui	Définition du type d'algorithme utilisé pour calculer l'empreinte lors du dépôt de l'objet dans le Coffre-fort électronique L'algorithme de calcul d'empreinte doit être dans le domaine public et largement utilisé (MD5, SHA-1, SHA-256, etc.)	SHA-1
Empreinte de l'objet réalisée lors du dépôt de cet objet	Obligatoire lors du Dépôt	Contient la valeur de l'empreinte calculée par le Coffre-fort électronique lors du dépôt de l'objet	GTF65GY654NBG
Libellé erreur	Oui	Si l'opération s'est effectuée sans incident contient Ok, sinon un texte libre indique la cause de l'anomalie	Ok
Champs commentaire	Non	Contenu libre décrivant l'action surtout pour les taches administratives	

11.2.3. Intégrité du journal

Le Coffre-fort électronique doit garantir l'intégrité de son journal des événements. La méthode pour assurer cette intégrité doit être conforme aux procédés de scellement numérique de la norme NF Z42-013 : 2009. Elle doit être décrite dans le dossier technique.

La périodicité de la mise en œuvre des procédés pour garantir l'intégrité du journal doit être paramétrable afin que l'exploitant du Coffre-fort électronique puisse la fixer à sa convenance, en fonction de ses besoins et du respect du niveau de sécurisation standard de la norme NF Z42-013 : 2009.

En cas d'arrêt programmé du Coffre-fort électronique le journal devra être scellé.

Le Coffre-fort électronique doit posséder une méthode permettant de clôturer le journal lors de chaque arrêt du Coffre-fort électronique.

Il est nécessaire de préciser dans le dossier technique les conditions de clôture et d'ouverture du journal des évènements, notamment après un incident ayant conduit à l'arrêt du Coffre-fort électronique.

11.2.4. Sauvegarde et extraction des journaux

Afin de garantir la préservation des journaux dans le temps, un dispositif de sauvegarde de ceux-ci doit être disponible.

Cette sauvegarde doit être réalisée :

- Soit en format texte fixe ;
- Soit en format texte avec délimiteurs (CSV) ;

- Soit en format balisé (XML).

L'encodage doit être réalisé :

- Soit en ASCII ISO 8859-1 (Traitement de l'information - Jeux de caractères graphiques codés sur un seul octet) ;
- Soit en UNICODE (ISO/CEI 10646) Technologies de l'information - Jeu universel de caractères codés sur plusieurs octets (JUC)

Les sauvegardes des journaux doivent posséder les mêmes garanties d'intégrité et de pérennité que celles mises en œuvre pour les objets numériques contenus dans le Coffre-fort électronique.

Il doit exister un ou des outils :

- Pour la consultation des journaux (clôturés ou actifs) ;
- Le contrôle de l'intégrité de ces journaux ;
- Le contrôle l'horodatage de ceux-ci.

Nota : la détermination des fréquences des sauvegardes des journaux ne fait pas partie du présent référentiel, celle-ci est laissée au choix de l'exploitant du Coffre-fort électronique en fonction de ses contraintes d'usage.

12. Les contrôles d'accès

12.1. Définition

Un contrôle des accès au Coffre-fort électronique est obligatoire. Ce contrôle doit permettre de filtrer les accès aux fonctions suivantes :

- Dépôt ;
- Lecture (mise à disposition) ;
- Elimination (suppression) ;
- Restitution ;
- Administration dont le contrôle de l'intégrité de ces objets numériques.

12.2. Profils d'accès

La gestion des droits doit être réalisée par la mise en place :

- D'une gestion de profils décrivant les actions autorisées (toute action non autorisée doit être interdite) ;
- D'une gestion des utilisateurs et de l'affectation d'un ou plusieurs profils spécifiques à chaque utilisateur.

Un profil est associé à un certain nombre de droits sur la gestion et sur l'exploitation du Coffre-fort électronique et des objets qui y sont contenus. A minima, trois profils doivent être disponibles :

- Administrateur : création, suppression et modification des gestionnaires du Coffre-fort électronique et Vidage des objets ;
- Gestionnaire : dépôt, lecture, élimination et restitution des objets d'un Coffre-fort électronique ;
- Lecteur : fourniture de copies des objets numériques contenus dans un Coffre-fort électronique.

Cette gestion des profils et des utilisateurs peut être implémentée par une couche protocolaire du type LDAP. Dans tous les cas, il est obligatoire de mettre en œuvre des techniques qui permettent la traçabilité des modifications de ces informations.

L'ensemble de la mise œuvre de la gestion des profils doit être décrite dans le dossier technique.

12.3. Contrôle des accès

Le contrôle des accès doit être réalisé au minimum par un mécanisme exigeant 2 niveaux d'authentification (exemple : du type "nom utilisateur/mot de passe associé").

Tout autre système assurant une sécurité d'accès équivalente ou supérieure peut être utilisé. Dans ce cas, il convient de préciser dans le dossier technique les caractéristiques de ce système de contrôle d'accès (par exemple : utilisation de certificats numériques).

La norme NF Z42-013 : 2009 décrit précisément les différents niveaux de sécurité des contrôles d'accès admis.

13. La fonction d'administration

La fonction d'administration doit couvrir au minimum les fonctionnalités de création, modification et suppression des utilisateurs du Coffre-fort électronique.

Les procédures qui s'appliquent à cette fonction d'administration sont les suivantes.

13.1. Contrôle d'accès

Les profils autorisés à réaliser cette fonction sont les suivants :

Profils	Autorisé
Administrateur	Oui
Gestionnaire	Non
Lecteur	Non

13.2. Intégrité

La fonction d'administration ne doit avoir aucune possibilité d'action sur les objets numériques contenus dans le Coffre-fort électronique.

13.3. Traçabilité

Il est obligatoire de tracer toutes les opérations d'administration.

14. Les fonctions de gestion des objets numériques

14.1. La fonction de dépôt

La fonction de dépôt a pour but d'archiver un objet reçu après avoir exercé la vérification de l'identité du déposant.

Dans le cas du stockage "contrôlé", le Coffre-fort électronique vérifie également l'intégrité de cet objet par la vérification de l'empreinte fournie par le déposant.

Les procédures qui s'appliquent à la fonction de dépôt sont les suivantes.

14.1.1. Contrôle d'accès

Les profils autorisés à réaliser cette fonction sont les suivants :

Profils	Autorisé
Administrateur	Non
Gestionnaire	Oui
Lecteur	Non

14.1.2. Intégrité des objets déposés

L'éditeur doit indiquer comment il garantit l'intégrité de l'objet numérique lors du transfert pour le stockage de celui-ci dans le Coffre-fort électronique. Les moyens utilisés pour contrôler cette intégrité doivent être précisés dans le dossier technique.

Dans le cas du mode "contrôlé", si l'empreinte fournie par le déposant n'est pas égale à l'empreinte de l'objet numérique calculée par le Coffre-fort électronique :

- Il n'y pas d'archivage de l'objet numérique ;
- L'anomalie est journalisée et signalée au déposant.

14.1.3. Traçabilité

Il est obligatoire de tracer toutes les opérations de dépôt.

14.1.4. Génération d'une attestation de dépôt

La documentation de l'éditeur détaillera la nature des informations constituant l'attestation de dépôt et le format de l'éventuelle signature électronique utilisée.

14.2. La fonction de lecture

La fonction de lecture a pour objet de fournir une copie conforme d'un objet numérique archivé après fourniture de l'IDU par un demandeur authentifié.

Les procédures qui s'appliquent lors d'une lecture sont les suivantes.

14.2.1. Contrôle d'accès

Les profils autorisés pour cette fonction sont les suivants :

Profils	Autorisé
Administrateur	Non
Gestionnaire	Oui
Lecteur	Oui

14.2.2. Traçabilité

La traçabilité des opérations de lecture est obligatoire.

14.3. La fonction d'Elimination (suppression)

La fonction d'élimination a pour finalité de supprimer un objet numérique archivé dans le Coffre-fort électronique.

Au moment de l'Elimination, les métadonnées ainsi que l'objet numérique sont supprimés de façon irréversible mais tous les enregistrements du journal liés à l'objet éliminé sont conservés.

Les procédures qui s'appliquent à la fonction d'élimination sont les suivantes.

14.3.1. Contrôle d'accès

Les profils autorisés pour cette fonction sont les suivants :

Profils	Autorisé
Administrateur	Non
Gestionnaire	Oui
Lecteur	Non

14.3.2. Traçabilité

La traçabilité des opérations d'Elimination est obligatoire.

14.4. La fonction de Restitution

La fonction de Restitution a pour finalité :

- De réaliser une copie d'un objet numérique contenu dans le Coffre-fort électronique ;
- D'éliminer cet objet numérique du Coffre-fort électronique après avoir réalisé la copie de l'objet et avoir reçu une confirmation que cette copie s'était bien effectuée.

Les procédures qui s'appliquent à la fonction de restitution sont les suivantes.

14.4.1. Contrôle d'accès

Les autorisations d'accès pour cette fonction sont les suivantes :

Profils	Autorisé
Administrateur	Non
Gestionnaire	Oui
Lecteur	Non

14.4.2. Traçabilité

La traçabilité des opérations de Restitution est obligatoire.

15. Les fonctions d'intégrité et de gestion groupée d'objets

15.1. Inventaire des objets d'un Coffre-fort électronique

15.1.1. Principe

Cette fonction doit permettre d'obtenir la liste exhaustive des identifiants des objets numériques (IDU) contenus dans un Coffre-fort électronique accompagnés de métadonnées descriptives. La liste de ces métadonnées sera fournie dans la documentation de l'Editeur.

15.1.2. Contrôle d'accès

Les profils autorisés pour cette fonction sont les suivants :

Profils	Autorisé
Administrateur	Non
Gestionnaire	Oui
Lecteur	Non

15.1.3. Traçabilité

La production d'un enregistrement dans le journal est obligatoire.

15.2. Contrôle de l'intégrité d'un objet numérique

15.2.1. Principe

Il doit exister un moyen permettant de contrôler l'intégrité de chaque objet stocké dans un Coffre-fort électronique.

Ce contrôle d'intégrité doit s'appuyer sur l'utilisation des empreintes calculées à partir de chaque objet lors du dépôt de celui-ci.

15.2.2. Contrôle d'accès

Les profils autorisés pour cette fonction sont les suivants :

Profils	Autorisé
Administrateur	Non
Gestionnaire	Oui
Lecteur	Non

15.2.3. Traçabilité

La production d'un enregistrement dans le journal est obligatoire.

15.3. Contrôle de l'intégrité du Coffre-fort électronique

15.3.1. Principe

Un Coffre-fort électronique doit disposer de moyens d'autocontrôle.

Ces moyens d'autocontrôle doivent permettre notamment :

- De s'assurer que l'inventaire des objets numériques contenus dans le Coffre-fort électronique est toujours disponible et vérifiable ;
- De vérifier que l'ensemble des objets numériques stockés est intègre.

Ces moyens doivent pouvoir être utilisés lorsqu'il y a un doute sur l'intégrité ou l'exhaustivité du Coffre-fort électronique, par exemple, suite à un incident sur un support de stockage.

L'ensemble de ces dispositifs doit être décrit dans le dossier technique.

15.3.2. Contrôle d'accès

Les profils autorisés pour cette fonction sont les suivants :

Profils	Autorisé
Administrateur	Oui
Gestionnaire	Oui
Lecteur	Non

15.3.3. Traçabilité

L'exécution de la fonction de vérification doit être journalisée.

15.4. La fonction de Vidage

15.4.1. Principe

La fonction de vidage a pour finalité :

- De réaliser une copie de tous les objets contenus dans le Coffre-fort électronique ;
- D'éliminer tous les objets du Coffre-fort électronique immédiatement après avoir réalisé cette copie, à condition que cette copie se soit bien déroulée ;
- De fournir le journal complet de ce Coffre-fort électronique avec tous les éléments d'intégrité de celui-ci, si l'utilisateur le demande.

Le Coffre-fort électronique doit, a minima, vérifier l'intégrité des journaux qu'il restitue.

Les procédures qui s'appliquent à cette fonction de vidage sont les suivantes.

15.4.2. Contrôle d'accès

Les profils autorisés à réaliser cette fonction sont les suivants :

Profils	Autorisé
Administrateur	Non
Gestionnaire	Oui
Lecteur	Non

15.4.3. Traçabilité

Le journal doit permettre d'enregistrer l'ensemble des opérations nécessaires au vidage des objets du Coffre-fort électronique.

Nota : Il convient de prévoir des méthodes d'effacement efficaces des objets numériques pour qu'ils ne soient pas lisibles dans le Coffre-fort électronique après vidage. Ces méthodes doivent être précisées dans le dossier technique.

16. Supports d'archivage

Les supports d'archivage des objets numériques devront être conformes à la norme NF Z42-013 : 2009.

17. Statistiques d'utilisation

Le Coffre-fort électronique doit fournir à la demande des données permettant l'élaboration de statistiques de fonctionnement élémentaires.

Au minimum les données à fournir par tranche de 24h00 sont :

- Nombre de Dépôts ;
- Nombre de Lectures (mises à disposition) ;
- Nombre d'Eliminations (suppressions) ;
- Nombre de Restitutions.

18. Scénarios de test

Ces scénarios de test ont pour but de vérifier que le Coffre-fort électronique est conforme aux exigences décrites précédemment.

Il existe deux scénarios de test :

- Le premier correspond à des dépôts en mode "non contrôlé" ;
- Le second à des dépôts en mode "contrôlé".

La description des fichiers nécessaires aux tests est fournie en Annexe I « Constitution du jeu de tests ».

18.1. Dépôt en mode « non contrôlé »

L'objet de ce test est d'effectuer le dépôt des fichiers contenus dans le support de test dans le Coffre-fort électronique.

Ce dépôt doit être effectué :

- En mode « non contrôlé » ;
- Manuellement pour un nombre de fichiers choisi par l'expert.

Pour valider le test une fois les dépôts des fichiers effectués comme indiqué ci-dessus, l'expert vérifiera:

- La conformité du journal ;
- L'existence des objets déposés dans le coffre.

18.2. Dépôt en mode « contrôlé »

L'objet de ce test est d'effectuer le dépôt des fichiers contenus dans le support de test dans le Coffre-fort électronique.

Ce dépôt doit être effectué :

- En mode « contrôlé » ;
- Manuellement pour un nombre de fichiers choisi par l'expert.

Pour valider le test une fois les dépôts des fichiers effectués comme indiqué ci-dessus, l'expert vérifiera:

- La conformité du journal ;
- L'existence des objets déposés dans le coffre.

18.3. Lecture

Demander des copies d'objets à partir d'une sélection des IDU fournis lors du dépôt.

Pour valider le test une fois les lectures des fichiers effectués comme indiqué ci-dessus, l'expert vérifiera :

- La vérification de l'intégrité des objets fournis ;
- La conformité du journal.

18.4. Élimination

Demander l'Elimination des objets à partir d'une sélection des IDU.

Pour valider le test une fois les éliminations des fichiers effectuées comme indiqué ci-dessus, l'expert vérifiera :

- L'absence dans le coffre des objets éliminés ;
- La conformité du journal.

18.5. Restitution

Demander la Restitution d'objets à partir d'une sélection d'IDU.

Pour valider le test une fois les éliminations des fichiers effectuées comme indiqué ci-dessus, l'expert vérifiera :

- La vérification de l'intégrité des objets fournis ;
- L'absence dans le coffre des objets éliminés ;
- La conformité du journal.

18.6. Vidage

Réaliser le vidage du coffre-fort.

Pour valider le test une fois le vidage effectué comme indiqué ci-dessus, l'expert vérifiera :

- La vérification de l'intégrité des objets fournis ;
- L'absence de tout objet dans le coffre ;
- La conformité du journal.

18.7. Vérification du journal

Réaliser plusieurs clôtures du journal, à différents moments, y compris lors d'un arrêt programmé.

Pour valider le test une fois la clôture effectuée comme indiqué ci-dessus, l'expert vérifiera :

- La conformité du journal.

19. Annexe I - Constitution du jeu de tests

La présente annexe a pour but de définir le contenu des fichiers de tests pour le Coffre-fort électronique.

La présente annexe définit :

- Le nom, la taille et le contenu des fichiers destinés aux tests ;
- Les empreintes associées à ces fichiers ;
- Le type de support de livraison de ces fichiers de test ;
- L'organisation de ce support de livraison ;
- Les principes pour la validation de ce support de livraison.

Nota : Les algorithmes de calcul d'empreintes retenus pour ces tests ne visent pas à démontrer les possibilités des coffres-forts électroniques audités en matière de garantie de la pérennité/intégrité des objets numériques qu'ils contiennent mais à démonter que ces Coffres-Forts électroniques sont capables de gérer et de vérifier des empreintes dans les deux modes de dépôt (contrôlé ou non contrôlé). C'est pourquoi, il n'a pas été retenu d'algorithme à très haut niveau de sécurité. Cependant, les coffres-forts doivent prévoir la possibilité de gérer d'autres algorithmes

19.1. La constitution des fichiers tests

Le programme de constitution des jeux de test génère de manière aléatoire l'ensemble des fichiers des diverses tailles ainsi qu'il calcule les empreintes associées à chacun de ces fichiers.

19.1.1. Les classes des fichiers

Les fichiers sont répartis en 6 classes suivant leur taille :

Classes	Taille en octets
T1	250
T2	25 000
T3	150 000
T4	2 500 000
T5	50 000 000
T6	100 000 000

19.1.2. Règles de nommage des divers fichiers

Les fichiers sont nommés de la façon suivante :

TX_999999

Où :

- TX indique la classe du fichier, X étant compris entre 1 et 6 ;
- 999999 est un nombre compris entre 000001 et 999999.

Exemples :

- T1_004276 pour un fichier de la classe 1 ;
- T6_000005 pour un fichier de la classe 6.

L'extension de ces fichiers est « .TXT ».

Exemples :

- T1_004276.TXT pour un fichier de la classe 1,
- T6_000005.TXT pour un fichier de la classe 6.

A chaque fichier est associé deux empreintes. La première empreinte est calculée avec la méthode SHA-1, la seconde

avec la méthode SHA-256. L'extension respective de ces fichiers est «SH1» pour les premiers et SH2 pour les seconds.

En conséquence il y a des groupes de trois fichiers associés :

- TX_999999.TXT est le fichier objet ;
- TX_999999.SH1 pour l'empreinte SHA-1 associée ;
- TX_999999.SH2 pour l'empreinte SHA-256 associée.

19.1.3. Contenu des fichiers

Les fichiers contiennent :

- Dans les 9 premiers octets le nom du fichier ;
- Pour les octets suivants : un texte en ISO latin-1.

19.1.4. Synthèse

L'ensemble des fichiers de test peu être synthétisé comme suit :

Tableau de répartition des fichiers de tests

Classes	Nombre fichiers	Taille en octets	Noms des fichiers
T1	4500	250	De T1_000001 à T1_004500
T2	2500	25000	De T2_000001 à T2_002500
T3	1150	150000	De T3_000001 à T3_0011500
T4	650	2500000	De T4_000001 à T4_000650
T5	20	50000000	De T5_000001 à T5_000020
T6	10	100000000	De T6_000001 à T6_000010

Les fichiers sont répartis dans 6 répertoires nommés REP01 à REP06.

20. Annexe II (Informative) - Stratégies pour la conservation des documents numériques

La présente annexe vise à préciser l'approche technique du présent référentiel vis à vis des stratégies pour la conservation des documents numériques. Cette annexe est informative et ne fait pas partie du référentiel.

20.1. Définition des diverses approches

Plusieurs approches sont possibles en matière de conservation des documents numériques pour atteindre les objectifs cités précédemment. Il existe principalement trois stratégies pour la conservation des documents numériques :

- L'émulation ;
- La conservation de tous les équipements et des supports ;
- La migration.

20.2. L'émulation

L'émulation qui consiste en la réalisation dans un environnement informatique actuel X (par exemple Windows XP) d'un environnement technique Y plus ancien (par exemple MS/DOS), n'a pas fait réellement ses preuves à ce jour.

Il n'existe pas actuellement de solutions commerciales disponibles et fiables.

De plus cette technique impose aussi la migration de supports. Par exemple, il est peut être possible de simuler dans un environnement LINUX un système d'exploitation comme GCOS et le moniteur de Time Sharing qui fonctionnait dans cet environnement. Cependant, il est sûr que des données sur des bandes au format 1/2 pouce enregistré à 6 250 BPI ne sont plus utilisables aujourd'hui, car les lecteurs de ces bandes n'existent plus ou sont très difficiles à intégrer dans un environnement technique moderne.

20.3. La conservation des équipements

La conservation de tous les équipements (matériels et logiciels) et des supports d'information est aussi une solution possible. Cette approche est notamment utilisée dans le domaine militaire pour assurer le fonctionnement de systèmes d'armes.

Si cette méthode est efficace, elle comporte cependant deux écueils :

- Le coût : il est nécessaire d'acheter en double ou en triple tous les équipements ;
- La limite dans le temps : la disponibilité de certains équipements est incertaine dans le futur.

20.4. La migration

Cette technique consiste essentiellement à conserver pendant un certain temps des objets numériques sur des supports puis à copier ces objets numériques d'un support à un autre quand le premier a atteint ses limites de fiabilité ou de pérennité.

Cependant, cette technique présente des contraintes :

- Il convient d'assurer la gestion de l'intégrité des fichiers numériques par des moyens spécifiques ;
- Il est nécessaire de réaliser périodiquement des migrations de supports physiques afin d'éviter l'obsolescence de ceux-ci ;
- Régler le problème de la conservation du format originel.

Le choix des formats de stockage doit être réalisé avec soin car la pérennité de ces formats doit être compatible avec les besoins en durées de conservation.

20.5. Conclusion

Seule la migration de supports et de formats semble aujourd'hui permettre d'assurer la conservation de fichiers numériques sur le long terme.