GROUPE DE TRAVAIL
REFERENTIEL

ADAP
APROGED
FEDISA
FNTC

Référentiel progiciel

Coffre Numérique

Version 4 du 10 mars 2006

SOMMAIRE

1 Suivi du document

Version	Date
V 1	10/01/2006
V2	15/01/2006
V2-1	26/01/2006
V3	16/02/2006
V4	03/02/2006
V5	10/02/2006

2 Introduction

Le présent document a pour but de définir les fonctionnalités minimales que doit posséder un progiciel de COFFRE NUMERIQUE.

3 Documents applicables

Les documents suivants sont applicables au présent document :

- Principes directeurs référentiels ;
- Constitutions des fichiers de tests.

4 Vocabulaire

Le vocabulaire suivant est applicable au présent document.

Nom	Définition
Objet	Train de bits numériques archivable dans un COFFRE NUMERIQUE
IDU	IDentification Unique d'un objet
Dépôt	Fourniture au COFFRE NUMERIQUE d'un objet pour stockage
Lecture	Fourniture d'une copie d'un objet contenu dans un COFFRE NUMERIQUE
Elimination	Suppression complète d'un objet dans un COFFRE NUMERIQUE
Export	Lecture d'un objet suivi de l'élimination de celui-ci dans un COFFRE NUMERIQUE
Extraction	Lecture de la totalité des objets suivi de l'élimination de ceux-ci dans COFFRE NUMERIQUE
Intégrité	Identité au bit près d'un objet dans le temps

5 Les contrôles d'accès

5.1 Définition

Un contrôle des accès au COFFRE NUMÉRIQUE est obligatoire. Ces contrôles doivent permettre de filtrer les accès aux fonctions :

- D'administration du COFFRE NUMÉRIQUE ;
- De gestion des objets ;
- De lecture des objets.

5.2 Profils d'accès

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

- D'une gestion de profils décrivant les services autorisés (tout service non autorisé étant interdit) ;
- D'une gestion des gestionnaires et de l'affectation d'un profil spécifique à chaque gestionnaire.

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

- Administrateur: création, suppression et modification des gestionnaires du COFFRE NUMÉRIQUE et la possibilté de l'extraction ;
- Gestionnaire : dépôt, lecture, élimination et export des objets d'un COFFRE NUMERIQUE ;
- Lecteur : lecture seule des objets sans aucune possibilité de modification.

Cette gestion des profils et des Gestionnaires peut s'appuyer sur des systèmes externes de gestion d'annuaire comme un annuaire d'entreprise (LDAP, Active Directory, etc.). Dans ce cas, l'intégration de ces outils devra être précisée dans le dossier technique. Il convient notamment de préciser les possibilités d'accès au COFFRE NUMERIQUE en cas d'indisponibilité de cet annuaire.

5.3 Contrôle des accès

Le contrôle des accès doit être réalisé au minimum par un mécanisme du type "nom Gestionnaire/mot de passe associé". Le mot de passe doit comporté au moins un caractère.

Tout autre système assurant une sécurité d'accès équivalente peut être utilisé. Dans ce cas, il convient de préciser dans le dossier technique les caractéristiques de ce système.

6 Contrôle d'intégrité

6.1 Auto-contrôle

Le coffre doit disposer de moyens d'auto-contrôle. Ces moyens doivent pouvoir être utilisés lorsqu'il y a un doute sur l'intégrité ou l'exhaustivité du COFFRE NUMERIQUE, par exemple, suite à un incident sur un support de stockage.

Ces moyens d'autocontrôle doivent permettre notamment :

- De s'assurer que le nombre d'objets est bien celui qui doivent normalement être stockés dans le COFFRE NUMERIQUE ;
- De vérifier que les objets sont intégres.

Les types et les moyens sont nécessaires à cet auto-contrôle sont laissés au choix de l'éditeur du logiciel.

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

6.2 Contrôle de l'intégrité des objets

Il doit exister un systèmede vérifier de contôle de l'intégrité de chaque objet stocké dans le COFFRE NUMERIQUE.

Ce contôle d'intégrité doit s'appuyer sur l'utilisation d'empreintes calculées à partir des objets.

Le choix des algorithmes disponibles dans le COFFRE NUMERIQUE pour calculer ces empreintes (SHA-1, SHA-256, MD5, ...) est libre. Les algorithmes retenues doivent être précisés dans le dossier technique.

L'algorithme spécifique qui a été utilisé lors d'une action sur un objet dans un coffre (dépôt, lecture, élimination, extraction ou exportation) doit être inscrit dans le journal afin de garantir la possibilité de contrôles ultérieurs.

7 Les services du COFFRE NUMERIQUE

7.1 Le service d'administration

Le service d'aministration a pour but de créer, modifier et supprimer les gestionnaires.

Les procédures qui s'appliquent au service d'administration sont les suivantes.

7.1.1 Contrôle d'accès

Les profils autorisés à réaliser ce service sont les suivants :

Profils	Autorisé
Administrateur	Oui
Gestionnaire	Non
lecteur	Non

7.1.2 Intégrité

Le service d'administration ne doit avoir aucune possibilité d'action sur les objets contenus dans le COFFRE NUMERIQUE.

7.1.3 Traçabilité

Il n'y a pas de traçabilité obligatoire dans le journal pour ce service.

7.2 Le service de dépôt

Le service de dépôt a pour but d'archiver un objet reçu après vérification de l'identité du déposant et dans le cas de l'archivage "contrôlé" de l'intégrité de cet objet.

Le COFFRE NUMÉRIQUE retourne au déposant pour chaque objet déposé :

- L'IDU de l'objet archivé ;
- L'empreinte de cet objet archivé.

Les procédures qui s'appliquent au dépôt sont les suivantes.

7.2.1 Contrôle d'accès

Les profils autorisés à réaliser ce service sont les suivants :

Profils	Autorisé
Administrateur	Non
Gestionnaire	Oui
lecteur	Non

7.2.2 Intégrité

Les deux types de dépôt suivants doivent être possibles dans un COFFRE-NUMERIQUE :

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

En conséquence, un COFFRE NUMERIQUE doit pouvoir :

- Recevoir des objets sans empreinte associée ;
- Recevoir des objets avec empreinte associée et effectuer un contrôle sur cette empreinte.

L'opération d'archivage doit respecter absolument la contrainte essentielle d'intégrité. L'objet fourni ne doit en aucun cas être altéré lors de toutes les phases nécessaire au dépôt.

Le fournisseur doit indiquer comment il garantit l'intégrité du transfert lors de l'archivage. Les moyens utilisés (empreinte, signature, scellement, ...) doivent être précisés dans le dossier technique.

7.2.3 Traçabilité

Il est obligatoire de tracer toutes les opérations de dépôt.

L'existence d'un certificat de dépôt est nécessaire au contrôle d'intégrité. Ce certificat doit comprendre a minima l'IDU de l'objet et l'empreinte de l'objet calculée par le COFFRE NUMERIQUE.

La forme du certificat est laissé libre, par exemple l'enregistrement dans le journal de l'opération répond à ce besoin. La forme de ce certificat doit être précisé dans le dossier technique.

7.3 Le service de lecture

Le service de lecture a pour mission de fournir une copie d'un objet archivé, grâce à la fourniture de l'IDU, après vérification de l'identité du demandeur.

Le COFFRE NUMÉRIQUE retourne au démandeur :

- Soit une copie de l'objet archivé ;
- Soit :
  - Dans le cas d'un dépôt simple, une copie de l'objet et son empreinte qui a été calculée lors du dépôt par le COFFRE NUMERIQUE ;
  - Dans le cas d'un dépôt contrôlé, une copie de l'objet, l'empreinte fournies par le déposant, ainsi son empreinte qui a été calculée lors du dépôt par le COFFRE NUMERIQUE.

La disponibilité des deux modes de lecture est obligatoire.

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

7.3.1 Contrôle d'accès

Les profils autorisés pour cette fonction sont les suivants :

Profils	Autorisé
Administrateur	Non
Gestionnaire	Oui
Lecteur	Oui

7.3.2 Intégrité

Le fournisseur doit indiquer comment il garantit l'intégrité du transfert lors de la consultation. Les moyens utilisés (empreintes, signatures scellements, etc.). doivent être précisés dans le dossier technique du progiciel.

7.3.3 Traçabilité

La traçabilité des opérations de lecture n'est pas obligatoire.

7.4 Le service d'élimination

Le service d'élimination a pour but de détruire les objets archivés dans le COFFRE NUMERIQUE.

Les procédures qui s'appliquent au service d'élimination sont les suivantes.

7.4.1 Contrôle d'accès

Les profils autorisé pour cette fonction sont les suivants :

Profils	Autorisé
Administrateur	Non
Gestionnaire	Oui
Lecteur	Non

7.4.2 Intégrité

Afin de garantir que l'élimination s'opère sur les bons objets, toute élimination doit être formulée en précisant simultanément :

- L'IDU de l'objet archivé ;
- L'empreinte associée pour cet objet.

L'opération d'élimination doit respecter absolument la contrainte d'intégrité, c'est-à-dire que l'objet à détruire doit donc correspondre à l'IDU présentée et être associée à la bonne empreinte.

Le fournisseur doit indiquer comment il garantit l'intégrité du reste de l'archive lors de la phase d'élimination.

La production d'un certificat d'élimination est obligatoire (par exemple l'enregistrement dans le journal de l'opération d'élimination répond à ce besoin).

7.4.3 Traçabilité

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

Cette journalisation doit permettre de suivre parfaitement les diverses opérations d'élimination suivant la méthodologie décrite dans le dossier technique.

7.5 Le service d'export

Le service d'export a pour fonction :

- De réaliser une copie de l'objet ;
- D'éliminer cet objet du coffre immédiatement après avoir réalisé cette copie de l'objet ;
- Les éléments de journalisation qui correspondent à cet objet.

Les procédures qui s'appliquent au service d'extraction sont les suivantes.

7.5.1 Contrôle d'accès

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

Profils	Autorisé
Administrateur	Oui
Gestionnaire	Non
lecteur	Non

7.5.2 Intégrité

Afin de garantir que l'export s'opère sur les bons objets, toute demande doit être formulée en précisant simultanément :

- L'IDU de l'objet archivé ;
- L'empreinte associée à cet objet.

L'opération d'export doit respecter absolument la contrainte essentielle d'intégrité. Le objet à extraire doit donc bien correspondre à l'IDU présentée associée à la bonne empreinte. Une vérification de cette intégrité doit être réalisée par le COFFRE NUMERIQUE lors de l'export.

La production d'un certificat d'extraction est obligatoire.La formede ce certificat est libre (par exemple l'enregistrement dans le journal de l'opération d'extraction répond à ce besoin).

7.5.3 Traçabilité

Le journal doit permettre de suivre complètement les diverses opérations nécessaires à l'export d'un objet.

7.6 Le service d'extraction

Le service d'extraction a pour fonction :

- De réaliser une copie de tous les objets du COFFRE NUMERIQUE ;
- D'éliminer tous les objets du coffre immédiatement après avoir réalisé cette copie ;
- De fournir le journal complet de ce coffre avec tous les scellements.

Les procédures qui s'appliquent au service d'extraction sont les suivantes.

7.6.1 Contrôle d'accès

Les profils autorisé à réaliser cette fonction sont les suivants :

Profils	Autorisé
Administrateur	Oui
Gestionnaire	Non
Lecteur	Non

7.6.2 Intégrité

Il n'y a pas d'IDU à fournir pour ce service.

Le COFFRE NUMERIQUE doit a minima vérifier l'intégrité des journaux qu'il restitue.

7.6.3 Traçabilité

Le journal doit permettre de suivre complètement l'ensemble des opérations nécessaires à l'extraction des objets du COFFRE NUMERIQUE.

8 Enregistrement des actions dans le COFFRE NUMÉRIQUE

8.1 Opérations journalisées

Un enregitrement dans le journal doit être obligatoirement produit pour les actions suivantes :

- Dépôt d'un objet ;
- Elimination d'un objet ;
- Export d'un d'objet ;
- Extraction d'un coffre.

8.2 Format du journal

Le journal doit contenir a minima les informations suivantes :

Rubrique	Obligatoire	Contenu	Exemple
Identifiant du coffre	Oui	Identifiant du coffre attribué lors de la création de celui-ci	GGJLP
Type Action	Oui	Actions possibles : ▪ Dépôt : DEP ▪ Elimination : ELI ▪ Export : EXP ▪ Extraction : EXT	DEP
Identifiant Déposant	Oui	Identifiant unique du Déposant attribué par le coffre numérique	CLT-9987
Identification unique des objets attribuée par le coffre numérique lors du dépôt des objets	Oui	Identifiant unique à l'intérieur du coffre	GGJLP-008876
Date	Oui	Format conforme à la norme NF EN 28601	2005/12/31
Heure	Oui	Format conforme à la norme NF EN 28601	23 :45 :17 :897
Algorithme utilisé pour le calcul de	Oui	Définition du type d'algorithme utilisé par le coffre MD5,	SHA-1

Rubrique	Obligatoire	Contenu	Exemple
l'empreinte du coffre numérique		SHA-1, SHA-256, etc.	
Empreinte de l'objet réalisé par le coffre numérique lors du dépôt de cet objet	Oui	Contient la valeur de l'empreinte calculée lors du dépôt avec l'empreinte	GTF65GY654NBG
Algorithme utilisé pour le calcul de l'empreinte fourni par déposant	Non	Cette information est renseignée lors d'un dépôt contrôlé par le déposant (la liste des algorithme est	MD5
Empreinte de l'objet fourni par le déposant	Non	Cette information est renseignée lors d'un dépôt contrôlé	GTDTDE54FR53S
Libellé erreur	Oui	Si l'opération s'est effectuée sans incident contient Ok, sinon un texte libre indique la cause de l'anomalie	Ok

8.3 Scellement du journal

Afin de garantir l'intégrité du journal des événements, un dispositif de scellement régulier doit être disponible.

La périodicité de ce scellement doit être être paramétrable afin que l'exploitant du COFFRE puisse la fixer àsa convenance.

Le scellement est fait en utilisant un algorithme public (MD5, SHA-1, etc.) qui doit être précisé dans le dossier technique.

Le scellement doit être horodaté.

Le progiciel doit pouvoir :

- Soit fournir un horodatage interne (dossier de description à fournir) ;
- Soit pouvoir utiliser, si l'Gestionnaire le désire, une TSA externe. L'éditeur doit indiquer les TSA qu'il peut exploiter.

Les événements d'une journée sont horodatés par cette TSA (interne ou externe) et le scellement du journal précédent est le premier enregistrement du noubeau journal. Le scellement doit être réalisé systématiquement lors de l'arrêt du système de production du journal (par lors de l'arrêt du COFFRE NUMERIQUE).

Il est nécessaire de préciser dans le dossier technique les conditions de clôture et d'ouverture du journal.

8.4 Sauvegarde et extraction du journal

Afin de garantir la préservation du journal dans le temps, un dispositif d'extraction doit être de celui-ci doit être disponible afin que l'exploitant du COFFRE NUMERIQUE puisse réalisé régulièrement des sauvegardes de journal.

Le format de cette sauvegarde peut être dans l'un des formats suivants :

- **ASCII ;**
- **CVS ;**
- **XML.**

Les journaux (extraits ou actifs) doivent pouvoir être disponibles pour la consultation et disposer des moyens nécessaires pour le contrôle des scellements.

Il ne sera possible d'expurger une partie d'un historique qu'après la sauvegarde de cette partie de celui-ci.

Cette sauvegarde doit posséder les mêmes garanties d'intégrité et de pérennité que pour les objets et l'identifiant unique de l'objet.

9 Dossier Technique

9.1 Définition du dossier technique

Le fournisseur doit fournir un dossier technique permettant à l'Gestionnaire de connaître le fonctionnement et les possibilités du COFFRE NUMÉRIQUE.

La forme du dossier technique est libre mais il doit comporter obligatoirement les éléments suivants :

- L'environnement d'exploitation ;
- La définition des imports et des exports / les moyens employés pour assurer la réversibilité ;
- Le référencement des objets (IDU) ;
- Les moyens mis en œuvre pour les contrôles d'accès ;
- Les outils pour l'horodatage et la signature des opérations ;
- L'enregistrement des événements ;
- Les mécanismes permettant les sauvegardes et les restaurations du COFFRE NUMÉRIQUE ;
- La maintenance et le support technique ;
- L'objet associé.

9.2 Version du progiciel

La version du progiciel doit être référencée de façon précise dans l'ensemble des livrables et des objets fournis à l'Gestionnaire.

Lorsque le progiciel est composé de sous-ensembles distincts, qui peuvent être installés de façon indépendante ou directement liés au progiciel, ces sous-ensembles doivent être eux aussi référencés de façon précise en matière de version du progiciel.

9.3 Dossier de description du progiciel

Ce dossier décrit les conditions d'installation et d'exploitation du progiciel.

Il doit comporter au minimum :

- L'architecture générale du progiciel, les grandes fonctions de celui-ci et les relations des composants de ce progiciel les uns avec les autres ;
- La version du progiciel livré et la version des éventuels composants nécessaires au bon fonctionnement du progiciel (par exemple la version SGBD nécessaire au fonctionnement du progiciel) ;
- La description des flux des objets depuis l'entrée dans le COFFRE NUMÉRIQUE jusqu'à leur éventuelle élimination en passant par l'archivage, la consultation et la restitution ;
- La description de toutes les procédures garantissant l'intégrité des objets au sein du COFFRE NUMÉRIQUE ;

- Les paramétrages, leur localisation, le moyen de les sauvegarder et la méthode pour la gestion de leurs versions.

9.4 Plan d'Assurance Qualité

Le fournisseur doit indiquer l'existence d'un Plan d'Assurance Qualité et décrire les procédures mises en œuvre pour :

- Le développement du progiciel ;
- La gestion des évolutions du progiciel (notamment la gestion des versions) ;
- La gestion de la configuration ;
- Et les signalements d'incidents relevés par Gestionnaires du progiciel et leur traitement.

9.5 L'environnement d'exploitation

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 progiciel.

Le dossier doit comporter :

- L'architecture matérielle type définie avec précision (type de matériel, configuration, schéma, ...) :
  - Pour le serveur ;
  - Pour les postes des gestionnaires.
- Les typologies des réseaux de communication supportés;
- Le système d'exploitation et plus généralement tout l'environnement requis pour l'exploitation du progiciel (système d'exploitation, bases de données, serveur http, etc.) pour les serveurs et les postes Gestionnaires ;
- Toute autre information jugée importante par le fournisseur et devant être portée à la connaissance de l'Gestionnaire pour le bon fonctionnement du progiciel.

9.6 Equipements minimum

Le fournisseur du progiciel doit préciser les équipements nécessaires au bon fonctionnement du progiciel. Notamment, il doit être précisé les performances du progiciel en fonction du nombre d'Gestionnaires sur un matériel type (par exemple, le temps de réponse après une interrogation en fonction du nombre de objets et la puissance du processeur du serveur).

9.7 Maintenance et Support Technique

Le fournisseur doit, dans le cadre d'un contrat de maintenance et support technique, intervenir auprès de l'Gestionnaire afin de lui apporter l'aide nécessaire au bon fonctionnement de l'application.

Le fournisseur doit indiquer :

- Les principes de gestion des versions du COFFRE NUMÉRIQUE ;
- L'impact sur les objets et les index 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 NUMÉRIQUE.

9.8 Documentation

La documentation minimale qui doit être associée au progiciel est la suivante :

- Documentation d'architecture générale ;
- Documentation d'installation ;
- Documentation d'exploitation ;
- Documentation Gestionnaire ;
- Schémas d'accès aux objets et d'enregistrement de ceux-ci.

10 Scénarii de test

Il existe deux scenarii de test : le premier correspond à un chargement « non contrôlé », le second à un chargement contrôlé.

La description des fichiers est fournie en dans le document « Constitution des Fichiers Tests ».

10.1Chargement

Effectuer le chargement des fichiers du support de test.

Ce chargement doit être effectué :

- En mode « non contrôlé » ;
- En lot pour les 9 premiers répertoires ;
- Manuellement pour 20 fichiers choisis au hasard dans le dernier répertoire.

Vérifier dans le journal le chargement des fichiers en réalisant un contrôle sur 30 IDU fournis par le COFFRE NUMERIQUE lors du chargement.

10.2 Consultation

Interroger le COFFRE NUMERIQUE avec 30 IDU. Vérifier la conformité des empreintes fournies lors du chargement.

Iln'y a pas de trace dans lejournal à vérifier pour ce type d'action sur le COFFRE NUMERIQUE.

10.3 Copie

Demander des copies d'objets à partir de 30 IDU fournis lors du chargement. Vérifier dans le journal la trace de ces copies.

10.4 Élimination

Demander l'élimination de 30 d'objets (à partir des IDU fournis lors du chargement). Vérifier dans le journal la trace de ces éliminations.

10.5 Extraction

Réaliser 30 éliminations avec des IDU obtenues au chargement (étape 8.1).

Vérifier dans le journal la trace de ces extractions.

Vérifier l'extraction du journal correspondant aux documents extraits.

10.6 Vérification du journal

Réaliser une clôture du journal. Vérifier que le journal contient latotalité des enregistrements attendus.

10.7 Fonctionnement en mode contrôlé.

Extraire la totalité des objets restant dans le coffre.

Recommencer la séquence complète des tests (de 9.1 à 9.6) en réalisant le chargement initial en « mode contrôlé ».