

***Coffre-fort électronique  
Livre Blanc***

---



## *Avant propos*

*Ceci est le premier livre blanc produit par FedISA Luxembourg.*

*Son sujet, le coffre-fort électronique, est emblématique de l'objectif que le Grand-Duché de Luxembourg s'est fixé à lui-même: devenir le coffre-fort numérique de l'Europe. Un dessein qui prend forme petit à petit, notamment avec l'ambitieuse réforme du cadre légal sur l'archivage électronique actuellement en cours de préparation.*

*Ce livre blanc représente aussi l'essence de FedISA.*

*Par la diversité des membres du groupe de travail qui lui a donné naissance d'abord: chercheurs, créateurs et utilisateurs de technologie, représentants de l'industrie, du secteur financier. C'est la raison d'être, mais aussi la singularité de FedISA, que de réunir et fédérer ces talents pour créer une véritable communauté.*

*Par la collaboration entre les différents chapitres nationaux de FedISA ensuite. Une rencontre, celle de représentants luxembourgeois et français de FedISA, en marge du congrès de FedISA France qui a eu lieu en février 2011, et l'échange de vue passionnant qui s'en est suivi, a permis d'enrichir ce livre blanc des expériences vécues de chaque côté de la frontière.*

*Merci et bravo aux membres de ce dynamique groupe de travail, ainsi qu'à ceux qui ont partagé leur expérience avec eux, d'avoir donné corps à ces valeurs de partage et d'échange qui font l'essence de FedISA.*

Cyril Pierre-Beausse

Président de FedISA Luxembourg

## Contents

---

I.	Introduction et objectifs du document.....	4
II.	Définition du coffre-fort électronique .....	5
1.	Définition générale .....	5
a)	Coffre-fort électronique (ou CFE) .....	5
b)	Espace virtuel de stockage et de conservation.....	5
c)	Sécurisé .....	6
d)	Inviolable.....	6
e)	Restituer.....	6
f)	ce.....	7
g)	Déposé .....	7
h)	Sans altération .....	8
2.	Éléments-clefs du CFE .....	9
III.	Différences entre CFE et autres systèmes .....	10
IV.	Services associés .....	11
1.	Horodatage .....	12
2.	Signature électronique.....	12
3.	Restitution des données .....	13
4.	Autres services .....	14
V.	Catégorisation des contenus.....	15
VI.	Positionnement et perspectives du CFE .....	16
VII.	Contexte législatif luxembourgeois .....	19
1.	Contexte législatif sur les données dématérialisées.....	19
2.	Contexte législatif sur la signature électronique .....	19
3.	Contexte législatif sur la cryptographie .....	20
4.	Contexte législatif sur la protection des données .....	21
5.	Validité des conventions .....	22
VIII.	Pistes d'extension du document.....	23
IX.	Conclusion.....	23
	Équipe rédactionnelle (par ordre alphabétique).....	24
Annexe A.	Pérennité.....	27
Annexe B.	Glossaire du chapitre III « Différences entre CFE et autres systèmes » .....	28
Annexe C.	Contexte législatif sur les coffres-forts non-électroniques.....	30

## I. Introduction et objectifs du document

---

Le patrimoine informationnel d'une personne physique ou morale a une forte valeur. Que cette valeur soit sentimentale, administrative ou encore financière (dans le cadre d'une entreprise, on parle d'actif immatériel), ce patrimoine doit être protégé efficacement.

À l'heure où les solutions d'archivage numérique sont de plus en plus nombreuses, dans le contexte de l'adoption de nouvelles règles luxembourgeoises modernisant le cadre légal et facilitant l'accès à un archivage électronique à valeur probante, nous constatons que le marché de la dématérialisation tente de s'approprier le monde du coffre-fort électronique. Cette appropriation, facilitée par l'ambiguïté entretenue entre les notions de coffre-fort électronique, d'espaces de stockage, de backup, d'archivage ou encore d'archivage à valeur probante, est de nature à semer la confusion parmi les utilisateurs. Ces derniers, à commencer par les chefs d'entreprises, sont soucieux d'offrir le meilleur avenir à des informations numériques dont l'importance et la valeur sont de moins en moins sous-estimées. On parle d'ailleurs de plus en plus d'actifs informationnels de l'entreprise.

Or, un coffre-fort électronique et une solution d'archivage numérique relèvent de deux visions distinctes. Le premier fonde sa raison d'être sur le secret et l'hyper-sécurisation de son contenu, alors que la seconde s'inscrit dans l'optique de la pérennisation des documents dans le cadre d'un cycle de vie défini.

Le stockage numérique à vocation pérenne est soutenu par une industrie qui a très bien compris les enjeux économiques : en 2009 on estimait que 0,8 Zb de données étaient stockées dans le monde, alors qu'il est prévu que plus de 35 Zb d'informations soient stockées en 2020, soit un facteur de 44 en dix ans<sup>1</sup>.

Néanmoins, la notion de secret et les espaces de réelle confidentialité sont peu développés dans un monde où le secret est vite associé à la fraude. Pourtant, on trouve aujourd'hui une réponse à ce besoin sécuritaire grâce à de véritables forteresses numériques.

Ce document vise à leur donner une définition et à lister les champs d'application.

Ce document est rédigé à l'attention des personnes désireuses de mieux comprendre les fondements qui distinguent un coffre-fort électronique de nombreuses solutions qui en empruntent le nom ou l'image. Particulier ou gestionnaire d'entreprise, employé d'une entreprise privée ou d'une organisation publique, chaque lecteur doté d'un léger bagage informatique sera à même de comprendre à la fois les spécifications et les enjeux que présente cet outil qui ne se développe que depuis quelques années.

---

<sup>1</sup> IDC Digital Universe Study, Mai 2010

## II. Définition du coffre-fort électronique

---

### 1. Définition générale

---

Un **[coffre-fort électronique]** est un **[espace virtuel de stockage et de conservation]** **[sécurisé]** et réputé **[inviolable]** permettant de **[restituer]** **[ce]** qui y a été **[déposé]** **[sans altération]**.

Cette définition est générale, c'est-à-dire qu'elle s'applique à tous les contextes, au Luxembourg ou ailleurs. Les termes entre crochets de la définition sont expliqués plus en détail dans les sections suivantes.

#### a) Coffre-fort électronique (ou CFE)

---

L'acronyme CFE est utilisé pour désigner un « coffre-fort électronique », un « coffre-fort virtuel », un « coffre-fort numérique » ou encore un « e-vault ». La définition qui en découle se différencie d'un backup, d'un archivage ou d'un répertoire virtuel. Le chapitre III développe ces différences.

#### b) Espace virtuel de stockage et de conservation

---

Le terme « espace virtuel » renvoie à une abstraction physique du stockage. Les données peuvent se trouver à n'importe quel endroit au niveau physique, ou même être fragmentées entre plusieurs supports et sites (par exemple dans un système de cloud computing). Néanmoins, ce terme n'exclut pas qu'un espace physique soit clairement identifié voire exigé, par exemple, pour satisfaire à des obligations réglementaires.

Le stockage et la conservation renvoient à l'obligation d'un CFE de permettre l'enregistrement de tous types et formats de données ou documents numériques et de maintenir leur accessibilité dans le temps, et ce dans leur état d'origine depuis leur dernier accès. La durée de conservation est illimitée, bien qu'une fin puisse être envisagée (voir par exemple le chapitre IV.3). Un CFE ne doit cependant pas garantir la pérennité des documents, qui relève de l'obligation de lisibilité et d'intelligibilité des documents dans un contexte d'archivage électronique (en procédant à des conversions de formats pour pallier à l'obsolescence informatique par exemple). L'utilisateur propriétaire des données dans le CFE doit être conscient qu'il est préférable de déposer des données dans des formats réputés pérennes (voir Annexe A) par les organisations internationales qui ont autorité en la matière (ISO, W3C, OASIS, Archives nationales...).

## c) Sécurisé

---

Le terme « sécurisé » englobe l'ensemble des moyens techniques et organisationnels garantissant la disponibilité et la confidentialité des données déposées au CFE.

Deux points sont importants dans le terme « sécurisé » :

- la protection logique (confidentialité des données), qui comprend :
  - la gestion des accès (autorisés et non autorisés) ;
  - le chiffrement (PKI et gestion / renouvellement des clefs) ; et
  - la protection contre la copie non autorisée de données
- la protection physique, qui comprend la capacité de mettre des données interprétables hors de portée d'un danger tel que :
  - le vol d'un support physique ; et
  - la destruction ou l'altération (par ex : incendie, dégât des eaux).

Le cryptage des informations et des documents déposés dans le CFE peut se faire sur le poste client ou sur le serveur applicatif, ce qui peut ajouter une garantie supplémentaire vis-à-vis de la confidentialité lors du transfert ou lors de la conservation.

Dans le cas du cryptage sur le serveur applicatif, le cryptage des échanges entre l'utilisateur et son CFE (la couche de transport) doit permettre d'échanger des informations entre deux ordinateurs de façon sûre. Il doit assurer trois fonctions :

1. Confidentialité : éviter l'espionnage des informations échangées,
2. Intégrité : ne pas pouvoir modifier les informations échangées, et
3. Authentification : s'assurer de l'identité du programme ou de la personne physique ou morale avec lequel la communication est établie.

## d) Inviolable

---

Le terme « inviolable » représente la qualité de ce qui est à l'abri de tout accès non autorisé.

Cela implique donc la mise en œuvre d'un ensemble de moyens techniques et organisationnels empêchant toute intrusion et garantissant un haut niveau d'invulnérabilité du CFE.

## e) Restituer

---

Le terme « restituer » souligne l'obligation de tout CFE de remettre à leur propriétaire les données que celui-ci a déposées dans son CFE (dans l'état dans lequel elles se trouvaient lors de leur dernier accès).

Ce qui est déposé par l'utilisateur est une suite de bits (voir la définition des termes « ce » et « déposé » plus bas), et ce qui doit être restitué par le CFE est cette même suite de bits. De même, cette suite de bits est dans un certain format, et c'est ce même format qui doit être restitué.

#### f) ce

---

L'item pouvant être stocké dans un CFE peut être toute donnée informatique dans le format livré par l'utilisateur représentant, par exemple (sans limite d'exhaustivité) :

- des sons,
- des images fixes ou vidéos,
- du texte,
- des documents : livres, contrats, assurances, factures, copies d'actes notariés,
- des formats de données propriétaires (applicatif, base de données, etc.),
- des données XML (facturations, impôts, certificats, etc.), ou encore
- des fichiers exécutables.

#### g) Déposé

---

Le dépôt vise le stockage organisé de données qui ont fait l'objet d'un enregistrement électronique. Le dépôt électronique est confié au CFE qui va le centraliser ou le décentraliser géographiquement ou logiquement. Il est le plus souvent organisé dans une ou plusieurs bases de données ou dans des fichiers. Les données doivent toutes pouvoir être localisées en vue de leur restitution.

L'adjectif « déposé » qualifie l'action de déposer. Il véhicule, comme schématisé avec la Figure 1, les notions :

- d'Objet (qui ?/quoi ?),
- de Positionnement à un endroit identifié (où ?),
- de Quantité (combien ?),
- de Temps (quand ?), et
- de Moyen (comment ?).

## h) Sans altération

Dans le cadre d'une information ou d'un document numérique, restituer « sans altération » signifie qu'il faut être en mesure de restituer « bit pour bit » ce qui a été déposé.

Cela induit un maintien de l'intégrité entre le dépôt et la restitution d'une information ou d'un document. Le CFE a pour obligation de mettre en œuvre tous les moyens techniques et organisationnels pour garantir cette intégrité.

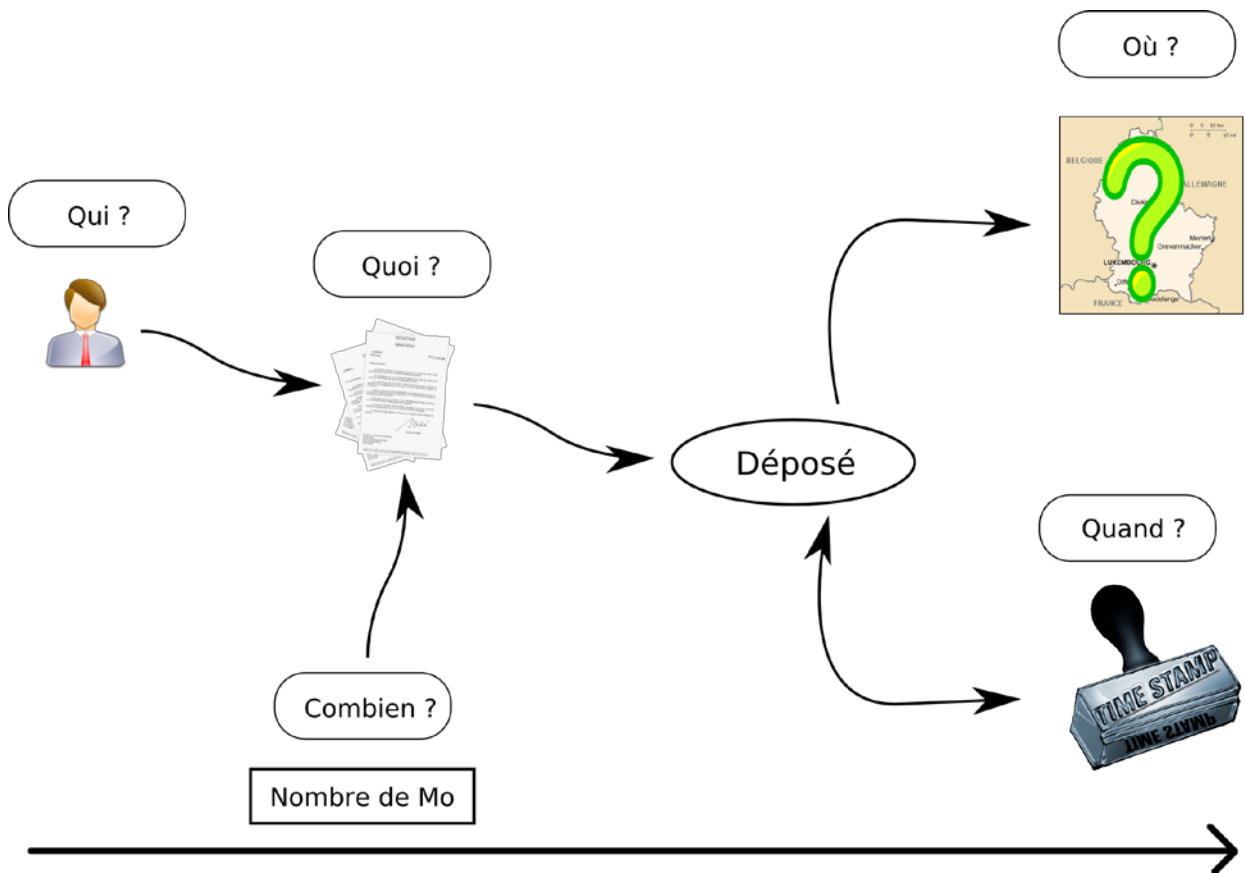


Figure 1. L'action « déposé »

## 2. Éléments-clefs du CFE

On peut considérer que des facteurs d'inviolabilité et de gestion des accès peuvent assurer une réelle solidité au CFE. L'authentification forte est dès lors une fondation essentielle du CFE, c'est en quelque sorte une réelle exigence qui caractérise le CFE et c'est sur cette base que vont se placer des garanties attendues par l'utilisateur. Les différentes garanties sont :

- l'authentification forte,
- l'autorisation ou contrôle d'accès (qui peut y avoir accès),
- la confidentialité (qui peut le voir),
- le droit de modification (qui peut le modifier), et
- la traçabilité (qui l'a fait).

On peut schématiser l'empilement de ces garanties comme sur la Figure 2.

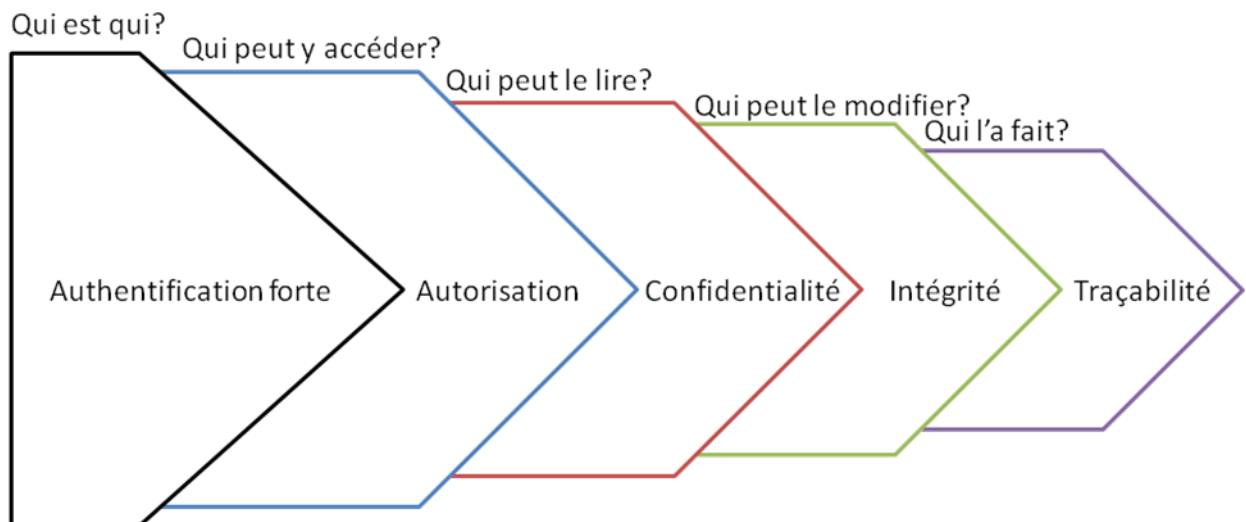


Figure 2. Pyramide des garanties

Chacune de ces couches repose sur, et nécessite, une couche inférieure forte. La traçabilité qui culmine au sommet, ne peut s'établir que sur de saines fondations. Un système ne pourrait être qualifié de CFE s'il ne respecte pas ces garanties.

### III. Différences entre CFE et autres systèmes

Afin de bien différencier le CFE des systèmes avec lesquels il est parfois confondu, le tableau suivant reprend les exigences de différentes appellations. Les exigences dans le tableau sont définies et détaillées en Annexe B. La méthode dite MoSCoW (l'acronyme MoSCoW signifiant (en anglais) : M - MUST have this (DOIT l'avoir), S - SHOULD have this if at all possible (DEVRAIT l'avoir, si possible), C - COULD have this (POURRAIT l'avoir), W - WON'T have this (NE L'A PAS)) a été utilisée.

Fonctionnalités	CFE	Système d'Archivage électronique	Backup	Stockage en ligne, répertoire virtuel
<b>Rétention</b>				
Période de rétention sur chaque groupe d'objets	W	M	W	W
Période de maintien opérationnel du contenant	M	W	M	S
<b>Protection du contenu</b>				
Chiffrement du contenu	M	C	C	C
<b>Contrôle d'accès</b>				
Accès au déposant	M	C	C	C
Accès à des tiers	C	C	C	C
<b>Fonctions</b>				
Plan de classement	C	M	W	W
Horodatage certifié	C	M	W	W
Conversion des formats (en entrée)	C	S	W	W
Conversion des formats (au sein de la solution)	W	M	W	C
Disponibilité (QoS)	S	C	C	M

Fonctionnalités	CFE	Système d'Archivage électronique	Backup	Stockage en ligne, répertoire virtuel
<b>Authenticité</b>				
Signature électronique	S	S	C	C
<b>Intégrité</b>				
Intégrité (bit par bit)	M	M	S	S
Intégrité avec évolution des données	W	M	W	C
Lisibilité dans le temps	W	M	C	W
<b>Confidentialité</b>				
Confidentialité (contenu secret) vis-à-vis de tiers	M	C	C	C
Confidentialité vis-à-vis d'administrateurs du système	M	S	C	S
<b>Protection</b>				
Protection logique des données	M+	M	M	S
Protection physique ( <i>facilities</i> )	M	M	M	M

#### IV. Services associés

---

Ce chapitre permet d'énumérer les différents services que l'on peut être amené à déployer ou qui peuvent être proposés dans le cadre d'un CFE.

Parmi ces services, les plus fréquemment rencontrés sont l'horodatage, la signature électronique et la restitution des données.

## 1. Horodatage

---

L'horodatage est un mécanisme qui consiste à associer une date et une heure certaines à des données. Cela permet, dans le cas d'un CFE, de connaître précisément le moment auquel des données ont été traitées et placées dans le CFE.

Plusieurs méthodes peuvent être utilisées, la plus sûre étant d'avoir recours à un tiers-horodateur de confiance respectant la norme RFC 3161 (*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*). Néanmoins, ce procédé a un coût, et il peut parfois être intéressant, pour des données de faible valeur ou en fonction des besoins, d'utiliser un système d'horodatage interne au système de CFE, voire de ne pas horodater.

## 2. Signature électronique

---

Dans le contexte d'un CFE, la signature électronique a deux fonctions principales :

- identifier le signataire, et
- assurer l'intégrité du document signé.

Un item déposé dans un CFE ne doit pas nécessairement être signé électroniquement. Il convient d'ailleurs de noter que, si cette possibilité peut être offerte par un prestataire de service, elle n'aura pas nécessairement pour effet de faire de l'item signé électroniquement un document électronique conforme à l'original offrant une valeur probante reconnue (par exemple, scanner un diplôme et le déposer dans un CFE avec une signature électronique ne fait pas nécessairement de ce document scanné une copie présumée conforme à l'original).

À noter que toute signature électronique (au sens de la loi luxembourgeoise) repose normalement sur un certificat électronique possédant une durée de validité limitée (qui ne peut excéder trois ans). En outre, les techniques (notamment cryptographiques) utilisées pour créer une signature électronique (et qui sont garantes notamment de la non-répudiation et de l'intégrité des données) tendent à devenir vulnérables, voire obsolètes, dans le temps.

### 3. Restitution des données

---

La restitution peut viser à la fois la restitution complète du contenu d'un CFE ou la simple consultation ou accès aux données y stockées.

Dans le cas du CFE, l'accès aux données et la consultation/modification de celles-ci font partie intégrante du système et de la définition.

Un CFE ne doit pas être ouvert par un tiers non autorisé par le propriétaire et les données doivent rester cryptées.

Néanmoins, l'ouverture d'un CFE pourrait être permise à un tiers de confiance comme un service ou une option. Pour ce faire, il faut que la récupération de la clef privée du propriétaire soit possible ; trois solutions sont proposées :

- la clef est séparée en deux parties, une moitié dans le CFE et chiffrée par une clef appartenant au prestataire, et l'autre moitié chiffrée chez un tiers (banque, etc.), ou
- l'entièreté de la clef est déposée chez une autorité de séquestre, ou
- la clef est séparée en multiples parties chez des tiers de confiance désignés par le propriétaire du CFE.

Lors d'une rupture de contrat (lors du décès avéré du propriétaire ou de non-paiement, par exemple), la clef peut donc dans ces cas être récupérée, ainsi que les données du CFE. Le CFE pourra donc, si cela est prévu dans le contrat, être « ouvert » et les données décryptées pourront être cryptées avec la clef globale du prestataire, permettant de garder ces données à un moindre coût pour le prestataire dans un CFE commun avec toutes les données des CFEs en rupture de contrat. Les données ne seront donc plus dans un espace personnel. De plus, les données seront lues (mais ne devront pas être interprétées) par le prestataire lors de l'ouverture du CFE personnel et du versement des données dans le CFE commun, analogie avec ce qui peut se passer dans une banque quand un client rompt le contrat, et que son coffre physique est ouvert pour placer son contenu dans un coffre global. Néanmoins, le prestataire de CFE pourrait avoir la possibilité de supprimer, si cela est spécifié dans le contrat, le contenu d'un CFE après une certaine durée prévue au contrat ou si d'autres événements se produisent (par exemple, la résiliation du contrat ou le décès du propriétaire).

Dans l'hypothèse où le contrat prévoit la conservation des données du CFE, la restitution devrait pouvoir se faire sans limite de temps. Le prestataire devrait alors garder les données du CFE pendant la période prévue au contrat

Enfin, l'export des données et de la structure des différents dossiers qui auraient pu être créés devrait idéalement être supporté de manière normalisée, pour permettre de changer facilement de prestataire de CFE, grâce à un export normalisé et structuré, et un import de ces données dans le nouveau CFE.

#### 4. Autres services

---

Un CFE peut également proposer des fonctionnalités telles que :

- le dépôt d'informations dans le CFE (afin de faciliter les dépôts, le CFE met à disposition de l'utilisateur des logiciels simples à utiliser et/ou des procédures simples à suivre), par le détenteur du CFE ou tout autre tiers autorisé,
- le classement de l'ensemble des documents déposés dans le CFE,
- la gestion des droits d'accès au CFE (afin de définir les dossiers ou sous-dossiers qui pourront être partagés avec d'autres utilisateurs autorisés par le propriétaire, issus de la sphère familiale (conjoint, enfants, parents, ...), de la sphère privée (fournisseurs divers, assureurs, banques, notaires,...) et/ou de la sphère professionnelle ou administrative (employeur, commune, école, ...) du propriétaire,
- la récupération et la transmission des documents à tout moment, en tout lieu et en toute occasion,
- la génération d'alarmes sur les documents déposés au CFE, pour par exemple prévenir de l'expiration d'un document d'identité, ou de l'échéance d'un abonnement,
- la connaissance et le suivi des accès au CFE et des manipulations effectuées sur les documents qui y sont déposés (journalisation – inscription dans un registre comme à la banque –, traçabilité),
- l'export d'un document vers un SAE (Système d'Archivage Electronique),
- la conversion en un format pérenne avant le dépôt (uniquement après acceptation et validation du résultat par le propriétaire),
- l'optimisation du poids des images,
- la possibilité de faire des actions sur les fichiers, apportant à l'utilisateur final une meilleure utilisation de son CFE, ou encore
- la possibilité d'une anonymisation du CFE.

## V. Catégorisation des contenus

---

Après avoir abordé quels outils, applications et services pouvant graviter autour du CFE, ce chapitre traite de l'information, qui peut être signée électroniquement, ainsi que des garanties attachées à cette technique.

La Figure 3 détermine des catégories de types de données pour lesquelles la signature électronique plus ou moins poussée est d'application. La Figure 3 illustre donc les trois niveaux que nous pouvons distinguer :

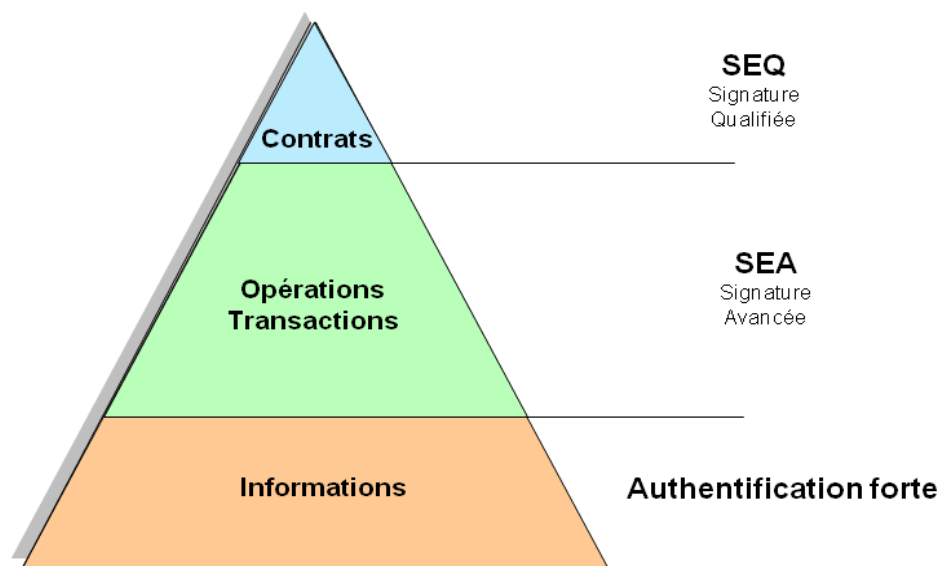


Figure 3. Pyramide des types d'information et leur méthode d'authentification associée

La base de ce triangle, qui représente le nombre le plus conséquent de données, ne nécessite pas d'élément externe certifiant leur conformité à un original ou à la réalité. On parle ici d'indices ou de renseignements (et pas nécessairement de preuve), ou encore d'éléments qui attestent ou complètent un dossier, **d'informations en général**. Cette première couche sera considérée comme fiable si l'application permet une authentification forte de l'utilisateur pour garantir la source. À titre d'exemple, on pourra classer dans cette catégorie des factures électroniques (électricité, téléphone, etc.), des fiches de salaire, des relevés de comptes, etc.

La couche intermédiaire peut être utilisée pour une majorité de **transactions**. L'ensemble des informations repris dans cette zone doit être signé avec une signature électronique au sens de la loi

luxembourgeoise (une signature dite avancée peut suffire selon les cas) afin d'apporter des garanties quant à la validité et l'intégrité de l'information. À titre d'exemple, on pourra classer dans cette catégorie des instructions de transfert bancaire.

La couche qui symbolise la pointe de la pyramide représente les données les plus sensibles, en plus faible quantité mais nécessitant un traitement particulier. Cette couche pourra par exemple être utilisée pour les **contrats**. Les pièces ici reprises devront être signées au moyen d'une signature électronique reconnue (c'est-à-dire d'une signature qualifiée) et non répudiable. À titre d'exemple, on classera dans cette catégorie des contrats, annexes ou avenants entre une société et ses clients, mais aussi des pièces administratives numériques (par exemple la déclaration fiscale, des extraits de registres du commerce).

## VI. Positionnement et perspectives du CFE

Afin de positionner le CFE sur la place luxembourgeoise, il est essentiel de déterminer les éléments de commercialisation qui feront un succès de la solution. Par quels éléments une entreprise luxembourgeoise peut-elle commencer sa démarche de dématérialisation de l'information sans prendre de risques inconsidérés ?

Sur base de la pyramide des signatures vue précédemment, grâce à la mise en place d'un CFE, une entreprise ne prend pas beaucoup de risques si elle se contente de traiter des informations situées dans les niveaux inférieurs, sans valeur juridique, à valeur informationnelle.

Pourtant, il est possible de rapprocher le CFE d'un système d'Electronic Records Management (e-archiving). Une proposition d'approche du marché est proposée en Figure 4, en considérant le flux de gauche à droite.

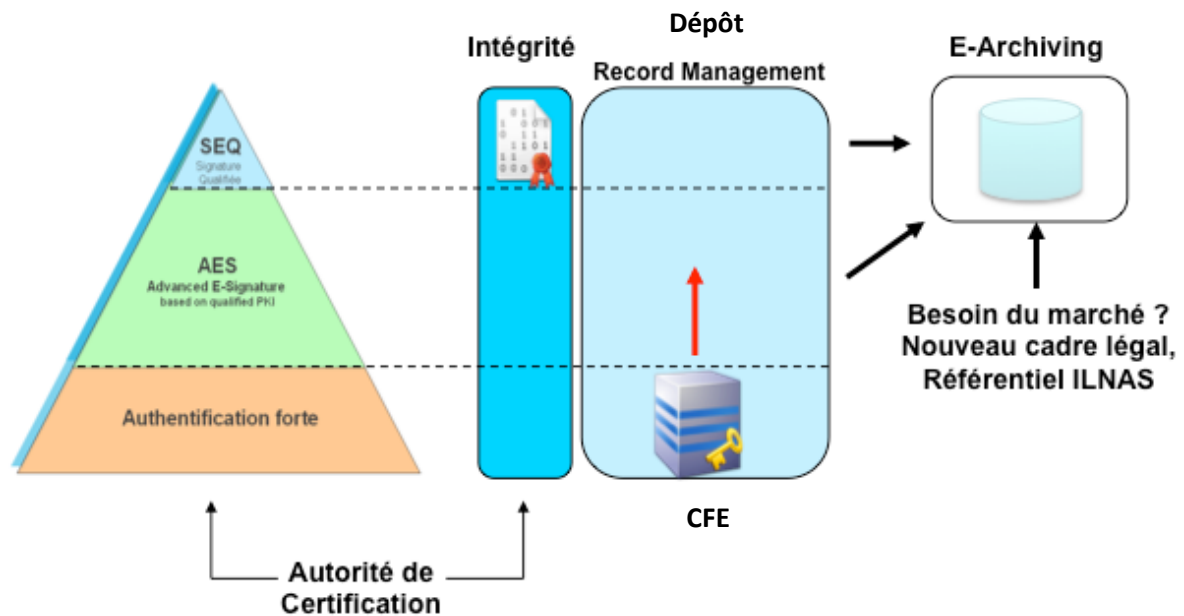


Figure 4. Approche d'après le flux

Dans un contexte légal et connu, il appartient à chaque entreprise de déterminer ses propres risques opérationnels, de savoir où vont se positionner les différentes pièces échangées par les parties.

La qualité de la signature afférente aux différents niveaux de la pyramide est essentielle et l'entreprise doit veiller à ce que la politique de signature soit bien respectée par rapport aux exigences des différents niveaux opérationnels de la pyramide. Une fois le système de catégorisation mis en place, l'entreprise sera en mesure de positionner ses informations dans un dépôt. Ce dépôt est un endroit où sont placées les données qui font partie d'un objet qui est stocké dans un dossier. Les données peuvent être en transit sur cet espace, mais elles peuvent également être conservées à long terme, sans subir la moindre modification.

À l'heure actuelle, les informations contractuelles signées de façon manuscrite ainsi que les documents sont stockés et souvent dématérialisés pour des raisons de productivité interne. Le contrat est un élément pivot qui détermine le cadre de la relation produit-service entre un fournisseur et son client. Grâce à l'intégration dans ces flux de la signature électronique qualifiée (SEQ), une dématérialisation complète du flux end-to-end sera possible et plus aucune intervention non-numérique ne sera utile (contrat sur support numérique exclusif). Dans ce scénario, la pérennité de ces documents doit être garantie dans le temps.

Le niveau le plus bas est un niveau informationnel. Il englobe un grand nombre de documents ou d'informations qui sont des attributs au contrat.

La Figure 5 illustre la problématique des niveaux de complexité, de responsabilité, etc. qu'une société (un prestataire de CFE ou un "tiers-archivateur") est prête à assumer par rapport à son cœur de métier :

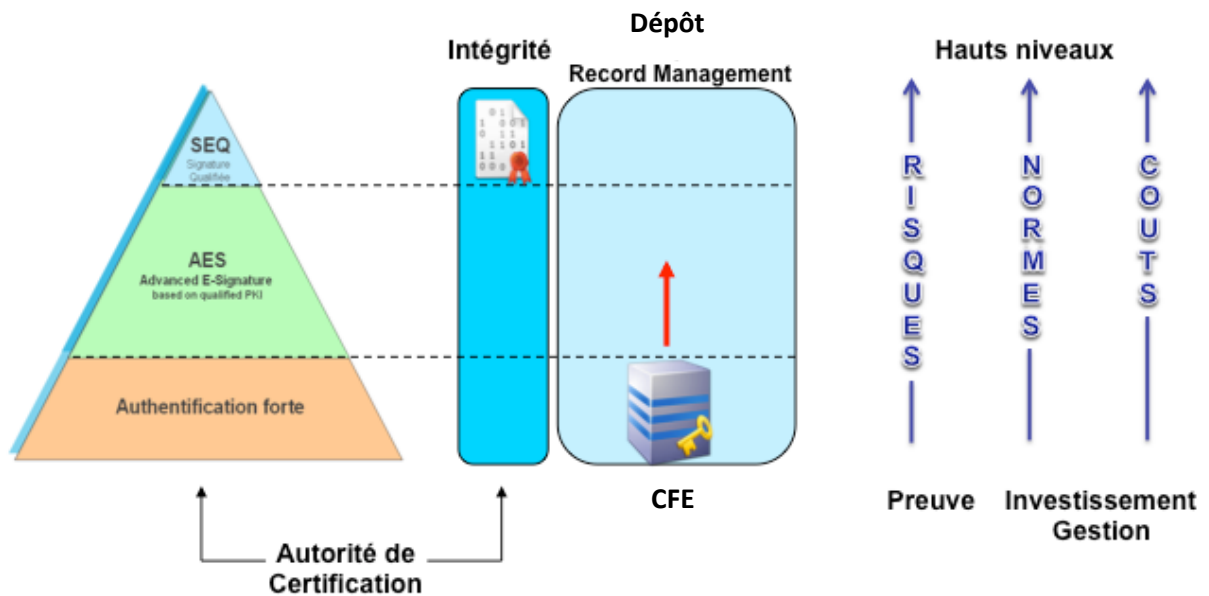


Figure 5. Niveaux de complexité d'un CFE

## VII. Contexte législatif luxembourgeois

---

Ce chapitre traite des différents aspects touchant au contexte législatif propre au Luxembourg, et ceci dans des domaines touchant au CFE : les données dématérialisées, la signature électronique, la cryptographie, la protection des données ainsi que les contrats. L'Annexe C donne pour sa part le contexte législatif propre aux coffres-forts physiques.

### 1. Contexte législatif sur les données dématérialisées

---

Plusieurs textes traitent des données dématérialisées. Le plus fondamental date du 22 décembre 1986. En effet, ce règlement grand-ducal énumère les critères permettant la reproduction fidèle et durable du document original, à savoir l'obligation :

- de procéder à la création des reproductions de façon systématique et sans lacune,
- d'effectuer et conserver des instructions de travail aussi longtemps que les reproductions ou enregistrements, ou encore
- de conserver les reproductions dans un ordre systématique et de les protéger contre toute altération.

Dans ce contexte, il est important de noter que l'article 1334 du Code civil précise que « *lorsque le titre original (acte sous seing privé papier) ou l'acte faisant foi d'original (acte sous seing privé électronique) n'existe plus, les copies effectuées à partir de celui-ci, sous la responsabilité de la personne qui en a la garde, ont la même valeur probante que les écrits sous seing privé dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été réalisées dans le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par règlement grand-ducal* ».

De même, il ressort de l'article 16 du Code du Commerce qu' « *à l'exception du bilan et du compte de profits et pertes, les documents ou informations visés aux articles 11 [...] peuvent être conservés sous formes de copie. Ces copies ont la même valeur probante que les originaux dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été réalisées dans le cadre d'une méthode de gestion régulièrement suivie et qu'elles répondent aux conditions fixées par un règlement grand-ducal* », c'est-à-dire aux règles énoncées ci-dessus.

Le règlement grand-ducal du 22 décembre 1986 est néanmoins obsolète sur de nombreux points nécessite une mise à jour. C'est notamment pour cette raison qu'un nouveau cadre de loi autour de l'archivage électronique et sur la conservation de données numériques devrait voir le jour prochainement.

### 2. Contexte législatif sur la signature électronique

---

Une signature électronique est un procédé qui garantit l'intégrité des données, l'identification du signataire, son adhésion au contenu de l'acte et assure sa non-répudiation. Une signature électronique

conforme aux exigences légales luxembourgeoise fournit en théorie une meilleure sécurité qu'une signature manuscrite.

La directive européenne 1999/93/CE du 13 décembre 1999 définit le cadre légal communautaire pour les signatures électroniques. Celle-ci établit qu'une signature avancée est « *une signature électronique qui satisfait aux exigences suivantes :*

- a) être liée uniquement au signataire ;*
- b) permettre d'identifier le signataire ;*
- c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et*
- d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable. »*

Au Luxembourg, cette directive a été transposée par la loi modifiée du 14 août 2000 *relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93 relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers* (Art. 18). Cette loi introduit entre autres le fait qu'une signature ne peut être refusée par un juge simplement à cause de sa nature électronique.

De plus, d'autres dispositions portant sur la signature électronique se retrouvent notamment dans le Code civil (Art. 1322-1, 1322-2, 1325 et 1326) et dans le *Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement et à la création du comité «commerce électronique»* (Art. 1-4).

Enfin, l'article 1322-2 du Code Civil dispose qu'un « *acte sous seing privé électronique vaut comme original lorsqu'il présente des garanties fiables quant au maintien de son intégrité à compter du moment où il a été créé pour la première fois sous sa forme définitive* ». De plus, l'article 1322-1 donne une définition de la signature électronique, à savoir qu'elle « *consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité* ».

### 3. Contexte législatif sur la cryptographie

La cryptographie au Luxembourg est encadrée par la *loi modifiée du 14 août 2000*.

L'article 3 de la *Loi modifiée du 14 août 2000* définit que l'usage de la cryptographie est libre au Grand-duché de Luxembourg. Des restrictions existent néanmoins à l'exportation de techniques de cryptage selon le règlement communautaire 428/2009/CE sur du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage.

#### 4. Contexte législatif sur la protection des données

---

Au Luxembourg, la Commission nationale pour la protection des données (CNPD) est chargée du respect de la législation en matière de protection des données, et notamment la loi modifiée du 2 août 2002 sur la protection des personnes à l'égard du traitement des données à caractère personnel et la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques applicables dans le secteur des communications électroniques.

La CNPD est chargée de contrôler et de vérifier la légalité des traitements des données à caractère personnel et doit assurer le respect des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel.

Les données à caractère personnel déposées dans un CFE doivent bien entendu être traitées en conformité avec la loi. Ces données peuvent contenir des données personnelles déposées par le propriétaire. Ces données peuvent porter sur le propriétaire même mais aussi sur des tiers. Dans ce cas, le prestataire agit comme sous-traitant du propriétaire dans la conservation de ces données, ce qui implique des obligations fortes pour les deux parties (éventuellement punies de sanctions pénales en cas de non respect), notamment l'obligation d'avoir un contrat de services écrit comportant certaines clauses imposées par la loi. Par définition, il est en effet impensable qu'un prestataire utilise à son profit ou pour ses propres finalités les informations que recèle un CFE. Enfin, le prestataire sera tenu de mettre en place des mesures de protection de la sécurité et de la confidentialité des données contenues dans le CFE.

En outre, le prestataire pourra être amené à collecter des données sur le propriétaire (ou des tiers auxquels le propriétaire accorde un accès au CFE), comme, par exemple, les noms, prénoms, adresse postale, adresse de courrier électronique et autres données comme les pays et communes de résidence et qui seront transmises par le propriétaire lors de l'entrée en relation contractuelle. Le prestataire devra traiter ces données de manière conforme à la loi, en notifiant ou au besoin en obtenant l'autorisation préalable de la CNPD selon les cas.

L'utilisation de ces données à des fins commerciales devra être particulièrement surveillée (même si elle n'est pas interdite *a priori*).

## 5. Validité des conventions

---

Quatre conditions sont essentielles pour la validité d'une convention :

- le consentement de la partie qui s'oblige,
- sa capacité de contracter,
- un objet certain qui forme la matière de l'engagement,
- une cause licite dans l'obligation (Art. 1108 du Code civil).

Dans le cas du CFE, deux cas peuvent se rencontrer. Dans le premier cas, pour un particulier, l'entrée en relation se fera le plus souvent *via* Internet par la transmission de ses coordonnées (vraies ou fausses) ainsi que par l'adhésion en ligne aux conditions générales entourant la fourniture du service par le prestataire. Dans le deuxième cas, il peut s'agir d'une adhésion en signant un contrat spécifique ou négocié.

Il n'y aura donc pas toujours de rencontre « physique » entre les parties contractantes. À cet égard, rappelons que « *toute personne peut contracter, si elle n'en est pas déclarée incapable par la loi* » et que « *sont incapables de contracter, dans la mesure définie par la loi, les mineurs non-émancipés ainsi que les majeurs protégés au sens de l'article 488 du présent code* » (Art. 1123 et 1124 du Code civil).

Dans tous les cas, les termes du contrat sont un élément primordial à ne pas négliger lors de l'ouverture d'un CFE auprès d'un prestataire. Rappelons à ce propos que le titre donné à un contrat (par exemple, « contrat de louage de coffre-fort électronique ») ne lie pas le juge et que la détermination précise de tout contrat dépend de son contenu. Ainsi, un contrat présenté comme un contrat de CFE peut en réalité s'analyser en une simple mise à disposition d'espace de stockage (selon les termes du contrat et les obligations fixées au prestataire).

Le contrat doit donc préciser toutes les fonctionnalités offertes par le CFE, les obligations du prestataire en matière de qualité de service ainsi que de définir ce qu'il adviendra si certains événements se produisent, comme en cas de non-paiement ou de décès du propriétaire. Ainsi, par exemple, même s'il découle de la définition du CFE que ce dernier est à vocation *ad vitam aeternam*, la durée pourra être limitée par le biais d'un contrat dans le cas d'une externalisation du service.

## VIII. Pistes d'extension du document

---

Ce livre blanc est amené à être mis à jour périodiquement par les membres du Groupe de Travail FedISA Luxembourg sur le coffre-fort électronique. Les prochains sujets qui pourront être développés dans les mises à jour futures seront notamment :

- les perspectives d'un PSF dans le monde du coffre-fort électronique,
- des informations relatives à l'héritage,
- le cas de défaut de paiement,
- les CFEs dans le cloud,
- un développement des services associés au CFEs.

Et bien sûr, les développements législatifs à venir.

## IX. Conclusion

---

Ce livre blanc présente ce qu'est un CFE, ses fondements, et ce qui peut par exemple lui être attaché comme services ou options. Un CFE offre des garanties de restitution de l'intégrité d'un dépôt ainsi qu'un niveau de sécurité élevé et une confidentialité préservée, ce qui lui confère une place à part dans le monde des espaces et systèmes de stockage sur le marché, au même titre que les systèmes d'archivage électronique. Le CFE s'avère donc être un système efficace pour le dépôt d'informations et de documents qui doivent rester à l'abri de regards. Cela n'empêche en rien le partage dans une salle des coffres virtuelle (qui peut être matérialisée sous forme de communauté) mais le contrôle de l'accès à cette information de nature sensible est totalement maîtrisé.

À noter également que le CFE peut héberger tout type de document électronique, de l'information au fichier dans un format non pérenne, ce qui le différencie des autres solutions existantes, un système d'archivage électronique préconisera par exemple une analyse des documents, et optimisera et/ou convertira de formats avant le dépôt dans le système d'archivage électronique pérenne ou à valeur probante.

L'AFNOR est en train de définir les « Spécifications d'un composant « coffre-fort numérique » destinés à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps ». Un premier projet de ce document est attendu dans le courant du mois de juin 2011. Ces spécifications pourraient par la suite être mises en parallèle avec ce livre blanc. L'ISO développe aussi en parallèle un système similaire.

La thématique du CFE n'a donc jamais été aussi présente autour de nous, et continue à se développer, avec un marché ouvert et une demande réelle.

## Équipe rédactionnelle (par ordre alphabétique)

---

Remerciements au Groupe de Travail « Coffre-fort électronique » de FedISA Luxembourg : ci-dessous les personnes ayant activement contribué à la rédaction et présents aux groupes de travail.

### Lucas Colet (Centre de Recherche Public Henri Tudor) – Secrétaire

---

Titulaire d'un Master Recherche en Informatique, Lucas Colet travaille en tant qu'ingénieur de recherche et développement au sein du Centre de Recherche Public Henri Tudor au Luxembourg. Lucas est spécialisé dans la standardisation en Electronic Records Management (archivage électronique), et est devenu à ce titre président du comité miroir luxembourgeois ISO / TC 46 / SC 11 spécialisé dans l'archivage et le records management. Lucas pilote également le Groupe de Travail FedISA Luxembourg portant sur la thématique du Coffre-fort électronique, qui a développé le présent livre blanc.

### Alain Devroede (Euroscript)

---

Ingénieur de formation, Alain Devroede a plus de 10 ans d'expérience dans l'utilisation des technologies ECM et de leur implantation dans divers secteurs d'activité. Il est actuellement analyste business et consultant principal en ECM pour le groupe euroscript. A ce titre il participe notamment à la définition et au développement des nouvelles solutions ECM.

### Cédric Jadoul (Fujitsu Technology Solutions Luxembourg)

---

Titulaire d'un master en Informatique, Cédric Jadoul est responsable de la pratique « Information Management » chez Fujitsu Technology Solutions à Luxembourg. À ce titre Cédric est en charge du développement et du positionnement stratégique de l'offre de service de Fujitsu Luxembourg dans le domaine incluant les problématiques liées à l'information risk management, la collaboration, le web content management, le case management et l'archivage à valeur probante. Cédric Jadoul est également en charge de la mise en place de projets ECM chez plusieurs clients majeurs du secteur bancaire à Luxembourg.

### Xavier Lisoir (PricewaterhouseCoopers)

---

Diplômé de HEC Liège et titulaire d'une maîtrise en informatique de gestion, Xavier Lisoir est expert en stratégie, en système d'information et en optimisation de processus. Au sein de PwC Luxembourg, Xavier est en charge des services liés à la transformation digitale (GED, workflow, eArchiving, record management). À ce titre il a déjà été amené à accompagner de nombreux acteurs privés et publics de la place dans leurs réflexions stratégiques et leurs démarches de dématérialisation en leur permettant d'identifier correctement les enjeux et de saisir avec succès les opportunités offertes par les dernières évolutions technologiques, réglementaires, fiscales ou métier.

### Marie-Emilie Mengal (Entreprise des Postes et Télécommunications)

---

Licenciée en Droit de l'Université Catholique de Louvain, titulaire d'une Spécialisation en Droit et Gestion des Technologies de l'Information et des Télécommunications (DGTIC) des Facultés Universitaires Notre-Dame de la Paix de Namur, Marie-Emilie Mengal a débuté sa carrière dans le droit au sein du barreau d'Arlon avant de rejoindre l'Entreprise des Postes et Télécommunications Luxembourg en 2008 en qualité de conseiller juridique. A ce titre, elle est notamment en charge des questions juridiques relatives au Cloud Computing et à l'archivage électronique à valeur probante. Marie-Emilie s'intéresse également à la sécurité des systèmes d'information et vient d'obtenir un Certificat Universitaire de Formation Continué en Management de la Sécurité des Systèmes d'Information (INFOSAFE) à l'Ichec.

## [Frank Poireau](#)

---

## [Christophe Porte \(BGL-BNP Parisbas\)](#)

---

Titulaire d'un diplôme d'ingénieur de l'Ecole Polytechnique de Nantes, Christophe Porte est responsable du Centre de Compétences Gestion Documentaire de BGL BNP Paribas. Christophe est à l'origine de la mise en place de solutions de gestion documentaires supportant des process critiques au sein de diverses entités du groupe BNP Paribas. Les solutions déployées dans différents pays ont pour objectif de répondre aux exigences légales et réglementaires et d'adresser des besoins stratégiques permettant à la banque d'optimiser ses processus métiers.

## [Frank Rockenbrod \(DEXIA-BIL\)](#)

---

Après ses études universitaires en facultés de Droits et Economie Industrielle, Frank Rockenbrod rejoint la Banque Internationale à Luxembourg SA en 1985. Poussé par son grand intérêt pour l'innovation, il assume par la suite la responsabilité de plusieurs grands projets stratégiques de Dexia-BIL, notamment en matière informatique (informatisation réseau des agences, refonte et migration d'applications frontend du mainframe), de sous-traitance (Cetrel, EBIS, Brinks, LuxTrust,..) et métiers (fusion bancaire, création du Electronic Banking et du WebBanking de DBL évolutions systèmes de paiements & clearing, monétique,...). Frank est maintenant Directeur et Responsable de l'Online Strategy pour l'intégration des innovations métiers de la banque de demain, et vice-président du CA de LuxTrust SA.

## [Pierre Van Wambeke \(SeeZam S.A.\)](#)

---

Ingénieur de formation et diplômé d'un MBA, Pierre Van Wambeke est un Entrepreneur du Net. Fondateur de SeeZam.com, premier coffre-fort virtuel en ligne basé au Luxembourg, Pierre a un parcours professionnel qui lui a permis de découvrir et de connaître le secteur financier et industriel de la place luxembourgeoise. Ancien consultant pour PricewaterhouseCoopers, Pierre Van Wambeke a dirigé l'informatique de l'Hôpital Kirchberg pendant 6 années, traitant ainsi des données médicales très sensibles et nécessitant de la haute disponibilité. Account Director Cargolux Services de 2007 à 2009, Pierre a quitté le secteur de l'aviation de Champ Cargosystems S.A. pour développer SeeZam.

## [Renaud Vanderoost \(Sogeti\)](#)

---

Renaud Vanderoost a plus de 15 ans d'expérience dans le domaine de la gestion de contenu (ECM). La force de ce consultant est d'avoir pu travailler, étudier et réfléchir sur les technologies Open-sources et propriétaires du monde de l'ECM. Cette compétence particulière lui a permis de faire de l'ECM une solution phare chez SOGETI et d'intervenir chez des clients comme CACEIS, Cactus, la Cour de Justice, la Commission... Aujourd'hui, il est responsable de la solution ECM pour Sogeti Luxembourg et accompagne des clients des secteurs publics et privés, dans leurs réflexions, démarches et réalisations de gestion de contenu ou de Knowledge Management.

### Gilles Vansteenkiste (CETREL)

---

Titulaire d'une licence en administration des affaires, Gilles Vansteenkiste est responsable de l'audit interne chez Cetrel à Luxembourg. Il a acquis son expérience chez Deloitte & Touche et Arthur Andersen dans l'audit financier et la consultance informatique. Il supervise les audits internes des processus comme la lutte contre la fraude ou l'archivage électronique autant que de les aspects informatiques comme la gestion de bases de données ou la politique de sécurité et coordonne les audits et certifications externes comme PCI-DSS, LuxTrust ou Multiline. Gilles Vansteenkiste représente également Cetrel au sein du groupe Sécurité des Moyens de Paiement et Instruments de l'ABBL.

## Annexe A. Pérennité

La plupart des fichiers créés avant les années 90 risquent d'être maintenant illisibles sans mettre en place de coûteuses mesures. Les raisons sont multiples, et sont le plus souvent relatives :

- à la connaissance perdue du contenu des fichiers,
- au format de fichier inconnu ou disparu,
- au support physique détérioré,
- au logiciel ou matériel de lecture disparu.

Le stockage pérenne de l'information numérique consiste à conserver le document et l'information qu'il contient :

- dans son aspect physique comme dans son aspect intellectuel,
- sur le très long terme (plus de 30 ans),
- de manière à pouvoir le rendre accessible et compréhensible.

Un format est jugé pérenne dès qu'il :

- est largement utilisé, et
- voit ses sources publiées.

De plus, on peut ajouter qu'il est conseillé de vérifier qu'il existe au moins deux solutions distinctes de deux éditeurs différents permettant d'interpréter le format.

Quelques exemples de formats jugés pérennes à l'heure actuelle :

- PDF/A-1 : ISO 19005-1,
- XML,
- TIFF Groupe 4,
- ODT,
- ...

Il est important de considérer ces formats avant de placer un document dans le CFE. En effet, ce document peut devoir être conservé assez longtemps pour que le problème de l'obsolescence dû au format se pose, et que ce document ne soit plus lisible lors de sa sortie du CFE. C'est en théorie au déposant de se préoccuper de cet état de fait en plaçant dans le CFE un document dans un format pérenne, le CFE n'ayant généralement pas de possibilité de conversion.

## Annexe B. Glossaire du chapitre III « Différences entre CFE et autres systèmes »

### RETENTION

#### Période de rétention sur chaque groupe d'objet

Période de rétention définie sur l'objet (document, données) ou groupe d'objets à l'intérieur du système

#### Période de maintien opérationnel du contenant

Période d'opération définie pour le contenant / système (CFE, système d'archivage électronique, système de backup, etc.)

### PROTECTION DU CONTENU

#### Chiffrement du contenu

Le contenu est-il protégé par des méthodes de chiffrement ?

### CONTROLE D'ACCES

#### Accès au déposant

Est-ce que l'accès au contenu du système est accordé au déposant ?

#### Accès à des tiers

Est-ce que l'accès au contenu du système est accordé à des tiers ?

### FONCTIONS

#### Plan de classement

Est-ce que le système dispose d'un plan de classement ?

#### Horodatage certifié

Est-ce que le système nécessite un horodatage certifié, c'est-à-dire un horodatage fourni par une autorité certifiée, à l'opposé d'un horodatage à la réception par le système (voir chapitre IV.1) ?

#### Conversion des formats (en entrée)

Est-ce que le système nécessite le recours à une conversion de format des documents acceptés en entrée ?

### Conversion des formats (en sein de la solution)

Est-ce que le système propose une solution de conversion de format assurant la pérennité ?

### Disponibilité (QoS)

Est-ce que l'accès aux données doit être garanti avec une forte qualité de service (disponibilité à 99,9% par exemple) ?

## **AUTHENTICITE**

### Signature électronique

Le contenu est-il authentifié grâce à une signature électronique ?

## **INTEGRITE**

### Intégrité (bit par bit)

Est-ce que le système possède une procédure permettant de garantir l'intégrité bit par bit de l'information stockée ?

### Intégrité avec évolution des données

Est-ce que le système possède une procédure permettant de garantir l'intégrité de l'information lors de changements de l'information, par exemple lors de la mise à jour / modification d'un fichier ?

### Lisibilité dans le temps

Est-ce que le système propose des mécanismes permettant aux données d'être lisibles dans le temps (par exemple en proposant la migration des formats) ?

## **CONFIDENTIALITE**

### Confidentialité (contenu secret) vis-à-vis de tiers

Est-ce que le système permet à l'information stockée de ne pas être divulguée à des tiers ?

### Confidentialité vis-à-vis d'administrateurs du système

Est-ce que le système permet à l'information stockée de ne pas être révélée aux administrateurs ?

## **PROTECTION**

### Protection logique

Est-ce que le système et son contenu sont protégés d'une atteinte à leur intégrité logique ?

### Protection physique (*facilities*)

Est-ce que le système et son contenu sont protégés d'une atteinte à leur intégrité physique (vol, destruction par le feu, par un tremblement de terre, etc.) ?

## Annexe C. Contexte législatif sur les coffres-forts non-électroniques

Le contrat de coffre-fort physique peut être défini comme « *la convention par laquelle, moyennant paiement d'une somme convenue, la banque met à la disposition exclusive de son client une case blindée, munie d'une serrure à secret perfectionné, située généralement dans les caves spécialement gardées et aménagées pour assurer la conservation des objets qui y sont gardés* »<sup>2</sup>.

La qualification de la relation juridique qui découle de cette convention n'est pas simple d'autant que le législateur n'a ni défini, ni prévu de dispositions spécifiques au contrat de coffre-fort.

Néanmoins, « *suivant une opinion ancienne, le contrat de location de coffre-fort serait un contrat de dépôt, le banquier étant considéré comme le dépositaire salarié des valeurs déposées dans le coffre. Suivant une autre, il serait un contrat de louage de choses (...). La jurisprudence et la doctrine dominantes soutiennent aujourd'hui qu'il s'agit d'une forme de location (...)* »<sup>3</sup>.

Il est vrai que, pour le coffre-fort physique, l'usage veut que l'on parle plutôt de « location » de coffre-fort.

Mais, « *même si ce contrat en a effectivement certaines caractéristiques, la qualification de contrat de louage pur et simple n'est pas pleinement satisfaisante* »<sup>4</sup>.

« *Le contrat de coffre-fort est un contrat complexe, participant à la fois du contrat de louage de chose et du contrat de louage d'ouvrage et de service. Les auteurs oscillent entre la qualification de contrat innommé sui generis et la qualification de louage de chose assorti d'une obligation spécifique de surveillance* ».

En France, la Cour de Cassation qualifie le contrat de coffre-fort de contrat de garde<sup>5</sup>. Selon la Cour de Cassation française, « *le contrat de coffre-fort est un contrat qui contient une obligation de garde mais qui n'est pas un contrat de dépôt car le banquier ignore le contenu du coffre* »<sup>6</sup>. Ce n'est pas un contrat de bail car il ne donne pas accès à son client le libre accès à la chambre des coffres. Il s'agit d'un

---

<sup>2</sup> FREDERICQ, Traité de droit commercial belge, Gand, T.X., 1952, n° 214

<sup>3</sup> Guy Loesch et François Kremer, Le banquier face à la saisie-arrêt civile de droit commun in Droit bancaire et financier au Luxembourg, Recueil de Doctrine, Volume 2, Edition De Boeck & Larcier, 2004, pp.719

<sup>4</sup> BUYLE et DAUBIES, Le contrat de location de coffre-fort, in le droit commun du bail, éditions la Charte, 2006

<sup>5</sup> Cass (fr.) (1re ch. Civ.), 2 juin 1993, Bull. civ., n°197, p. 136

<sup>6</sup> Ce qui n'est pas forcément le cas au Luxembourg puisque le Code civil prévoit, dans son article 1931, que le dépositaire « ne doit point chercher à connaître quelles sont les choses qui lui ont été déposées, si elles lui ont été confiées dans un coffre fermé ou sous une enveloppe cachetée ».

contrat par lequel une banque loue un compartiment ou coffre dont elle assure la sécurité et auquel le client n'a accès qu'avec le concours du banquier : le contrat de coffre-fort ne constitue donc pas un contrat de location : pas de jouissance privative pour le client dès lors que l'accès est subordonné au concours du banquier. Le contrat de coffre-fort serait un contrat *sui generis* qui serait un contrat de garde."

En Belgique, le contrat de coffre fort est qualifié de « *contrat complexe s'apparentant à la fois au louage de choses et au louage d'ouvrages ou de services* »<sup>7</sup>.

En définitive, que ce soit au Luxembourg, en France ou en Belgique, « *quelle que soit la qualification retenue, les obligations qui découlent du contrat de coffre-fort sont de manière générale définies par référence au contrat de louage auquel est assorti une obligation de surveillance* »<sup>8</sup>, qui est essentielle au contrat ».

Il faudra donc surtout veiller à définir, dans la convention entre parties, les obligations découlant du contrat de coffre-fort.

---

<sup>7</sup> Bruxelles, 11 mai 2000, R.D.C., 2001, p. 833, note J.P.BUYLE et M. DELIERNEUX

<sup>8</sup> En Belgique, le tribunal de Commerce de Louvain a, dans une décision du 16 mai 19958, considéré que « un contrat de coffre-fort implique l'obligation, dans le chef de la banque, de garder et de conserver soigneusement les coffres et leur contenu. Ce devoir n'implique toutefois pas une obligation de résultat dans une telle mesure que la banque garantit aux locataires que le contenu du coffre reste intact. »

---

FedISA Luxembourg  
B.P. 1173 L-1011 Luxembourg