Coffre-fort électronique
Livre Blanc

Version 2

FedISA
Fédération
ILM, Stockage & Archivage
Luxembourg

FedISA
Fédération
ILM, Stockage & Archivage
Luxembourg

Avant-propos

Chers amis.

Le coffre-fort électronique est sans aucun doute un service d'avenir.

Grâce aux technologies de cryptage et de redondance, couplé aux réseaux ouverts et au cloud computing, il permet d'assurer la sécurité et la confidentialité des informations et des documents.

Il offre surtout l'extraordinaire avantage de mettre de hauts standards de sécurité et de disponibilité de l'information à la portée de tous, entreprises privées de toutes tailles comme organisations publiques, travailleurs indépendants et surtout aux citoyens.
Qui peut dire que ses informations et documents personnels sont totalement à l'abri de la destruction, de l'altération ou du vol?

Le coffre-fort électronique est en réalité le trait d'union entre grand public, archivage électronique et cycle de vie de l'information. Ce qui rend ces matières tangibles à l'homme de la rue, et surtout répond à ses besoins.

FedISA Luxembourg est donc particulièrement fière de vous présenter la seconde édition de son livre blanc sur le coffre-fort électronique.

Un document de grande qualité et qui a vocation à devenir une référence sur ce sujet.
Un travail réalisé par un groupe de travail dynamique dont je tiens ici à remercier chaque membre.

A tous, je souhaite bonne lecture.

Cyril Pierre-Beausse
Président de FedISA Luxembourg

Table des matières

CFE	Coffre-fort électronique
CFN	Coffre-fort numérique (au sens de la norme AFNOR NF Z42-020)
CNPD	Commission nationale pour la protection des données
IETF	Internet Engineering Task Force
ILNAS	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services
PKI	Public Key Infrastructure – Infrastructure à clef publique
PSDC	Prestataire de service de dématérialisation ou de conservation
SSCD	Secure Signature Creation Device – Dispositif sécurisé de création de signature
SAE	Système d'archivage électronique
SLA	Service Level Agreement – Contrat de niveau de service

Définitions et acronymes

Authenticité	Propriété selon laquelle une entité est ce qu'elle revendique être (ISO/IEC 27000 :2009) dont l'exactitude, la vérité ne peut être contestée et dont l'origine est indubitable.
Intégrité	Propriété de protection de l'exactitude et de la complétude des actifs (2.3) (ISO/IEC 27000 :2009).
Non-répudiation	Propriété selon laquelle on ne peut remettre en cause ni les parties signataires, ni la validité.
Interopérabilité	Propriété d'un produit ou d'un système dont les interfaces ont un certain niveau de compatibilité avec d'autres produits ou systèmes existants ou futurs et ce sans restriction d'accès ou de mise en œuvre.
Signature électronique	Donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification (Directive 1999/93/CE du Parlement Européen et du Conseil) et qui en garantit l'intégrité.
Certificat électronique	Attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne (Directive 1999/93/CE du Parlement Européen et du Conseil).
Certificat Qualifié	Un certificat qualifié est un certificat qui satisfait aux exigences visées à l'art. 2 du règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques et à la création du comité "commerce électronique" et qui est fourni par un prestataire de services de certification satisfaisant aux exigences de l'art. 3 de ce même règlement grand-ducal.
Signature électronique avancée	Donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification qui doit, en outre, d'une part, être liée uniquement au signataire et permettre son identification et, d'autre part, être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable[1] de manière unique au signataire;
Signature électronique qualifiée	Signature électronique avancée basée sur un certificat qualifié, ayant été faite à l'aide d'un dispositif sécurisé de création de signature. Les exigences quant à ce dispositif sont définies dans l'art. 4 du règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques et à la création du comité "commerce électronique".
Vérification de signature	Processus effectué par un vérificateur soit peu après la création de la signature électronique ou plus tard. Cela permet de déterminer si une signature électronique est conforme au certificat de signature électronique.

Définitions et acronymes

[1] *Art. 2. §2. de la Dir. sur les signatures électroniques*

Valeur probante	Caractère convaincant lui permettant d'emporter la conviction du juge[2] / Force déterminée par le législateur pour marquer l'intensité avec laquelle un mode de preuve lie le juge et les parties.
Cryptographie	Discipline qui englobe les principes, moyens et méthodes servant à la transformation des données afin d'en dissimuler le contenu informatif, empêcher sa modification sans détection ou empêcher son utilisation sans autorisation[3].
Backup (sauvegarde)	Action qui consiste à dupliquer les données contenues dans un système informatique, dans le but d'une éventuelle utilisation ultérieure.
SAE (Système d'Archivage Électronique)	Système de gestion de document qui interdit la modification et la destruction des documents pendant la durée de rétention, qui comprend un contrôle rigoureux des durées de conservation ainsi qu'une structure rigoureuse de classement et qui constitue un fonds sécurisé des documents probants[4].
Système de stockage en ligne	Système qui permet aux utilisateurs d'héberger des fichiers sur des serveurs distants.
Fournisseur de service de CFE	Personne physique ou morale ayant la propriété de la solution de coffre-fort électronique et étant garante des données y stockées. Peut être interne ou externe.
Emetteur	Personne physique ou morale autorisée à déposer des données dans le CFE d'un utilisateur.
Utilisateur d'un CFE	Personne physique ou morale ayant souscrit aux services d'un CFE.
Pérennité	Propriété d'un document qui reste lisible pendant tout son cycle de vie (adapté de ISO 14641-1) (cf. Pérennité).
Cloud computing (ou infonuagique)	Paradigme informatique permettant de mettre à disposition le concept de Computing as a Service, représentant l'utilisation de ressources distantes virtuelles, pour remplir des tâches (calcul, utilisation de logiciels, stockage, etc.). D'après le NIST (National Institute of Standards and Technology), le cloud computing est l'accès via le réseau, à la demande et en libre-service, à des ressources informatiques virtualisées et mutualisées.
PSDC (Prestataire de Service de Dématérialisation ou de Conservation)	Statut défini dans le projet de loi sur l'archivage électronique lié à une certification basée sur la « Règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation (PSDC) » éditée par l'ILNAS, permettant de faire reconnaître une organisation comme étant un tiers de confiance pour la dématérialisation des documents papier et/ou pour la conservation de données numériques.

***Note** : Une signature n'a de valeur que si elle peut être vérifiée.*

[2] *D. Et R. Mougenot, la preuve, 3e éd., Bruxelles, Larcier, 2002, n°14-2, p. 75 et n°6, p. 66*

[3] *Règl. (CE) No 428/2009 du Conseil, instituant un régime communautaire de contrôles des exportations de biens et technologies à double usage, http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc_143390.pdf*

[4] *Adapté du Tableau 1.1 tiré du modèle européen MoReq pour l'archivage électronique*

Quoi de neuf ?

chapitre

0

Ce livre blanc est une évolution du premier livre blanc publié par FedISA Luxembourg sur la thématique du coffre-fort électronique. Ce premier document donnait une définition générale de ce qu'est un CFE ainsi que les différences entre celui-ci et d'autres solutions proches (archivage électronique, stockage en ligne, backup). Enfin, il a également permis de placer le CFE dans le marché luxembourgeois, et de prouver son utilité.

Ce nouveau livre blanc permet de mettre le concept du CFE à la portée de tous, en éclaircissant tous les points d'ombre que ce genre de technologie pourrait soulever. En ce sens, les éléments les plus importants ont été encadrés tout le long du document, et des aspects ont été approfondis (par exemple la signature électronique).

Voici les éléments qui ont été ajoutés dans cette évolution :

- un glossaire et des définitions,
- un chapitre indicatif sur ce qui peut être placé dans un coffre-fort électronique,
- les fonctionnalités minimales d'un coffre-fort électronique.

Dans le même temps, des modifications ont été effectuées dans les chapitres existants. Ces modifications et ajouts permettent d'augmenter la lisibilité du document ainsi que sa compréhension, par l'ajout d'annexes approfondissant certains sujets (pérennité, législation, signature électronique).

Enfin, une nouvelle charte graphique a été instaurée.


Password:
****

Introduction et objectifs poursuivis

chapitre

1

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 technique 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.

Le CFE peut être considéré comme l'endroit idéal où stocker ses documents et informations sensibles, hors de portée d'un regard externe non désiré.

Et le sujet de la confidentialité des données est une préoccupation actuelle croissante!

En effet, 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. On parle d'ailleurs de plus en plus d'actifs informationnels de l'entreprise et on le valorise. Selon la nature de l'activité d'une entreprise, on déterminera son niveau de tolérance aux risques. Par exemple, une entreprise internationale, plus exposée aux litiges, aura surement un profil plus risqué qu'une entreprise locale.

IBM Research, au travers de Jan Camenisch, chef de projet Cryptography & Privacy, déclarait en fin novembre 2013 dans une conférence sur la sécurité de l'information tenue à Berne (CH) que nous avons un gros problème de sécurité : ce n'est pas seulement parce que des utilisateurs non autorisés peuvent accéder au contenu de notre ordinateur, mais également parce que nous ne savons pas ce qu'il va advenir de nos données.

Les données privées sont la nouvelle monnaie d'échange, internet vit des données privées. Il faut donc que nous les protégions.

À l'heure où le Luxembourg finalise l'adoption de nouvelles règles modernisant le cadre légal et facilitant l'accès à un archivage électronique à valeur probante, il nous a semblé utile de briser l'ambiguïté entretenue dans la plupart des pays entre les notions de CFE, d'espaces de stockage, de backup, d'archivage ou encore d'archivage à valeur probante.

Un CFE, vu sous une législation luxembourgeoise, fonde sa raison d'être sur le secret et l'hyper-sécurisation de son contenu. Ce document le rappelle, la législation luxembourgeoise sur la confidentialité des données n'impose pas de limite quant au niveau de cryptage des données (L'usage des techniques de cryptographie est libre)[5].

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

Le Luxembourg ne possède pas de législation propre au domaine du CFE, même si quelques dispositions éparses ont vocation à s'appliquer à ce type de service. Ce livre blanc permet d'asseoir ce concept et de lui donner un périmètre précis.

[5] *http://www.legilux.public.lu/leg/textescoordonnes/recueils/COMMERCE_ELECTRONIQUE/SIGNATURE_ELECTRONIQUE.pdf*

Définition du coffre-fort électronique

chapitre 2

Définition générale

La définition que l'on retiendra dans ce document pour le coffre-fort électronique est la suivante :

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. Les termes entre crochets sont expliqués plus en détail dans les sections suivantes.

[Coffre-fort électronique]

L'acronyme CFE est utilisé pour désigner un «coffre-fort électronique», un «coffre-fort virtuel» 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 6 (**Différences entre CFE et autres systèmes**) développe ces différences.

[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 versement ou leur dernier accès/modification. La durée de conservation est illimitée, bien qu'une fin puisse être envisagée (voir par exemple le chapitre **Restitution des données**).

Un CFE ne doit cependant pas garantir la lisibilité et l'intelligibilité des données comme le ferait un système 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 donc être conscient qu'il est préférable de déposer des données dans des formats réputés pérennes (voir Annexe B) par les organisations internationales qui ont autorité en la matière (ISO, W3C, OASIS, Archives nationales...). En effet, le CFE n'a ni accès aux informations stockées ni idée du format, contrairement à un système d'archivage électronique. Il ne peut donc pas les modifier en les convertissant pour assurer leur pérennité.

La gestion du contenu d'un CFE tient du propriétaire du CFE, et non au fournisseur du CFE. La durée de conservation peut donc être illimitée dans le CFE, mais certaines exigences légales auxquelles le contenu doit se confronter devraient être respectées par l'utilisateur du CFE.

[Sécurisé]

Le terme **sécurisé** englobe l'ensemble des moyens techniques et organisationnels garantissant la disponibilité, l'intégrité et la confidentialité des données déposées dans le 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 chiffrement (ou cryptage) des informations et des documents déposés dans le CFE peut se faire sur le poste client avant envoi des informations ou sur le serveur applicatif à l'entrée du CFE, ce qui peut ajouter une garantie supplémentaire vis-à-vis de la confidentialité lors du transfert ou lors de la conservation.

En plus du chiffrement du contenu du CFE, il est recommandé d'utiliser un canal de transmission sécurisé pour ces données afin de garantir la confidentialité et l'intégrité des échanges (voir *Figure 1*).

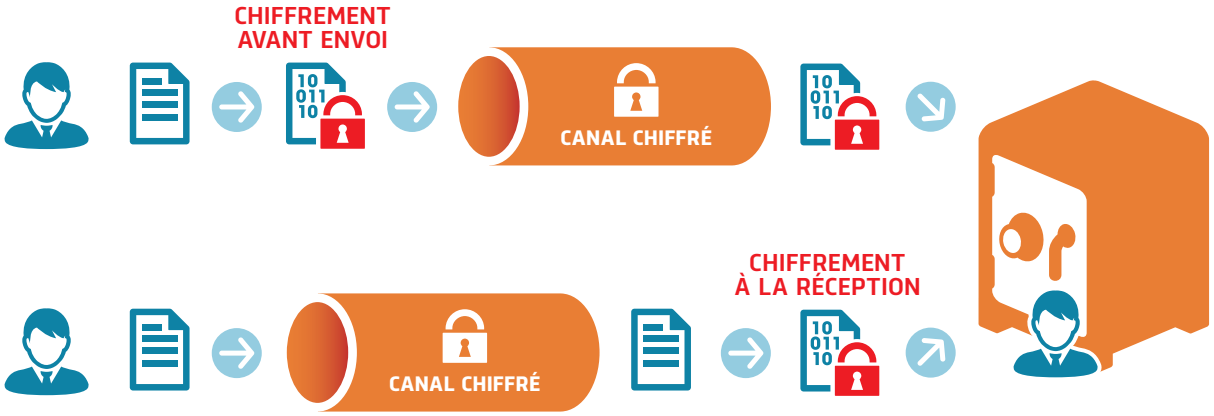

Figure 1. Chiffrement avant envoi ou après réception par le CFE :
l'envoi peut se faire par un individu ou par un système (automatisé ou non)

En effet, le chiffrement des informations sur le canal, établi entre l'utilisateur et son CFE, doit permettre d'échanger des informations entre deux ordinateurs de façon sûre. Il peut assurer une fonction principale (la confidentialité), et deux fonctions annexes (l'intégrité et l'authentification) :

- **Confidentialité** : éviter l'espionnage des informations échangées pendant le transport,
- **Intégrité** : ne pas pouvoir modifier les informations échangées pendant le transport, et
- **Authentification** : s'assurer que la communication est établie entre 2 parties qui se connaissent ou se reconnaissent.

Le chiffrement du document permet lui de garantir :

- **Confidentialité** :
- **Intégrité** (dépend de la méthode de chiffrement utilisée) :

Le chiffrement des données et de leur transport ne doit cependant pas être confondu avec le périmètre et les fonctions assurées par la signature électronique elle-même qui tend à assurer :

- l'identification des signataires sur le contenu :
- l'adhésion des signataires au contenu signé :
- l'intégrité du message signé :
- la non-répudiation du contenu/message signé.

	Confidentialité des données	Intégrité des données	Authenticité des données
Chiffrement du canal	✔	?	✘
Chiffrement du message	✔	?	✘
Signature électronique	✘	✔	✔

[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 au CFE.

[Restituer]

Le terme **restituer** souligne l'obligation de tout CFE de remettre ou de donner l'accès 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 peut être dans un format spécifique, et c'est ce même format qui doit être restitué (voir l'annexe Pérennité sur la pérennité des formats).

[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, certificats, 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.

De par sa qualité intrinsèque d'opacité, le CFE pourrait contenir certaines informations qui, dans un système d'archivage, nécessiteraient un agrément ou une autorisation spécifique (par exemple des données médicales ou bancaires).

Le prestataire de service du CFE doit exiger de ses utilisateurs qu'ils respectent la législation à laquelle ils sont soumis.

[Déposé]

Le dépôt vise le stockage organisé de données qui ont fait l'objet d'un enregistrement électronique. Le dépôt électronique est confié au système de 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.

Ce terme permet au passage de qualifier juridiquement la nature du lien entre utilisateur et prestataire de service de CFE : au-delà du service informatique proprement dit, il s'agit d'un contrat de dépôt.

L'adjectif **déposé** qualifie l'action de déposer. Il véhicule, comme schématisé avec la *Figure 2*, les notions :

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

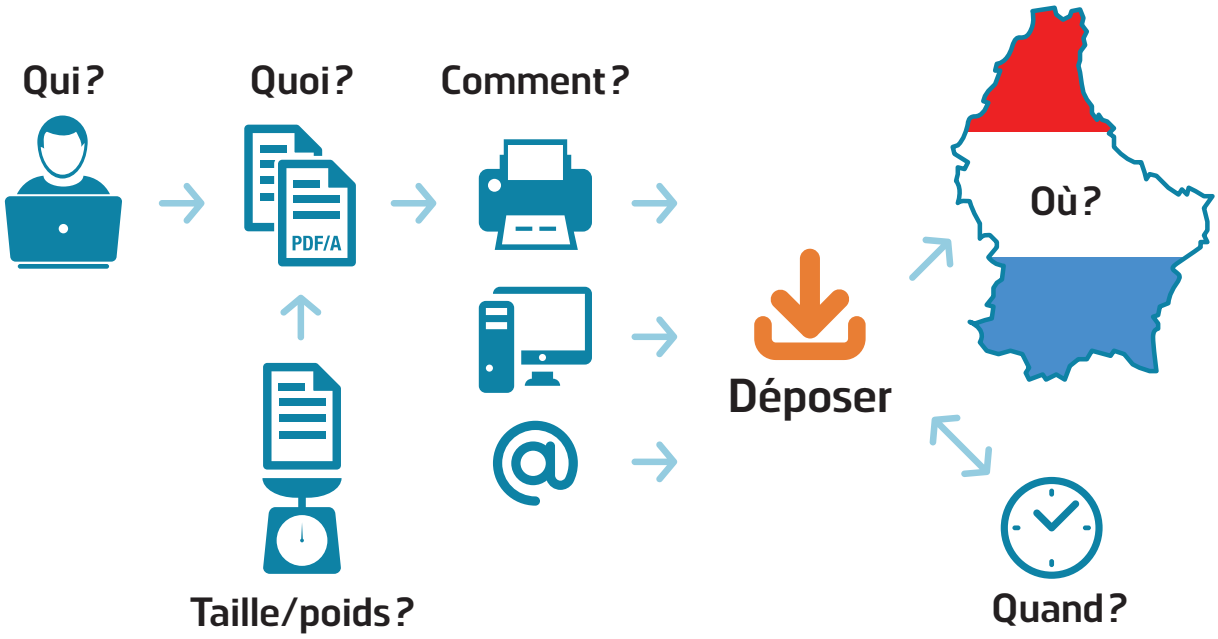

Figure 2. Action "déposer"

[Sans altération]

Dans le cadre d'une information ou d'un document numérique, restituer **sans altération** signifie qu'un CFE est en mesure de restituer dans son intégralité («bit pour bit») ce qui a été déposé.

Cela induit un maintien de l'intégrité entre le moment du dépôt (ou de la dernière modification faite au document dans le CFE, si les documents sont éditables) 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.

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, voire l'identification forte, est dès lors la première brique de cette solidité, 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 (qui est qui).
- l'autorisation ou contrôle d'accès (qui peut y avoir accès).
- la confidentialité (qui peut le lire).
- 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 3*.

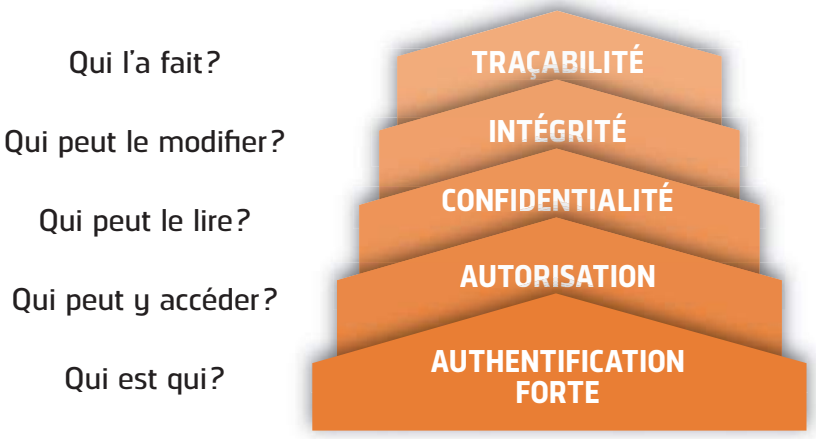

Figure 3. Pyramide des garanties nécessaires pour un CFE

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

La traçabilité peut être un élément optionnel, de façon à offrir une discrétion accrue demandée par certains utilisateurs.

État des lieux du CFE en France

On peut noter qu'en France, par une délibération du 19 septembre 2013[6] portant recommandation relative aux services dits de **coffre-fort numérique ou électronique** destinés aux particuliers, la CNIL[7] (l'équivalent français de la CNPD[8] au Luxembourg) définit le CFE comme **une forme spécifique d'espace de stockage numérique, dont l'accès est limité à son seul utilisateur et aux personnes physiques spécialement mandatées par ce dernier**. Elle précise par ailleurs qu'un service qui ne répondrait pas à ces critères serait **un simple espace ou service de stockage numérique** et surtout, qu'en **analysant les solutions de coffre-fort disponibles sur le marché, la CNIL a constaté que la majorité des services de coffre-fort numérique n'étaient pas suffisamment sécurisés**[9].

On note quelques différences par rapport à la définition donnée dans ce document :

- la notion d'**espace sécurisé** n'est pas mentionnée :
- un utilisateur ne peut être que physique, ne peut donc pas être un système :

Par ailleurs, lors de cette même délibération, la CNIL a émis une série de recommandations portant sur les services de CFE en France :

a. le numéro de sécurité sociale des personnes physiques ne doit pas être utilisé pour le routage d'un document dématérialisé vers un coffre-fort numérique, y compris lorsqu'il s'agit du routage d'un bulletin de paye (les utilisateurs peuvent néanmoins stocker leurs bulletins de paye dans leurs CFE).

b. les prestataires doivent obtenir un agrément ministériel spécifique pour stocker des données de santé :

c. la consultation des documents stockés ne peut se faire que par l'utilisateur concerné et les personnes spécialement mandatées par ce dernier, ce qui implique la mise en place de mesures techniques appropriés pour rendre les documents stockés incompréhensibles aux tiers non autorisés :

d. la suppression d'un document contenu dans l'espace personnel d'un utilisateur (ainsi que les éventuelles copies) doit être immédiatement prise en compte, et les copies du document supprimé dans lesquelles peuvent figurer ces données ne peuvent être conservées au-delà d'un mois :

e. le prestataire s'engage quant à la pérennité du stockage et la fermeture de ce type de service nécessite **d'en informer les utilisateurs suffisamment en avance afin de leur laisser le temps nécessaire pour récupérer les documents stockés**;

f. le prestataire doit **rendre accessible, sans surcoût, un outil permettant aux utilisateurs de récupérer l'intégralité du contenu de leur coffre-fort de façon simple, sans manipulation complexe ou répétitive, et ce afin de faciliter le changement de fournisseur** : et les transferts d'information vers et depuis un CFE.

g. mettre en œuvre des mesures de sécurité : chiffrement avec clef privée, conservation des clefs par un tiers pour la conservation à long terme, etc.

[6] *Délibération n° 2013-270 du 19 septembre 2013 portant recommandation relative aux services dits de «coffre-fort numérique ou électronique» destinés aux particuliers : JORF n°0235 du 9 octobre 2013, texte n°39: http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000028048730&dateTexte=&oldAction=dernierJO&categorieLien=id*

[7] *Commission nationale informatique et libertés*

[8] *Commission nationale pour la protection des données*

[9] *http://www.cnil.fr/linstitution/actualite/article/article/adoption-dune-recommandation-sur-les-coffre-forts-electroniques/*

Par ailleurs, par une délibération du 23 janvier 2014[10], la CNIL a défini un référentiel décrivant les modalités de création et de gestion ainsi que le contenu d'un CFE. La création d'un nouveau label relatif aux services de CFE a pour but d'assurer la conservation sécurisée et la protection des données à caractère personnel contenues dans un coffre-fort, qui ne seront accessibles qu'à leur utilisateur et aux personnes physiques spécialement mandatées par ce dernier.

Enfin, on peut noter que la loi française vient d'évoluer récemment puisque la nouvelle loi de programmation militaire[11] du 18 décembre 2013 prévoit, dans son article 20, la possibilité pour les services de renseignement d'accéder aux informations ou documents traités ou conservés par les réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications. On peut constater que l'usage de la notion d'informations et documents traités ou conservés par les réseaux ou services de communications électroniques peut permettre aux services de renseignement d'avoir non seulement accès aux données de connexion, mais aussi aux données de contenu.

Au regard des préoccupations croissantes exprimées par les internautes et le contexte particulier de l'affaire Prism aux Etats-Unis, certains auteurs parlent de Patriot Act à la française[12] du nom de la loi votée aux Etats-Unis au lendemain des attentats du 11 septembre 2001. On peut toutefois noter que le recueil de ces informations ou documents nécessite toutefois une autorisation auprès du Premier ministre ou des personnes qualifiées qu'il aura désignées, et ce pour une durée maximale de trente jours, qui peut être renouvelée dans les mêmes conditions de forme et de durée.

[10] *Délibération n° 2014-017 du 23 janvier 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de services de coffre-fort numérique*

[11] *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*

[12] *http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-News-31-January-2014/Pages/France%E2%80%93New-Patriot-Act-imposes-surveillance-obligations.aspx*

Fonctionnalités minimales, avancées et services additionnels associés

chapitre

3

Ce chapitre permet d'énumérer les fonctionnalités minimales obligatoires d'un CFE, les fonctionnalités avancées, et les différents services que l'on peut être amené à utiliser ou qui peuvent être proposés dans le cadre d'un CFE.

Fonctions minimales

Un CFE doit obligatoirement, pour être considéré comme tel, pouvoir recevoir des données et les stocker, permettre l'accès à ces données, les restituer, et les supprimer.

Il doit également permettre de sécuriser le contenu du CFE, et n'y donner accès qu'aux personnes autorisées. La cryptographie des données, permettant de protéger les données en les rendant inintelligibles pour qui n'est pas autorisé à les voir, notamment les propres administrateurs du prestataire de service, est un service de base d'un CFE (pour plus d'informations sur la cryptographie des données, voir l'annexe Signature électronique, chiffrement, cryptographie).

Scénario de création et d'utilisation

Un scénario possible de création d'un CFE et d'utilisation des avantages qui y sont associés peut être schématisé comme suit :

1. Création / ouverture du compte de CFE : avant tout, il faut créer un espace personnel sécurisé : l'accès à celui-ci doit être protégé (par une authentification forte).
2. Partage / Alimentation du CFE (voir exemple en *Figure 4*) : cette seconde étape implique l'utilisation du CFE. Cela peut consister en un stockage et la consultation des informations stockées (fonctions de base), en

la modification des informations placées (optionnel), en la réception de données provenant d'un tiers, mais également en un partage des coordonnées du CFE à différents acteurs de la vie quotidienne. En effet, un CFE pourrait fonctionner comme le courrier classique ou, par analogie avec le domaine électronique, comme une boîte e-mail, si tous les acteurs peuvent s'interfacer avec le CFE. Avec les coordonnées du CFE personnel, pour autant qu'ils en aient les droits, les différents acteurs pourront alors verser des documents dans cet espace sécurisé. Par exemple, l'employeur peut verser les contrats de travail ainsi que les fiches de salaire, les administrations communales peuvent y verser une copie de la carte d'identité, du livret de famille, etc.

3. Démarches (optionnel) (voir *Figure 4*) : grâce aux différents documents présents dans le CFE personnel, plusieurs démarches pourraient être effectuées, si les acteurs le permettent. Bien que les démarches soient différentes, le fonctionnement global reste le même.

    a. Se connecter au CFE : il suffit de se connecter au CFE personnel grâce à son authentification forte.
    b. Autoriser l'accès aux données (pièce par pièce, pour autant que possible) aux acteurs concernés.
    c. Échanger avec un tiers : finalement, ces documents seront soit envoyés à l'acteur, soit serviront au remplissage de formulaires, qui seront communiqués à ce tiers : par exemple le remplissage de la fiche d'impôt basé sur les fiches de salaire présentes dans le CFE, l'envoi de diplômes à un nouvel employeur, etc.

4. Suppression d'informations ou du compte : si le CFE peut être créé et peut stocker des informations, il doit aussi être en mesure de donner la possibilité au propriétaire de supprimer les informations dont il ne veut plus. Un accusé de suppression de données pour prouver que toute information relative à l'information supprimée a été dûment effacée peut être établi par le système de CFE. Le système de CFE doit également laisser l'opportunité de fermer son CFE à n'importe quel moment, ce qui entraînera la suppression irréversible de l'accès à toutes les informations de ce CFE.

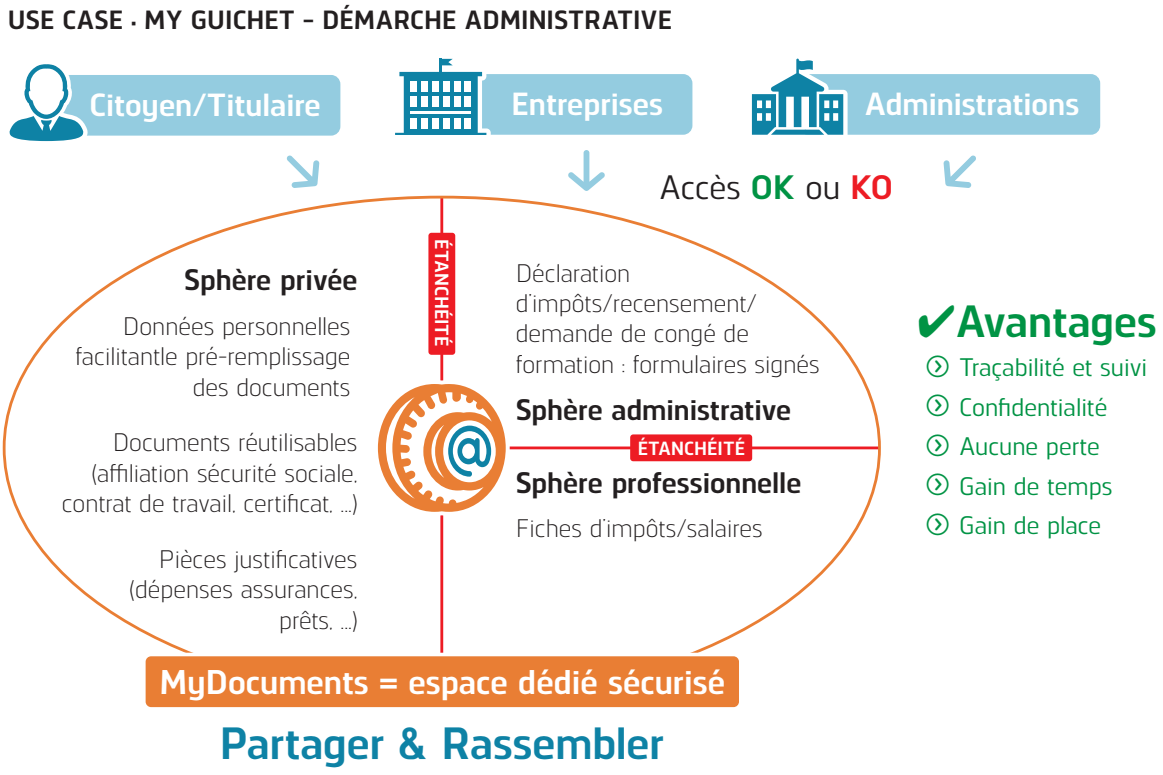

***Figure 4**. Aperçu des liens pouvant être faits avec les entreprises, les administrations...*

Services additionnels et fonctionnalités avancées

Parmi ces services additionnels, les plus fréquemment rencontrés sont :

- la dématérialisation des données :
- la signature électronique, permettant de garantir l'intégrité des informations et d'authentifier l'auteur de cette signature (voir l'annexe Signature électronique, chiffrement, cryptographie pour une définition de la signature électronique, son fonctionnement général et son utilisation).
- l'horodatage, permettant d'enregistrer l'instant auquel une opération (versement par exemple) a été effectuée (voir ci-après).
- la restitution des données après une rupture de contrat (voir ci-après) :
- le changement de prestataire de service et la réversibilité des données y associée (voir ci-après) :
- le stockage dans des pays bien définis :
- la production d'un accusé de réception avec l'empreinte de l'objet d'archive :
- le partage des données avec des personnes de confiance (voir ci-avant).

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 qui y sont 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 devrait pas pouvoir 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 du prestataire 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 (au moins deux) chez des tiers de confiance désignés par le propriétaire du CFE (solution la plus verrouillée).

Rupture de contrat

Lors d'une rupture de contrat ou conditions générales d'utilisation (lors du décès avéré du propriétaire ou de non-paiement, par exemple), 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 d'un contenu crypté devrait pouvoir se faire sans limite de temps. Le prestataire devrait alors garder les données du CFE pendant la période prévue au contrat.

Le CFE pourra, si cela est prévu dans le contrat, être ouvert par des tiers autorisés.

Réversibilité des données

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 système ou prestataire de CFE, grâce à un export normalisé et structuré, et grâce à un import de ces données dans le nouveau CFE. De même, la gestion des clefs devrait pouvoir être transmise de la façon la plus normalisée possible pour permettre d'éviter à quelqu'un souhaitant changer de prestataire de déchiffrer ses données pour les chiffrer à nouveau dans le nouveau CFE.

Héritage

En cas de décès du propriétaire du CFE, les données sont en théorie perdues, car la clef d'accès ne devrait être connue que du propriétaire de ce CFE. Néanmoins, une procédure spéciale peut être mise en œuvre, si proposée par le système de CFE. En effet, si les dispositions ont été prises, plusieurs personnes (usuellement deux) de confiance peuvent avoir en leur possession une partie de la clef secrète, parties qui peuvent être réunies en cas de décès du propriétaire du CFE pour ouvrir le coffre. Il faut pour cela généralement apporter une preuve du décès pour permettre ceci. Un autre cas de figure possible est que la clef se trouve chez un notaire, qui la transmettra lors de la succession.

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. L'horodatage est un cachet effectué à l'aide d'un certificat dédié pour ce service : il permet donc également de prouver que le contenu des données n'a pas été modifié depuis le moment où les données se sont vues apposer ce tampon numérique.

Plusieurs méthodes peuvent être utilisées, la plus sûre étant d'avoir recours à un tiers-horodateur de confiance respectant des standards reconnus (comme RFC 3161[13] (Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), protocole développé par l'IETF (Internet Engineering Task Force) qui permet entres autres de s'abstraire du contenu, car le protocole est indépendant des données, le tiers-horodateur ne recevant que l'empreinte des données à horodater). 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.

[13] *"Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)". http://www.ietf.org/rfc/rfc3161.txt*

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'usager 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 (grâce par exemple à des dossiers).
- la gestion des droits d'accès au CFE (voir *Figure 4*) (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 possibilité d'accès multi-plateforme/multi-device.
- 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 de toute activité 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) (voir problématique de la pérennité en annexe Pérennité).
- 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, permettant de ne pas donner son identité lors de la création du coffre.

Pourquoi utiliser un CFE, et qu'y placer ?

chapitre

4

Le CFE permet de sécuriser de l'information. Néanmoins, certaines informations sont plus à même de se trouver dans un CFE que d'autres.

Pour un particulier

Voici une liste non exhaustive d'informations et documents qu'il peut être intéressant de déposer dans un CFE pour un particulier :

- Mots de passe, pin codes et autres identifiants :
- Copies de documents d'identité (passeport, carte d'identité, permis de conduire, etc.) :
- Documents liés à la famille (actes, contrats de mariage, pactes, testament...) :
- Assurances :
- Factures :
- Documents liés
  - à l'épargne – Assurance vie :
  - à la Santé :
  - à l'activité salariale :
  - à la Retraite :
  - au Logement :
- Locataire :
- Propriétaire.
  - aux Crédits :
  - aux Voitures – Motos :
  - à la Banque (relevés bancaires, etc.) :
  - aux Impôts et taxes (déclaration, justificatifs, avis d'imposition....) :
- Documents personnels :
- Diplômes et certificats :
- Notices techniques (ex : alarme) :
- Photos.

Pour une entreprise

Voici une liste non exhaustive d'informations et documents qu'il peut être intéressant de déposer dans un CFE spécifiquement pour une organisation (en plus des informations pouvant être déposées par un particulier) (voir par exemple *Figure 5*) :

- Documents administratifs et comptables (bons de commande, de livraison, commandes clients, accords de confidentialité, contrats commerciaux, documents fiscaux et d'assurance, factures clients, etc.) :
- Rapports de Conseil d'Administration :
- Propriété intellectuelle, études et documents relatifs aux dépôts de marque et/ou brevets :
- Informations secrètes :
- Partage d'informations confidentielles :
- Relevés de comptes, images-chèques, ordres de bourse :
- Factures dématérialisées au sens du droit fiscal[14] :
- Documents divers liés aux salariés (RH, etc.) :
- Les fiches de salaire : Une fiche de salaire électronique est parfaitement similaire à sa version papier, excepté le fait qu'elle n'est pas systématiquement imprimée. Les points sensibles d'une fiche de salaire électronique sont :
  - Confidentialité (donc gestion fine des droits d'accès) :
  - Inaltérabilité (par exemple grâce au format PDF) :
  - Accessibilité :
  - Traçabilité.

  Le CFE respectant ces quatre points, une fiche de salaire peut donc s'y retrouver.

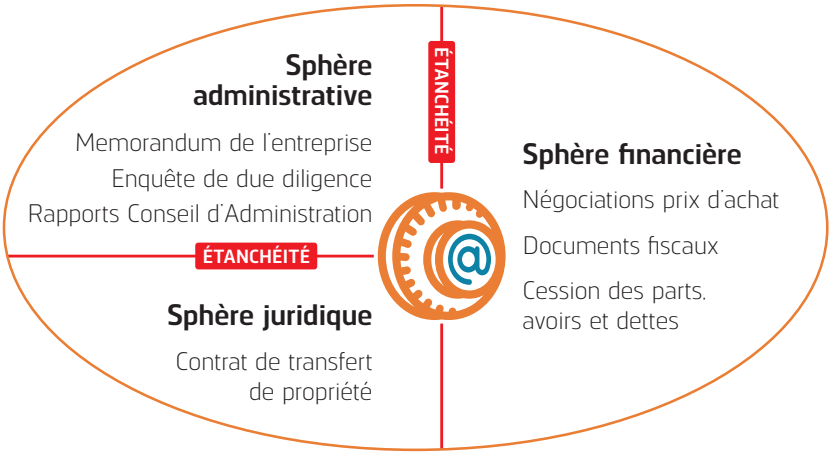

Figure 5. Exemple de CFE d'une entreprise

[14] *Directive 2001/115/CE du Conseil du 20 décembre 2001 modifiant la directive 77/388/CEE en vue de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée et Directive 2010/45/CE du Conseil du 31 juillet 2010*

Catégorisation des contenus et positionnement du CFE

chapitre

5

Catégorisation de contenus

Après avoir abordé les outils, applications et services pouvant graviter autour du CFE, ce chapitre traite de l'information ayant de la valeur pour son possesseur. Différents types d'informations existent.

La *Figure 6* détermine des catégories de types de données, en illustrant schématiquement les trois niveaux que nous pouvons distinguer en général, et qui sont décrits ci-après.

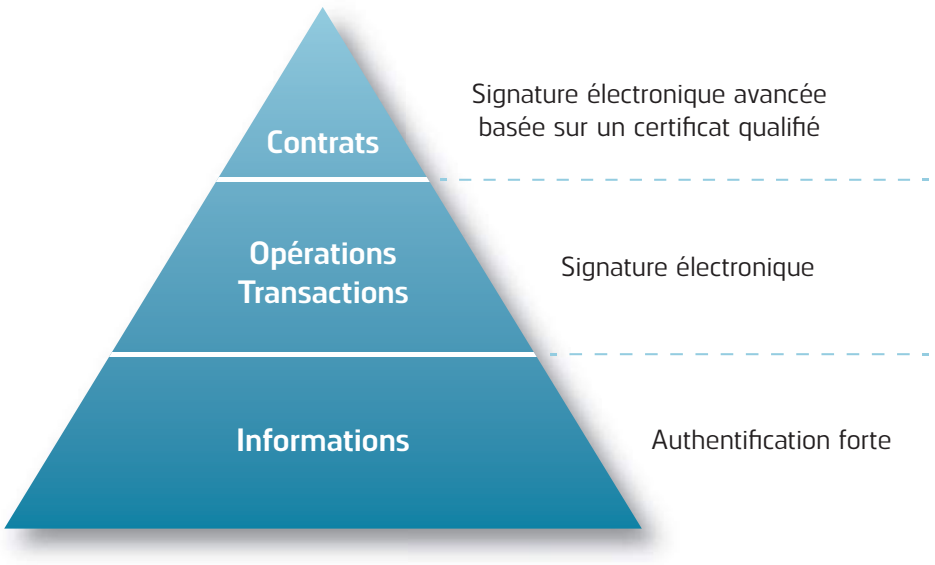

Figure 6. Pyramide des types d'information et leur méthode d'authentification associée

Première couche : informations

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 peut parler ici, pour se rapprocher de l'acceptabilité auprès d'un juge de ces informations, 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 pourra être considérée comme sécurisée 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.

Signature électronique

Certaines informations peuvent nécessiter une signature électronique plus ou moins poussée. La *Figure 6* reprend les couches informatives qu'il peut être nécessaire, pour leur garantir un certain niveau de fiabilité, de signer électroniquement.

Une signature électronique avancée offre divers avantages techniques et légaux qui permettront à un tiers de pouvoir se fier au contenu des données reçues (voir pour plus d'informations l'annexe Signature électronique, chiffrement, cryptographie pour la définition de la signature électronique, son fonctionnement et son utilisation).

La signature électronique avancée :

- garantit l'intégrité et l'authenticité des données.
- assure la non-répudiation de la signature.
- en cas d'utilisation d'un certificat qualifié et d'un SSCD, la signature sera du type qualifiée, elle délivre alors une valeur légale reconnue automatiquement comme égale à celle d'une signature manuscrite.

Deuxième couche : transactions

La couche intermédiaire peut être utilisée pour une majorité de transactions. L'ensemble des informations repris dans cette zone pourrait ou devrait 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, l'authenticité et l'intégrité de l'information. À titre d'exemple, on pourra classer dans cette catégorie des instructions de transfert bancaire.

Troisième couche : pièces pouvant servir en cas de litige

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 ou pièces pouvant faire l'objet d'un litige. Afin d'obtenir une valeur légale égale à celle de la signature manuscrite, les pièces ici reprises devraient être dotées d'une signature électronique avancée basée sur un certificat qualifié. Cela conférera à ces données le plus haut niveau de confiance juridique qu'il est possible d'accorder à des données numériques.

Pour signer, l'utilisateur devra utiliser un certificat qualifié et un SSCD (autrement dit actuellement un couple lecteur de carte et Smartcard accrédité selon des standards définis).

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).

Positionnement du CFE

Nous avons classifié les différents types d'informations globalement rencontrés dans la partie précédente, il nous faut maintenant positionner le CFE pour comprendre à quels types d'informations il peut correspondre et être une solution. Afin de positionner le CFE par rapport à d'autres solutions, il est essentiel de déterminer les éléments qui composent la solution. Par quels éléments une entreprise luxembourgeoise peut-elle commencer sa démarche de dématérialisation et de stockage de l'information sans prendre de risques inconsidérés ?

Sur base de la pyramide des types d'information et des signatures associées vue dans la partie précédente, la mise en place d'un CFE permet à une entreprise de ne prendre en théorie que peu 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'Archivage Électronique (SAE) ou d'un système compatible PSDC (voir introduction du Différences entre CFE et autres systèmes). Une proposition d'approche des différentes options de stockage de l'information de manière sécurisée est proposée en *Figure 8* reprend un exemple de ce que peut échanger une entreprise dans le cadre de ses activités, ici notamment dans le cadre d'une fusion d'entreprises.

Des transactions et des informations pourraient donc cohabiter dans le CFE. Néanmoins, 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. 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 espace de stockage sécurisé. Cet espace est donc un endroit où sont placées les données. Ces 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. Grâce à l'intégration dans ces flux de la signature électronique avancée basée sur un certificat qualifié, une dématérialisation complète du flux de bout en bout 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.

La *Figure 7* illustre la problématique des niveaux de complexité, de responsabilité, etc. qu'une société (un prestataire de CFE ou un «tiers-archiveur») est prête à assumer par rapport à son cœur de métier :

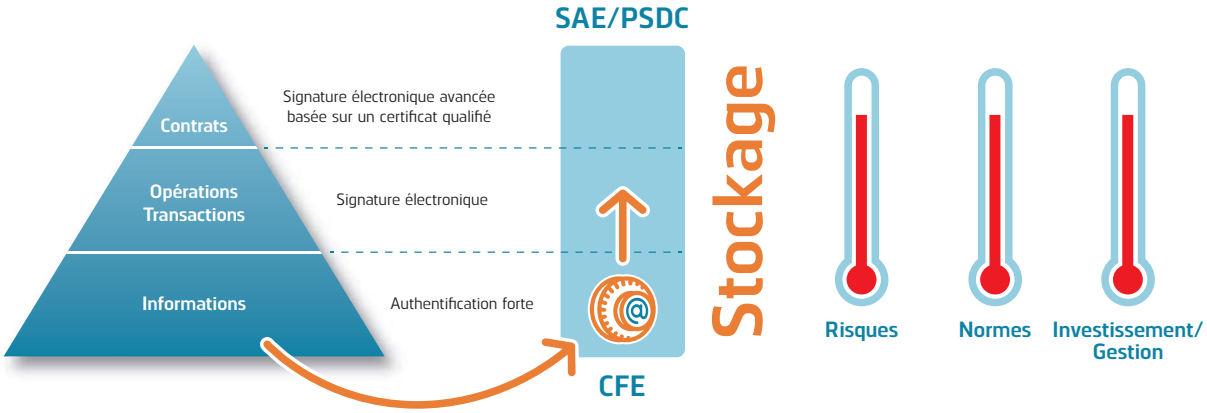

Figure 7. Niveaux de complexité d'un CFE

La *Figure 8* reprend un exemple de ce que peut échanger une entreprise dans le cadre de ses activités, ici notamment dans le cadre d'une fusion d'entreprises.

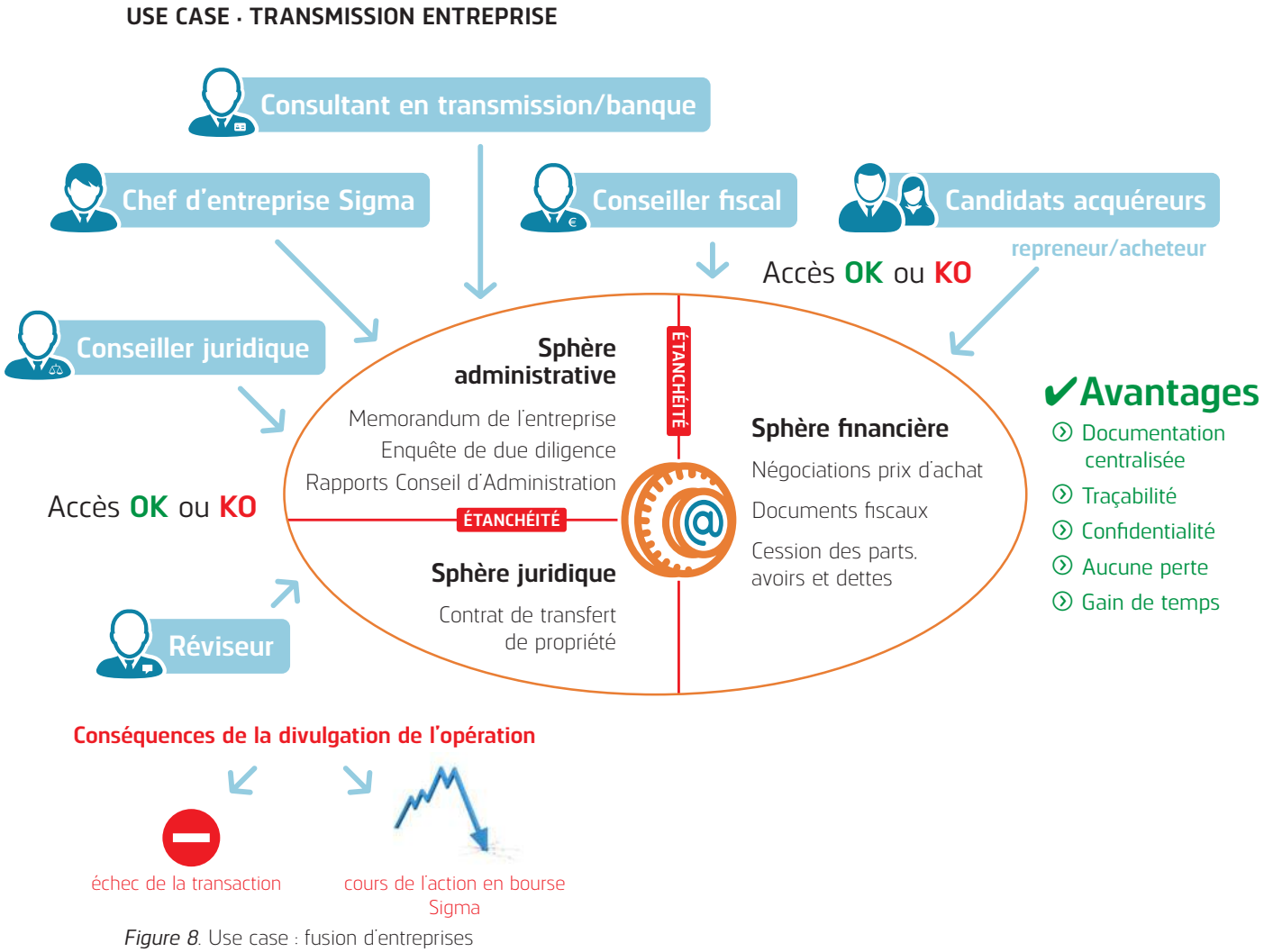

Figure 8. Use case : fusion d'entreprises

Différences entre CFE et autres systèmes

chapitre

6

Les informations numériques prennent de plus en plus de place dans la vie des entreprises et des particuliers. Au Luxembourg, cet état de fait a amené une prise de conscience au niveau législatif. En effet, l'ILNAS[15] a publié une règle technique des exigences minimales pour obtenir une certification de PSDC[16]. Cette règle technique permet notamment à un prestataire de fournir un service de conservation qui respecte des principes de confidentialité, d'intégrité et de disponibilité, ainsi que d'authenticité, de fiabilité et d'exploitabilité. L'approche de la conservation dans la règle technique PSDC s'appuie sur un système d'archivage électronique.

Afin de bien différencier le CFE du PSDC et des systèmes avec lesquels il est parfois confondu, le tableau suivant reprend les exigences de différentes appellations (Système d'Archivage électronique, Backup, stockage en ligne). Les exigences dans le tableau sont définies et détaillées dans l'annexe reprenant un glossaire.
La méthode dite MoSCoW a été utilisée, les lettres MSCW 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).

[15] *Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services*
[16] *Prestataire de Service de Dématérialisation ou de Conservation*

Fonctionnalités	CFE	Système d'Archivage Électronique	Backup	Stockage en ligne, répertoire virtuel
Rétention				
Période de rétention sur chaque groupe d'objets	✗	✓	✗	✗
Période de maintien opérationnel du contenant	✓	✗	✓	!
Protection du contenu				
Chiffrement du contenu	✓	?	?	?
Contrôle d'accès				
Accès au déposant	✓	?	?	?
Accès à des tiers	?	?	?	?
Fonctions				
Plan de classement	?	✓	✗	✗
Horodatage certifié	?	✓	✗	✗
Conversion des formats (en entrée)	?	!	✗	✗
Conversion des formats (au sein de la solution)	✗	✓	✗	?
Disponibilité (SLA)	!	?	?	?

Fonctionnalités	CFE	Système d'Archivage Électronique	Backup	Stockage en ligne, répertoire virtuel
Authenticité				
Signature électronique	!	!	?	?
Intégrité				
Intégrité (bit par bit)	✔	✔	!	!
Intégrité avec évolution des données	✘	✔	✘	?
Lisibilité dans le temps	✘	✔	?	✘
Confidentialité				
Confidentialité (contenu secret) vis-à-vis de tiers	✔	?	?	?
Confidentialité vis-à-vis d'administrateurs du système	✔	!	?	!
Protection				
Protection logique des données	✔	✔	✔	!
Protection physique *(installations, équipements, commodités)*	✔	✔	✔	✔

Contexte législatif luxembourgeois

chapitre

7

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 **Contexte législatif sur les coffres-forts non-électroniques** donne pour sa part le contexte législatif propre aux coffres-forts physiques.

La notion de coffre-fort électronique est parfois rattachée à la notion juridique de **force probante** : l'utilisation d'un coffre-fort pourrait en effet permettre d'attester, en cas de conflit ou tout simplement en cas de demande de justification, de la valeur probante d'une information. Rappelons qu'un coffre, contrairement à une gestion électronique documentaire, ne traite pas que des documents.

Contexte législatif sur les données dématérialisées, plus particulièrement sur les documents

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 que

> " 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 et 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.

En France

On peut noter que la jurisprudence française reprend les mêmes critères qu'énoncés ci-dessus : ainsi, dans un arrêt rendu par la deuxième chambre civile de la Cour de Cassation en France le 4 décembre 2008 (pourvoi n°07-17622), la Cour de Cassation rappelle que **l'écrit électronique ne vaut preuve qu'à condition que son auteur puisse être dûment identifié et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité**, et doit être horodaté.

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.

Ainsi, un document électronique a, d'un point de vue juridique, la même valeur qu'un original à condition de pouvoir démontrer, dès l'origine et jusqu'à la fin de sa période de conservation, l'authenticité, l'intelligibilité et l'intégrité du document. Même si chaque État membre de l'Union Européenne est libre de définir les modalités pratiques concernant l'archivage électronique, chaque État membre doit respecter ces principes.

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, ce qui implique par exemple qu'il n'est pas nécessaire pour un prestataire d'avoir une clé permettant d'ouvrir les CFE, ni de posséder une copie des clés des utilisateurs, ni de soumettre les clés à une autorité nationale ou à un tiers de confiance. Ceci est un élément différentiateur fort par rapport à d'autres pays européens.

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.

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. Par conséquent, le prestataire ne doit pas pouvoir accéder aux données conservées, ni à ses éventuelles sauvegardes, sans le consentement exprès de l'utilisateur concerné.

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 (par exemple, un agrément spécifique en ce qui concerne le stockage de données de santé).

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

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.

Conclusion

chapitre

8

Cette nouvelle mouture du 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 ou les systèmes estampillés PSDC. Dans une époque où la moindre information peut vraisemblablement être épiée, le CFE traduit sous une législation luxembourgeoise s'avère donc être un système efficace pour le dépôt d'informations et de documents qui doivent rester à l'abri de regards indiscrets. 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.

Les bénéfices que peut apporter un CFE sont nombreux, mais aussi dépendants des services associés :

- Espace de totale intimité, de confidentialité, de protection d'informations personnelles
- Conservation sécurisée d'informations.
- Partage d'information avec des tiers disposant des clefs d'accès sans devoir sortir les données de leur écrin de sécurité.
- Dépôt d'informations dans le coffre d'un tiers.
- Intégration semi-automatique de données certifiées venant de différentes origines.
- Économie de manutention des documents de format divers
- Gain de temps dans la réalisation des formalités.
- Point de centralisation pour une personne physique ou morale.

L'AFNOR (Association Française de Normalisation) a publié en juillet 2012 la norme NF Z42-020 portant le nom de **Spécifications fonctionnelles d'un composant Coffre-Fort Numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps**. Bien que le terme **Coffre-fort numérique** (ou CFN) soit très proche de **Coffre-fort électronique** (ou CFE), les deux sont bien distincts et ont des buts radicalement opposés. Quand le CFE défini dans ce document est un espace virtuel de stockage et de conservation sécurisé, le CFN est une interface entre les données et la technologie de stockage permettant de s'abstraire de la connaissance du support : grâce à lui, l'interface avec les données est simplifiée et unifiée, que le support de stockage soit un disque dur, une mémoire flash, une bande, etc., comme décrit dans la *Figure 9*. Un CFN pourrait donc être utilisé pour l'interface avec les données gérées par un CFE, ou par un Système d'Archivage Électronique, ou par tout autre système de gestion de stockage!

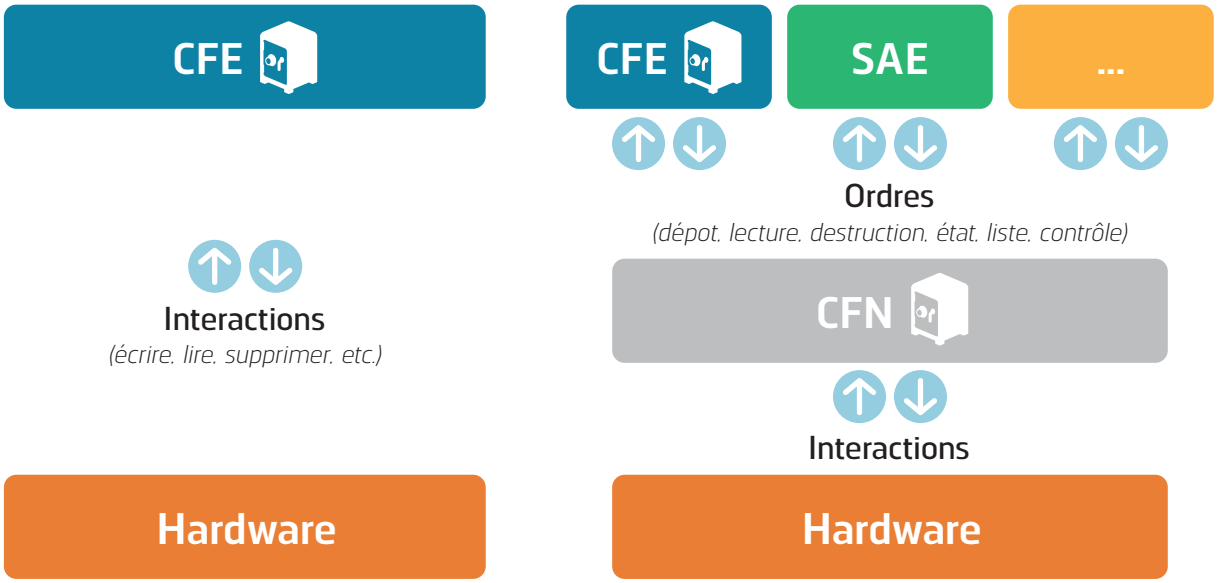

Figure 9. CFE et CFN : à gauche les interactions d'un CFE avec le hardware sans CFN.
à droite avec : l'interface peut se faire pour un CFE, un SAE et d'autres systèmes de stockage.

La thématique du CFE et les besoins de confidentialité n'ont donc jamais été aussi présents autour de nous, et continuent à se développer, avec un marché ouvert et une demande réelle.

Équipe rédactionnelle
(par ordre alphabétique)

annexe

A

Remerciements au Groupe de Travail **Coffre-fort électronique** de FedISA Luxembourg :
ci-dessous les personnes ayant activement contribué à la rédaction de cette version du livre blanc et présents aux groupes de travail :

Aurélie Bayard (LuxTrust S.A.)

Ingénieur civil électronicien (Université de Liège) de formation et titulaire d'un diplôme de 3ème cycle en Marketing stratégique & opérationnel (HEC Liège). Aurélie Bayard travaille en tant que Key Account Manager & Marketing leader chez LuxTrust. LuxTrust est une Autorité de certification qui délivre des certificats électroniques et fournit des services d'authentification forte et de signature électronique, pouvant être utilisés dans le cadre de l'utilisation d'un Coffre-fort électronique.

Lucas Colet

Titulaire d'un Master Recherche en Informatique, Lucas est spécialisé dans la normalisation 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, ainsi que le groupe de travail portant sur la dématérialisation. Il met son expérience et cette expertise au service des acteurs du marché, privés et publics.

Paul Lanois

Avocat inscrit aux barreaux de New York, de Paris et du Luxembourg (Liste IV). Paul a débuté sa carrière en tant qu'avocat au sein du cabinet américain Simpson Thacher & Barlett LLP à Londres. Il a également enseigné le droit des affaires à l'Université de Cergy-Pontoise en France. Il exerce actuellement la profession d'avocat dans un cabinet international basé au Luxembourg. Il a obtenu à l'Université Paris I - Panthéon-Sorbonne un Master en Droit anglais et nord-américain des Affaires ainsi que le diplôme du Magistère de Droit des Activités Economiques. Il est également titulaire d'un LLM de l'University of Pennsylvania Law School (Etats-Unis) ainsi que d'un diplôme de commerce de la Wharton School of Business (Etats-Unis).

Xavier Lisoir

Diplômé de HEC Liège et titulaire d'une maitrise en informatique de gestion. Xavier Lisoir est expert en stratégie, en système d'information et en optimisation de processus. 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, règlementaires, fiscales ou métier.

Marie-Emilie Mengal (Post Luxembourg)

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 Universitaire Notre-Dame de la Paix de Namur et d'un Certificat Universitaire en Management de la Sécurité des Systèmes d'Information (INFOSAFE). 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. À ce titre, elle est notamment en charge du Pôle contentieux et de la Sécurité de l'Information. Marie-Emilie s'intéresse également à la gestion de l'information numérique et suit actuellement un Certificat Universitaire en Gestion de l'Information Numérique (DOCSAFE).

Pierre Van Wambeke (SeeZam S.A.)

Ingénieur de formation et diplômé d'un MBA, Pierre Van Wambeke est un entrepreneur du Net. Fondateur et CEO 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 a dirigé l'informatique d'un grand hôpital privé 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 pour faire décoller SeeZam. C'est en 2013 que SeeZam a rejoint le groupe Systemat BeLux, assurant un développement des solutions à l'international.

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.

Gilles Wagener (BIL)

En tant que Head of Document Management de la BIL, Gilles Wagener assume la responsabilité des flux de numérisation, d'archivage et de restitution des documents. Sa mission consiste également à élaborer des processus de dématérialisation pour les services métiers répondant aux critères d'un archivage à valeur probatoire tout en appliquant les méthodes de gestion régulière dans le cadre d'un plan d'archivage actualisé.

Nos remerciements vont également à l'équipe rédactionnelle du premier livre blanc (et leurs affectations à date de publication de ce premier livre blanc) :

- **Lucas Colet** (Centre de Recherche Public Henri Tudor) – Secrétaire
- **Alain Devroede** (Euroscript)
- **Cédric Jadoul** (Fujitsu Technology Solutions Luxembourg)
- **Xavier Lisoir**
- **Marie-Emilie Mengal** (Entreprise des Postes et Télécommunications)
- **Frank Poireau**
- **Christophe Porte** (BGL-BNP Parisbas)
- **Frank Rockenbrod**
- **Pierre Van Wambeke** (SeeZam S.A.)
- **Renaud Vanderoost** (Sogeti)
- **Gilles Vansteenkiste** (CETREL)

Pérennité

annexe

B

La plupart des fichiers créés avant les années 90 risquent d'être maintenant illisibles sans mettre en place de coûteuses mesures. Ce sera bientôt le cas pour d'autres formats plus récents. 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.

Glossaire du chapitre « Différences entre CFE et autres systèmes »

annexe

C

Rétention	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 rétention sur chaque groupe d'objet Période de rétention définie sur l'objet (document, données) ou groupe d'objets à l'intérieur du système
Protection du contenu	Chiffrement du contenu Le contenu est-il protégé par des méthodes de chiffrement ?
Contrôle d'accès	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 3 : **Horodatage**) ?
	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 (SLA) Est-ce que l'accès aux données doit être garanti avec une forte qualité de service (disponibilité à 99.9% par exemple) ?

Authenticité	Signature électronique Le contenu est-il authentifié grâce à une signature électronique?
Intégrité	Intégrité (bit par bit) Est-ce que le système possède une procédure permettant de garantir l'intégrité totale (on parle d'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)?
Confidentialité	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.)?

Contexte législatif sur les coffres-forts non-électroniques

annexe

D

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[17].

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 (...)[18].

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[19].

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.

[17] *FREDERICQ. Traité de droit commercial belge. Gand. T.X.. 1952. n° 214*

[18] *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*

[19] *BUYLE et DAUBIES. Le contrat de location de coffre-fort. in le droit commun du bail. éditions la Charte. 2006*

En France, la Cour de Cassation qualifie le contrat de coffre-fort de contrat de garde[20]. 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[21]. 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 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[22].

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[23], 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.

[20] *Cass (fr.) (1re ch. Civ.), 2 juin 1993, Bull. civ., n°197, p. 136*

[21] *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».*

[22] *Bruxelles, 11 mai 2000, R.D.C., 2001, p. 833, note J.P.BUYLE et M. DELIERNEUX*

[23] *En Belgique, le tribunal de Commerce de Louvain a, dans une décision du 16 mai 1995 , 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.»*

Signature électronique, chiffrement, cryptographie

annexe

E

Cryptographie

La confiance que peuvent avoir les utilisateurs de coffre-fort électronique dépend largement des conditions techniques entourant le stockage ainsi que le transfert électronique des données stockées. Elle repose sur l'utilisation de procédés de cryptographie par les prestataires de coffre-fort électronique.

La cryptographie est un domaine assez ancien. En effet, cette technique vient du besoin de garder des informations confidentielles ou du moins cachées aux yeux des personnes non concernées. Le chiffre dit de César est l'exemple antique le plus connu de cryptographie : Jules César utilisait pour rendre incompréhensible ses messages un mécanisme simple : toutes les lettres de son message étaient décalées dans l'alphabet d'un nombre déterminé (dans l'exemple de la *Figure 10*, les lettres sont décalées de 3 positions dans l'alphabet, ce qui fait que dans le message chiffré, A sera remplacé par D, B par E, ... X par A, Y par B et Z par C) : le message n'est plus compréhensible sans connaître cette astuce. Un autre exemple d'application de la cryptographie est la machine Enigma, utilisée pendant la Deuxième Guerre Mondiale.

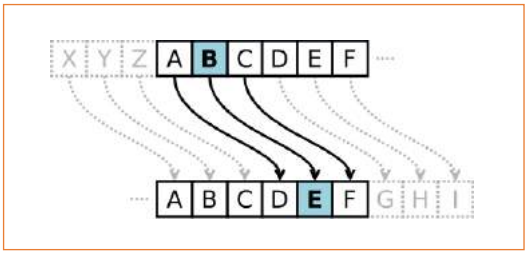

Figure 10. Chiffre de César (avec décalage de 3 lettres)

En 1883, Auguste Kerckhoffs[24] a rappelé les principes de base de la cryptographie :

1. Le système doit être matériellement, sinon mathématiquement indéchiffrable ;
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
3. La clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;
4. Il faut qu'il soit applicable à la correspondance télégraphique ;
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

[24] *Voy. A. Kerckhoffs, « La cryptographie militaire », Journal des sciences militaires, vol IX, 1883, pp. 5-38*

Aujourd'hui, la cryptographie est utilisée tant pour rendre certaines informations secrètes illisibles que pour générer des signatures électroniques.

Au Luxembourg, l'usage de la cryptographie est libre.

Deux concepts s'affrontent : le chiffrement symétrique, et le chiffrement asymétrique.

Le chiffrement symétrique

Le chiffrement symétrique permet d'encrypter et de décrypter avec une clé secrète unique (pouvant être un mot de passe par exemple) (voir exemple *Figure 11*).

L'avantage de ce type de chiffrement réside dans sa rapidité et dans son coût réputé moins élevé.

Par contre, puisque seule la clé utilisée pour chiffrer le document peut être utilisée pour le déchiffrer, il faut que l'émetteur transmette la clé à la personne autorisée à déchiffrer la donnée chiffrée et assure la sécurité de la transmission de la clé utilisée.

Par ailleurs, les procédés de chiffrement symétrique sont réputés moins fiables en raison des progrès de la cryptanalyse et de la puissance de calcul des ordinateurs rendant les attaques plus faciles : attaques par mot de passe, etc.

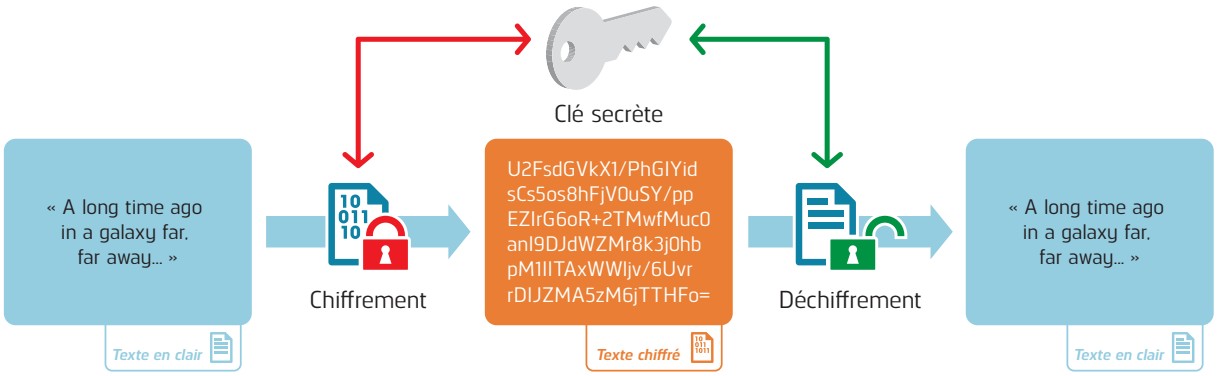

Figure 11. Chiffrement symétrique

Le chiffrement asymétrique

Figure 12. Une clé publique et une clé privée, base du chiffrement asymétrique.

Le principe mathématique du chiffrement asymétrique se base sur une paire de clés (voir *Figure 12*) : tout ce qui est encrypté par une clé peut être décrypté par la clé correspondante. La clé privée doit être gardée secrète alors que la clé publique peut être distribuée

Le chiffrement asymétrique permet de distribuer sa clé publique. Alice transmet sa clé publique à une personne qui pourra donc lui envoyer un message encrypté à l'aide de la clé publique d'Alice. Ceci garantit que seule Alice peut déchiffrer le message (voir exemple *Figure 13*). Ce chiffrement est réputé plus coûteux et plus lourdent à cause de sa nature mathématique et de la longueur des clefs.

Il implique généralement le recours à la fonctionnalité de hachage (voir plus bas) permettant de réduire la taille des informations à chiffrer.

Il est cependant beaucoup plus fiable.

En effet, générer les clés est très coûteux en ressources pour un ordinateur, de même qu'appliquer cette clef à un long document (c'est pourquoi il est utilisé principalement pour chiffrer des données courtes (hash, etc.)). Néanmoins, grâce à sa longueur de clef, cette technique est plus sûre que le chiffrement symétrique, pour peu que l'algorithme utilisé soit fiable.

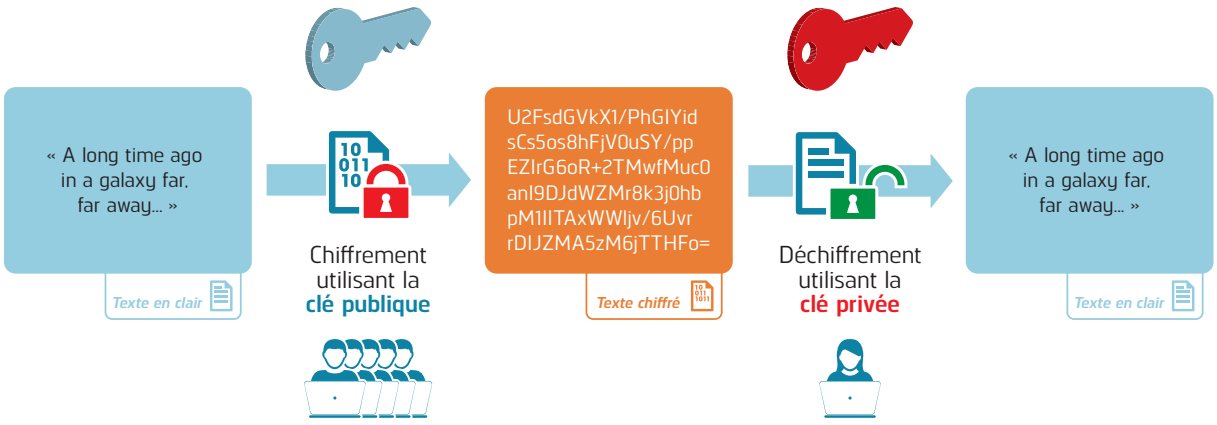

Figure 13. Chiffrement asymétrique

La signature électronique

Les signatures électroniques sont basées sur le chiffrement de l'empreinte d'un document. Cette empreinte est une chaîne de bits obtenue de manière automatique. Cette méthode mathématique donnera toujours la même empreinte avec le même texte en entrée (voir exemple *Figure 14*). Par contre, il suffit de changer un seul caractère dans tout le document et l'empreinte sera différente.

L'encryption asymétrique, comme vu plus haut, est un processus lent. Il est donc souhaitable de ne pas signer (encrypter avec sa propre clé privée) le contenu d'un document mais bien l'empreinte de celui-ci qui est toujours d'une longueur limitée.

Figure 14. Exemple d'empreintes : une modification du texte de départ entraîne un changement probant sur l'empreinte.

Création d'une signature électronique

La signature électronique d'un document est obtenue en encryptant l'empreinte d'un document à l'aide de la clé privée, comme indiqué en *Figure 15*.

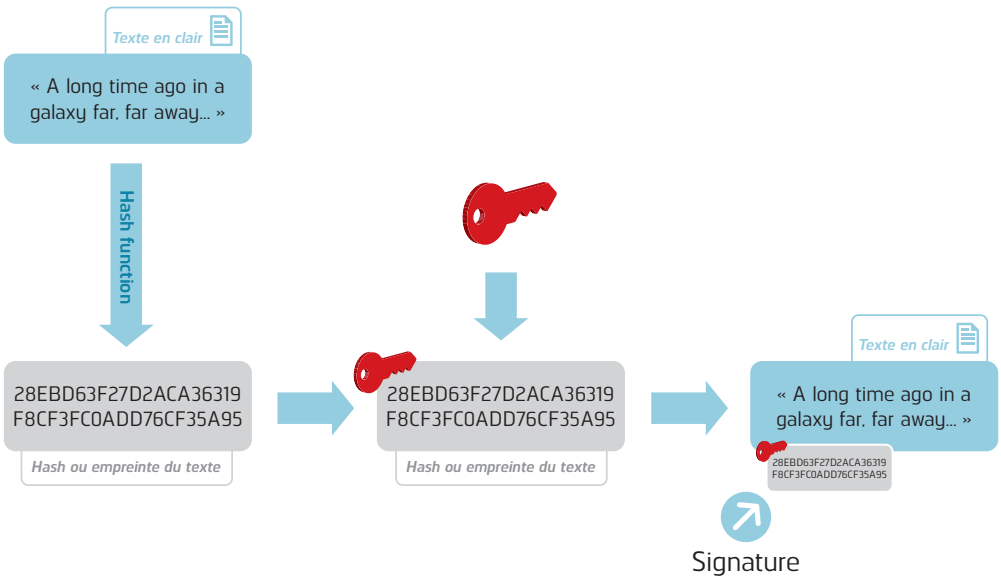

Figure 15. Création d'une signature électronique

Validation d'une signature électronique

La validation d'une signature électronique se déroule comme suit (voir *Figure 16*) :

1. L'empreinte du document original, extrait des données signées, est calculée.
2. La signature est décryptée à l'aide de la clé publique pour obtenir l'empreinte du document
3. Les 2 empreintes sont comparées. Le fait qu'elles soient identiques valide la signature

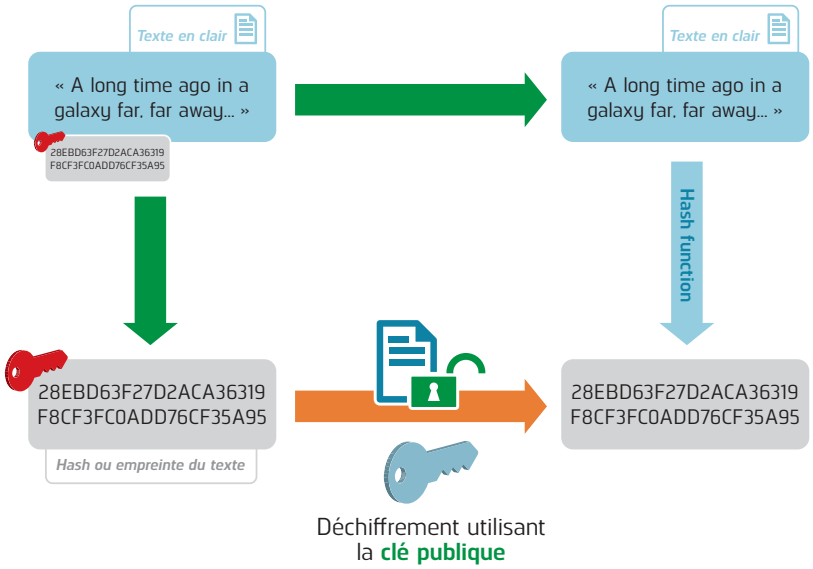

Figure 16. Validation d'une signature électronique

Signature électronique

Une signature électronique offre des garanties qui permettent à un tiers d'avoir confiance en des données électroniques.

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

- assurer l'intégrité et l'authenticité des données signées.
- assurer la non-répudiation de la signature
- en cas d'utilisation d'un certificat qualifié et d'un SSCD, la signature sera du type qualifiée, elle délivre alors une valeur légale reconnue automatiquement comme égale à celle d'une signature manuscrite.

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).

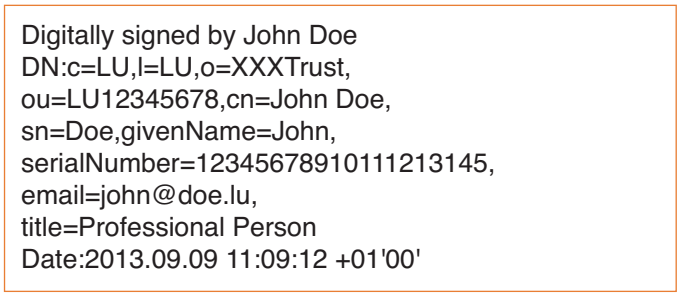

Figure 17. Exemple de certificat servant pour la signature électronique

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 cinq ans : voir exemple de certificat en *Figure 17*). En effet, 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.

FedISA Luxembourg
C/O Labgroup

2-4 rue Edmond Reuter
L-5326 CONTERN

info@fedisa.eu

www.fedisa.eu

La mise en page du présent livre blanc est co-financée par systemat
A PASSION FOR IT SOLUTIONS