Sécurité, disponibilité, confidentialité et intégrité de vos documents dans Zeendoc

Version 1.3
Mai 2018

Table des Matières

1 Introduction

Zeendoc est une solution de Gestion Electronique des Documents disponible en ligne.

Elle ne nécessite aucun investissement, peut être « installée » très rapidement, est accessible 24h/24 7j/7, et l'administration technique et fonctionnelle de la solution est intégrée à la prestation…

L'objet de ce document est d'identifier l'impact de l'externalisation des documents de votre organisation sur leur sécurité, la confidentialité et la conformité à la réglementation, ainsi que de déterminer les mesures techniques ou organisationnelles à mettre en œuvre pour garantir leur sécurité au sein de votre système d'information en complément des mesures déjà intégrées à Zeendoc.

Zeendoc étant une solution packagée utilisée dans une très large variété de contextes, le présent document ne peut pas traiter de toutes les situations possibles. L'existence de ce document ne dispense pas chaque client de réaliser sa propre analyse de risques et de formaliser sa propre politique de sécurité.

Ce document permet simplement de poser en termes les plus clairs possible la problématique de la sécurité des documents et d'identifier la manière dont la solution Zeendoc permet de répondre en partie à cette problématique. Zeendoc participe à une meilleure sécurisation des documents, mais doit être accompagnée de mesures complémentaires au niveau du système d'information client.

Le document est structuré de la manière suivante :

- ✓ Dans un premier temps, les risques encourus par les documents d'une entreprise sont identifiés
- ✓ Les mesures mises en place au sein de Zeendoc pour contrer ces risques sont ensuite détaillées, et une comparaison avec les mesures mises en place au sein d'un PME standard est fournie à titre d'exemple
- ✓ Les mesures qu'il est conseillé de mettre en place par le client sont ensuite listées
- ✓ Enfin, l'option « Archivage à Valeur Probatoire » est présentée. Cette option permet d'utiliser Zeendoc en tant que partie d'un Système d'Archivage Electronique (SAE) de documents conforme à la norme NF Z42-013, c'est-à-dire offrant la meilleure garantie de valeur légale.

2 Quels sont les risques encourus par les documents d'une entreprise ?

On distingue trois familles de risques susceptibles de peser sur des biens critiques d'une entité :

- Les risques pesant sur leur **disponibilité,**
- Les risques pesant sur leur **confidentialité,**
- Les risques pesant sur leur **intégrité.**

Les impacts d'éventuelles atteintes aux documents d'une organisation sont multiples. On peut par exemple citer, parmi les plus fréquents :

- La perte de temps pour restaurer, récupérer ou regénérer l'information perdue (exemple : suppression malencontreuse d'un document issu d'un travail de plusieurs jours)
- Le risque juridique ou fiscal lorsque le document est nécessaire dans un cadre juridique ou fiscal (exemple : altération ou perte d'un contrat ou d'un avenant)
- L'impact financier lorsque le document justifie un profit (exemple : perte d'un avoir)
- La dégradation de l'image de l'organisation (exemple : un document à usage interne diffusé à l'extérieur)
- La perte de savoir-faire (exemple : perte d'une procédure écrite)
- La perte de part de marché (exemple : correspondance interne diffusée par erreur à un client / un concurrent)

Les risques sont variés, et leur probabilité dépend très fortement du contexte dans lequel l'entité évolue : une entreprise de négoce est soumise aux mêmes risques qu'une entreprise à forte expertise technologique, mais les probabilités d'occurrence de chaque risque et leur impact diffèrent très fortement.

Certains de ces risques peuvent paraître anecdotiques dans certains contextes, mais peuvent être particulièrement pertinents dans d'autres. L'objet de ce chapitre est simplement de les lister, sans les prioriser, de manière à permettre ensuite d'identifier des mesures permettant de les contrer.

2.1 Pertes de disponibilité

INCAPACITE TEMPORAIRE A RETROUVER UN DOCUMENT

C'est le cas le plus fréquent de perte de disponibilité : le document est bien présent dans l'entité, mais personne n'est en mesure d'identifier rapidement son emplacement et/ou de le mettre à disposition de la personne qui en a besoin.

DESTRUCTION NON INTENTIONNELLE DU DOCUMENT

Il peut s'agir par exemple d'un incendie dans la pièce où sont stockés les documents, d'une inondation dans la salle des archives, de la suppression involontaire par un utilisateur d'un document numérique non sauvegardé, d'une panne définitive d'un support de stockage, ….

DESTRUCTION VOLONTAIRE OU VOL D'UN DOCUMENT PAR UNE PERSONNE MALINTENTIONNEE

On retrouve par exemple dans ce cadre les vols de titre de propriétés / licences, la « disparition soudaine et inexpliquée » de documents mettant en cause un salarié, ou encore la destruction par un salarié sur le départ de documents qu'il a produit, par simple malveillance.

INCAPACITE A RELIRE DES DOCUMENTS

C'est typiquement le cas de documents produits dans des formats numériques propriétaires ou anciens, pour lesquels l'entité ne dispose plus d'outil de visualisation. Dans le meilleur des cas, l'éditeur commercialise un outil permettant de lire le fichier.

On peut également mettre dans cette rubrique tous les documents qui ne sont pas archivés en tant que tels car susceptibles d'être regénérés à volonté avec le logiciel métier (ERP / Logiciel de gestion commerciale / Paye / …) jusqu'à ce que le logiciel métier soit remplacé par un logiciel plus récent ou plus puissant, et qu'il devienne alors totalement impossible de regénérer les anciens documents.

2.2 Pertes de confidentialité

ACCES D'UN SALARIE A UN DOCUMENT CONFIDENTIEL

Il peut par exemple s'agir d'un salarié ayant accès à un document qui le concerne mais dont il est censé ignorer le contenu (ou l'existence). Dans des secteurs particulièrement critiques, il peut également s'agir d'un salarié sur lequel l'entité à une confiance relative mais ayant par erreur ou omission accès à des documents confidentiels.

ACCES D'UN CONCURRENT / CLIENT A UN DOCUMENT QUI NE LUI EST PAS DESTINE

On peut par exemple citer le cas de documents mis par erreur sur Internet à disposition du plus grand nombre, et notamment de la concurrence. On peut également mettre dans cette rubrique les documents transmis à un prospect / client qui les retransmet intentionnellement à un concurrent.

ACCES D'UN INCONNU A UN DOCUMENT DE L'ENTITE

Rentrent typiquement dans cette rubrique les intrusions de tiers dans le Système d'Information de l'organisation, soit par le biais d'une faille de sécurité dans le système d'information (pare-feu inexistant, mal paramétré, ou intégrant une vulnérabilité), soit par un comportement imprudent d'un utilisateur légitime (clic sur une pièce jointe malveillante, mot de passe faible), soit par un virus, ….

2.3 Pertes d'intégrité

ALTERATION NATURELLE DU DOCUMENT

On peut par exemple citer les dégradations imposées sur les documents papier par la lumière (perte de la visibilité de l'encre), les champignons (en cas d'humidité excessive), le temps (bavure de l'encre), les rongeurs, ….

ALTERATION HUMAINE ET INVOLONTAIRE DU DOCUMENT

Il peut par exemple s'agir d'un liquide renversé malencontreusement sur un document, un froissage du document, des traces de doigts sur un document patrimonial, des déchirures suites à un désagrafage malheureux, ….

ALTERATION INTENTIONNELLE DU DOCUMENT

On trouvera dans ce cadre le remplacement de documents originaux par des copies modifiées, ou la disparition « malencontreuse » de pages spécifiques de documents.

3 Mesures de sécurité intégrées à Zeendoc

3.1 Mesures visant à garantir la disponibilité des documents

SERVEURS EQUIPES DE DISQUES EN RAID

Les serveurs utilisés pour héberger l'architecture Zeendoc sont équipés de technologies RAID, hotspare, et reconstruction à chaud. Le RAID permet de répartir de manière redondante les données sur plusieurs disques durs, de manière à garantir que les données restent disponibles même lorsqu'un disque tombe en panne. Le « hotspare » est un disque supplémentaire intégré au serveur et qui est activé automatiquement par le système en disque de secours lorsqu'une défaillance est détectée sur un des disques principaux. La reconstruction à chaud permet d'enlever un disque défaillant du volume RAID tout en maintenant le serveur en fonctionnement, et de le remplacer par un disque fonctionnel, sans jamais éteindre le serveur ou porter atteinte à la disponibilité des données stockées.

DOUBLE ALIMENTATION DES SERVEURS

Tous nos serveurs disposent de deux alimentations électriques redondantes : lorsque le système détecte une panne sur l'une des alimentations, il bascule automatiquement sur l'autre sans arrêter le serveur et signale par une alerte le dysfonctionnement de l'une des deux alimentations.

DOUBLE ATTACHEMENT RESEAU DES SERVEURS

Tous nos serveurs disposent de deux cartes réseau, connectées chacune à un commutateur réseau différent. Ainsi, si l'une des cartes ou l'un des commutateurs vient à dysfonctionner, le système bascule automatiquement sur l'autre carte et l'autre commutateur.

DOUBLE STOCKAGE DES DONNEES

Les documents archivés dans Zeendoc sont stockés en doubles exemplaires sur deux serveurs de stockage distincts. Dès qu'un fichier est déposé sur un serveur de stockage, il est déposé également sur le second support, de sorte que les deux supports sont strictement identiques à tout instant. Un défaut de fonctionnement sur l'un des deux supports de stockage n'entraîne donc aucune perte de données.

DATA CENTERS SECURISES

Les serveurs de Zeendoc sont hébergés au sein de Data Centers entièrement sécurisés :

- Protection anti-incendie
- Protection anti-inondation
- Régulation de la température
- Ondulation électrique avec secours par groupe électrogène
- Accès restreint aux seules personnes autorisées à accéder physiquement aux serveurs

UN SITE PRINCIPAL ET UN SITE DE SECOURS GEOGRAPHIQUEMENT ELOIGNES

Le site principal peut être secouru par un site de secours pouvant accueillir tout ou partie des services mis à disposition par le site principal. Ces deux sites sont géographiquement éloignés (Paris et Strasbourg), de manière à garantir qu'un événement de grande ampleur impactant l'un des deux sites (tremblement de terre, coupure électrique régionale, perte locale de connexion Internet, …) n'impacte pas l'autre.

SAUVEGARDE QUOTIDIENNE DES DONNEES ARCHIVEES

Une sauvegarde des données archivées au sein de Zeendoc est réalisée quotidiennement.

CONVERSION DES DOCUMENTS VERS UN FORMAT PERENNE

Les documents déposés dans Zeendoc sont convertis (lorsque le format le permet) dans le format actuellement considéré comme le plus pérenne, le format PDF/A.

Si l'état de l'art venait à changer sur le sujet, Zeendoc s'engage contractuellement à convertir à sa charge les documents archivés dans Zeendoc vers le nouveau format, de sorte que les utilisateurs de Zeendoc disposent de la garantie de pouvoir relire leurs documents aussi longtemps qu'ils souscrivent au service.

A noter que le document est également conservé dans son format originel au sein de Zeendoc, de manière à permettre de récupérer au besoin le document dans son format initial, et de le retravailler par exemple avec l'application ayant servi à le créer.

HAUTE DISPONIBILITE

Les serveurs de Zeendoc sont administrés en Haute Disponibilité. En cas de défaillance de l'un des serveurs une solution de secours peut être mise en œuvre soit manuellement soit automatiquement pour prendre le relais du serveur défaillant par un autre serveur. Cette bascule est entièrement transparente pour les utilisateurs.

SUPERVISION CONTINUE

Les serveurs de Zeendoc sont supervisés continuellement. Un dysfonctionnement sur l'un des éléments de l'architecture donne lieu à la génération d'une alerte sur une console centralisée, et éventuellement de l'envoi de mails ou de SMS aux administrateurs techniques et/ou au personnel d'astreinte. L'alerte est alors traitée par l'un des administrateurs de Zeendoc selon les procédures définies.

SUPPRESSION REVERSIBLE D'UN DOCUMENT

La solution Zeendoc a été conçue pour qu'il soit possible de restaurer les documents supprimés. Lorsque l'utilisateur demande la suppression d'un document, le document est simplement « taggué » comme étant supprimé, mais reste stocké sur les serveurs de Zeendoc. Il est ainsi possible pour les utilisateurs disposant des droits adaptés de restaurer un document supprimé, et d'identifier l'utilisateur à l'origine de la suppression.

Cette conservation des documents supprimés n'engendre aucun surcout : le service Zeendoc n'est pas facturé au volume de documents conservés, mais au volume de documents ajoutés par mois.

SUPPRESSION DEFINITIVE D'UN DOCUMENT[1]

Dans certains cas, en particulier lors de l'exercice d'un droit à l'oubli, il peut être nécessaire de procéder à la suppression définitive de documents. C'est une procédure explicite, qui devient effective après un certain délai qui court à compter de la demande de suppression définitive. Cette suppression peut générer des alertes envoyées à la personne qui l'a demandée avant de devenir définitive et irréversible. Cela permet d'annuler les demandes de suppression définitive jusqu'au dernier moment.

[1] La fonctionnalité de suppression définitive sera mise en place dans ZeenDoc courant 2018.

3.2 Mesures visant à garantir la confidentialité et la sécurité des documents

CHIFFREMENT DES DOCUMENTS STOCKES SUR LES SERVEURS DE ZEENDOC

Après avoir subi les différents traitements de valorisation, les documents déposés au sein de Zeendoc sont chiffrés avec une clef spécifique à chaque client, en utilisant le protocole AES. La clef de déchiffrement est elle-même cryptée avec le mot de passe de l'utilisateur, de sorte que seul le détenteur de ce mot de passe est capable de déchiffrer le document. En accédant directement aux serveurs, les documents ne sont pas lisibles, ni par nos administrateurs, ni par un éventuel pirate informatique.

ACCES SECURISE PAR MOT DE PASSE

La fourniture d'un identifiant et d'un mot de passe valides sont nécessaire pour se connecter à Zeendoc. Si une personne malveillante tente de se connecter au compte d'une autre personne, après trois échecs d'authentification, un email d'alerte est envoyé automatiquement à la personne dont le compte est utilisé pour tenter de se connecter à Zeendoc.

LES MOTS DE PASSE DES UTILISATEURS NE SONT PAS STOCKES AU SEIN DE ZEENDOC

Pour vérifier que la personne qui se connecte est bien celle qu'elle prétend être, un mot de passe est demandé à l'identification. Néanmoins, aucun mot de passe utilisateur n'est stocké au sein de Zeendoc.

Lors de l'enregistrement initial du mot de passe de l'utilisateur, une fonction de chiffrement à sens unique est appliquée au mot de passe, et c'est le résultat de cette fonction qui est stocké en base. L'utilisation d'une fonction de cryptographie à sens unique permet de garantir qu'il n'est pas possible de retrouver le mot de passe à partir du résultat de la fonction.

Lors du renseignement du mot de passe par l'utilisateur, cette même fonction est appliquée sur le mot de passe, et si le résultat est identique à celui stocké en base, c'est que le mot de passe fourni est identique à celui d'origine.

Une des conséquences de ce mode de stockage est que les personnels de Zeendoc ne peuvent jamais accéder à votre mot de passe. En particulier, si vous avez oublié votre mot de passe, ce n'est pas la peine de leur demander de vous le communiquer, ils ne sont pas en mesure de le faire. Seul un courriel de réinitialisation du mot de passe peut vous être envoyé. Il est alors essentiel que vos propres politiques de sécurité et de confidentialité prennent en compte la sécurisation et la confidentialité des accès aux courriels de réinitialisation des mots de passe.

CHIFFREMENT SSL/TLS DES COMMUNICATIONS AVEC LES SERVEURS ZEENDOC

Dès la connexion à une armoire Zeendoc, les communications entre le poste de l'utilisateur et les serveurs Zeendoc sont chiffrées au sein d'un tunnel SSL/TLS. Ce tunnel est fourni par le protocole HTTPS. C'est exactement le même protocole et le même niveau de sécurité que celui mis en place par les banques pour se connecter à leurs interfaces en ligne de gestion de comptes.

Ainsi, même si les communications entre le poste de l'utilisateur et les serveurs de Zeendoc étaient interceptées, le contenu de ces communications, y compris le contenu des documents, ne serait pas accessible.

DATA CENTERS A ACCES RESTREINT AUX SEULES PERSONNES AUTORISEES

Les accès physiques aux Data Centers hébergeant les serveurs de Zeendoc sont strictement limités aux seules personnes autorisées. Les personnes ne disposant pas de droits d'accès explicites au serveur n'y ont pas physiquement accès. Par ailleurs, les accès font l'objet d'une journalisation.

PROTECTION DES ACCES LOGIQUES AUX SERVEURS PAR UN PARE-FEU (FIREWALL) PROFESSIONNEL

Les accès logiques aux serveurs de Zeendoc sont contrôlés par un pare-feu professionnel. Seuls les accès strictement nécessaires sont autorisés. Les accès administratifs sont limités aux seules adresses IP des postes d'administration.

LES ACCES AUX DOCUMENTS SONT GERES PAR LE CLIENT DIRECTEMENT

Les utilisateurs disposant de privilèges d'administration peuvent gérer les personnes susceptibles d'accéder à leurs classeurs. En complément, au sein même de ces classeurs, ils peuvent gérer à la fois les fonctionnalités auxquelles ces personnes ont accès et les documents auxquels ils ont accès.

LES TRAITEMENTS DES DOCUMENTS SONT JOURNALISES

Tous les traitements sur les documents sont journalisés. Cela permet des analyses a posteriori.

Que ce soit dans le cas d'une consultation, d'une modification ou d'une suppression de document, les actions des utilisateurs sur les documents font l'objet d'une journalisation. Ces journaux sont accessibles soit depuis les pages d'administration, auquel cas tous les événements relatifs aux documents de votre armoire sont visibles, soit depuis la page de consultation d'un document, auquel cas seuls les événements relatifs au document courant sont affichés.

Cette mesure permet de remplir les obligations réglementaires de journalisation, notamment dans le cadre du Règlement Général sur la Protection des Données (RGPD).

VEILLE TECHNOLOGIQUE ET MISES A JOUR REGULIERES

Les Systèmes d'Exploitation et logiciels utilisés au sein de Zeendoc font l'objet d'une veille technologique permettant à nos administrateurs systèmes d'être informés très rapidement de toute faille découverte sur ces outils. Sur détection d'une faille, le correctif mis à disposition par l'éditeur est immédiatement testé, validé et appliqué.

ANALYSES DE VULNERABILITE ET TESTS DE PENETRATION

Les services et serveurs de Zeendoc sont régulièrement soumis à des analyses de vulnérabilité et à des tests de pénétration. S'ils révèlent des failles ou des vulnérabilités présentant un risque pour la sécurité et la confidentialité des documents et des données de Zeendoc, des mesures de correction sont rapidement mises en place.

3.3 Mesures visant à garantir l'intégrité des documents

LES UTILISATEURS ACCEDENT A UNE COPIE DU DOCUMENT

Contrairement à ce qui se passe lorsque les utilisateurs accèdent à un document sur un serveur local, lorsqu'ils consultent un document archivé au sein de Zeendoc, les utilisateurs accèdent à une copie du document. Quelles que soient les actions qu'ils réalisent sur leur copie du document, le document stocké au sein de Zeendoc n'est pas impacté.

L'INTEGRITE DES DOCUMENTS EST REGULIEREMENT VERIFIEE

Au dépôt du document dans Zeendoc, une empreinte du document est calculée lors du dépôt, via un algorithme de hachage (SHA-3), et cette empreinte est enregistrée conjointement au document (sur un support différent).

Régulièrement, un contrôle d'intégrité est lancé sur les documents archivés au sein de Zeendoc : l'empreinte de chaque document est de nouveau calculée et comparée à celle qu'il avait lors de son dépôt. En cas de perte d'intégrité, les administrateurs système sont immédiatement alertés, de manière à pouvoir traiter l'erreur, et récupérer éventuellement le fichier intègre depuis une sauvegarde.

A LA MISE A DISPOSITION DU DOCUMENT ORIGINAL, L'INTEGRITE DU DOCUMENT EST CONTROLEE

Lorsque l'utilisateur demande à télécharger le document original, il peut contrôler que l'empreinte calculée lors du dépôt du document est toujours identique à l'empreinte actuelle du document.

Il peut également utiliser ces empreintes pour vérifier que le fichier n'a pas subi d'altération après téléchargement, en contrôlant que le fichier une fois téléchargé à toujours la même empreinte SHA-3.

LES DOCUMENTS PEUVENT ETRE SCELLES

Les documents versés au sein de Zeendoc peuvent être signés électroniquement par l'application d'un certificat. Le certificat utilisé au sein de Zeendoc est de type RGS 2* (référentiel général de sécurité [2]deux étoiles). On parle alors de certification ou de scellement électronique du document. L'application de la signature est horodatée et cet horodatage est inclus dans la signature. Une telle certification a une valeur légale et/ou fiscale en ce sens qu'elle rend compte du fait que le document a été scellé au moment de l'application de la signature électronique et qu'il n'a pas été modifié depuis. Ainsi, quand un document doit être conservé pour des raisons réglementaires son scellement peut avoir une valeur probatoire en ce qui concerne son intégrité et le fait qu'il n'a pas été modifié depuis la date de scellement.

Une fois scellé, le document numérique peut être copié, téléchargé, visualisé et sa signature peut être vérifiée de façon à apporter la certitude que le document n'a pas été modifié depuis son scellement, et ce même lorsqu'il est extrait de Zeendoc, par exemple lorsqu'il est envoyé par courriel ou, plus généralement, fourni de façon numérique (clé USB, stockage informatique etc.).

Vous pourrez produire des documents scellés très facilement et très rapidement, et ce à chaque fois que cela vous sera nécessaire. Leur scellement rendra compte du fait qu'ils n'ont pas été modifiés depuis la date de la signature électronique qui y est apposée.

[2] Référentiel Général de Sécurité, voir https://fr.wikipedia.org/wiki/référentiel_général_de_sécurité

4 Exercice des droits des personnes concernées

La réglementation en termes de données personnelles, en particulier dans le cadre du RGPD, impose aux responsables de traitement et à leurs sous-traitants de rendre possible l'exercice des droits des personnes concernées, notamment les droits d'accès, de modification et d'oubli. Dans le cadre de l'utilisation de Zeendoc, les personnes concernées sont celles dont les données, notamment nom, prénom, adresse postale, etc., sont présentes dans les documents déposés au sein de Zeendoc.

Zeendoc intègre des moyens permettant l'exercice des droits des Personnes Concernées au sens de la réglementation, notamment le droit à l'oubli ou le droit d'accès, ainsi que le droit à la portabilité. Ainsi, lorsque vous recevez une demande d'exercice d'un tel droit et que vous avez déposé au sein de Zeendoc des documents contenant des données à caractère personnel concernant le demandeur, vous pouvez très facilement effectuer des recherches permettant de trouver toutes les données associées à la personne concernée, notamment des recherches sur les identifiants du demandeur (nom et prénom, référence client ou de dossier, etc.). L'extraction, la consultation et l'effacement des documents qui contiennent des données à caractère personnel concernant la personne qui demande l'exercice d'un de ses droits se trouve grandement facilitée par le fait que les documents contenant des données associées au demandeur ont été versés dans ZeenDoc.

Par ailleurs, certains documents doivent être archivés pour des raisons réglementaires : bulletins de salaires, factures, bons de commandes, etc. Si vous envisagez de supprimer des documents pour permettre l'exercice d'un droit de suppression, veillez à archiver, dans Zeendoc ou ailleurs, une copie de chaque document qui doit être archivés. Si vous conservez un tel document dans Zeendoc, indiquez avec un champ d'index dédié que le document est une archive ou déplacez le dans un classeur dédié aux documents archivés ne devant plus être traités et mettez en place les contrôles nécessaires à ce que les données contenues dans ces documents archivés ne fassent l'objet d'aucun traitement ultérieur. En particulier, les documents ainsi indexés ne devraient pas faire l'objet d'extraction de coordonnées aux fins de prospection.

Risques / Contre-mesures	Sans Zeendoc Au sein d'un système d'information standard	Avec Zeendoc
Destruction non intentionnelle du document	✓ RAID (dans le meilleur des cas) ✓ Sauvegarde régulière	✓ RAID, redondance ✓ DataCenters protégés (incendies, inondations) ✓ Double stockage ✓ Sauvegarde quotidienne et supervisée ✓ Suppression impossible ✓ Journalisation des accès
Destruction volontaire d'un document		
Incapacité temporaire à retrouver un document		✓ Capacités de recherche étendues ✓ Recherche dans le contenu des documents
Incapacité à relire des documents numériques		✓ Utilisation d'un format de conservation pérenne ✓ Conversion de formats suivant l'état de l'art
Accès d'un salarié à un document confidentiel	✓ Gestion des accès (physiques et logiques)	✓ Gestion des accès (logiques) et fonctionnalités ✓ Traçabilité des accès
Accès d'un concurrent / client à un document	✓ Soin lors de la diffusion des documents	✓ Soin lors de la diffusion des documents ✓ Traçabilité des accès
Accès d'un pirate à un document	✓ Réseau protégé par un routeur filtrant ✓ Antivirus, sensibilisation des utilisateurs	✓ Réseau protégé par un pare-feu professionnel ✓ Antivirus, pas d'utilisateur sur les serveurs ✓ Système de Détection d'Intrusion ✓ Chiffrement des documents
Altération naturelle du document		✓ Numérisation des documents papiers ✓ Empreinte lors du dépôt + Vérification régulière
Altération humaine et involontaire du document	✓ Limitation des manipulations sur le document	✓ Réversibilité des modifications sur le document ✓ Action sur une copie des documents ✓ Scellement du document
Altération intentionnelle du document		✓ Réversibilité des modifications sur le document ✓ Action sur une copie des documents ✓ Traçabilité des modifications

5 Utiliser Zeendoc de manière sécurisée

L'ensemble des mesures prises au sein de Zeendoc doivent être complétées par des bonnes pratiques « utilisateur » :

- Utiliser un mot de passe fort (évitez la date de naissance, le prénom de son conjoint ou de ses enfants, et toute information qui peut être consultée facilement en particulier sur les réseaux de communications, les réseaux numériques comme Internet ou les réseaux sociaux…) !

- Ne pas enregistrer son mot de passe dans son navigateur Internet (qui est sur un poste qui peut être volé ou piraté)

- Modifier son mot de passe d'accès à Zeendoc dès que celui-ci a été transmis sur un support non sécurisé (comme par exemple une messagerie)

- Ne pas réutiliser pour Zeendoc un mot de passe déjà utilisé pour se connecter à un service moins sécurisé (par exemple utiliser un mot de passe différent de celui utilisé sur les sites de ventes en ligne ou sur les réseaux sociaux)

- Ne pas utiliser Zeendoc depuis un poste non sécurisé comme un poste public (sur lequel peut par exemple avoir été installé un mouchard par un tiers malveillant). Pour une utilisation sécurisée, les postes utilisés pour se connecter à Zeendoc doivent être sécurisés notamment à l'aide d'anti-virus, d'un pare-feu et d'outils de détection et de suppression des logiciels malveillants

- Sécuriser l'accès à sa messagerie : via une messagerie compromise, un pirate peut accéder à tout message reçu sur la messagerie, y compris un message permettant la réinitialisation du de passe Zeendoc, qui est envoyé en cas de demande de réinitialisation, à son initiative ou à celle de l'utilisateur légitime.

6 Zeendoc et l'option SAE

La valeur probatoire ou probante des documents est une question intimement liée à la notion de « document original », au sens juridique du terme, c'est-à-dire à un document

1. à la disposition de celui qui acquiert un droit par le document,
2. qui est intègre,
3. qui est produit par celui qui prétend l'avoir produit, et
4. qui a été produit au moment où il prétend l'avoir été.

Un document original produit ou reçu de manière numérique est généralement acceptable juridiquement s'il est possible de démontrer qu'il a été conservé dans un système garantissant que les caractéristiques qui en font un original (disponibilité, intégrité, signature, et horodatage) n'ont pas pu être mises à mal.

De la même manière, un document papier numérisé est généralement acceptable juridiquement :

- ✓ S'il est possible de démontrer que le processus de numérisation n'a pas mis à mal ces caractéristiques,
- ✓ S'il la conservation de la version numérique s'est faite au sein d'un système garantissant que ces caractéristiques n'ont pas pu être mises à mal
- ✓ Si l'original papier a été détruit de manière non intentionnelle

Lorsqu'on désire profiter de la meilleure valeur probatoire offerte par un coffre-fort électronique certifié, ces documents peuvent être conservés au sein d'un Système d'Archivage Electronique (SAE) permettant d'obtenir le meilleur niveau de confiance qu'il n'y a eu aucune altération du caractère original du document. Le législateur ne fournissant pas d'indication sur la manière dont ce SAE doit être conçu et géré, l'AFNOR et l'APROGED (Association des Professionnels de la GED) se sont réunis pour rédiger une norme décrivant la manière de concevoir et d'administrer un SAE pour qu'il soit accepté par un juge comme système d'archivage de documents originaux. Cette démarche a donné lieu à la norme **NF Z42-013**[3].
Le respect de cette norme ne permet pas d'obtenir la valeur probante des documents (un juge n'est pas obligé d'accepter le document en tant qu'original), même si c'est une chose qu'on lit très souvent… Elle permet par contre d'obtenir une valeur probatoire, c'est-à-dire qu'elle fournit au juge la meilleure garantie possible sur le fait que les documents qu'il contient ont conservé leur caractère original.

Zeendoc a établi un partenariat avec la société CDC ARKHINEO, son sous-traitant en la matière, filiale de la Caisse des Dépôts et Consignation, pour permettre à ses clients de conserver, en complément de la conservation au sein de Zeendoc, une copie conforme des documents versés au sein du coffre-fort numérique de la CDC. Ce stockage complémentaire et optionnel permet un archivage à valeur probante conforme à la norme NF Z42-013 et certifié NF 461, et une conservation par un tiers indépendant de Zeendoc. Zeendoc peut ainsi être utilisée comme un élément constitutif d'un SAE à valeur probante. Le bénéfice de cette option est lié à la valeur conférée aux documents ainsi stockés : Tout document stocké dans le SAE Arkineo sera acceptable juridiquement en tant que copie conforme du document versé dans Zeendoc, qu'il soit nativement numérique ou issu d'une numérisation. En particulier, les documents issus de factures (nativement numériques ou numérisées) et bénéficiant de l'option de stockage CDC-Arkhineo sont ainsi réputés être des copies conformes des documents qui ont été déposés dans Zeendoc.

Pour plus de détails, consulter le site CDC Arkhineo : http://cdcarkhineo.com

En ce qui concerne l'archivage avec scellement de certains types de documents, notamment les factures, on pourra par ailleurs se référer aux sections Les documents peuvent être scellés et Archivage des factures et piste d'audit fiable ci-dessus.

[3] Le lecteur pourra se référer à la norme NF Z42-013 pour des informations plus précises et détaillées à ce sujet. L'objet de ce chapitre n'est pas d'en faire une synthèse, mais d'expliquer certains aspects de la problématique liée à la valeur légale ou probatoire des documents numériques et ce que ZeenDoc peut apporter à un client dans cette démarche.