



A propos de la sécurité

Jean-Michel Drappier & Franck Valetas

REF : GMA/COM/Sécurité
révision mars 2025

Table des matières

Introduction.....	2
Conformité aux normes des coffres forts.....	2
La continuité d'accès et la protection contre la perte de données.....	3
A propos des Datacenter.....	3
Solution souveraine.....	4
Le contrôle d'accès et la confidentialité.....	5
Les contrôles d'entrées-sorties.....	5
Les contrôles d'identité.....	5
Cas de l'API.....	5
Le chiffrement.....	5
Maintenance.....	6

Introduction

La sécurité absolue n'existe pas, ni dans la vie réelle ni dans le numérique. Ce qui est important, c'est les moyens mis en œuvre pour atteindre le niveau de sécurité souhaitée.

Ce document vous informe sur les mesures prises par *GererMesAffaires* pour garantir la sécurité des données et des documents que vous enregistrez dans vos coffres. Le but est de vous permettre de juger si le niveau de sécurité que nous proposons, vous convient.

La sécurité des données et des documents enregistrés dans un coffre recouvre deux aspects bien distincts abordés dans les deux chapitres suivants.

- La continuité d'accès et la protection contre la perte de données.
- Le contrôle d'accès et la confidentialité.

Conformité aux normes des coffres forts.

Ce produit est conforme aux exigences de la marque NF203 CCFN certifié par :

AFNOR Certification
11, rue Francis de Pressensé
93571 SAINT DENIS LA PLAINE CEDEX

Le référentiel de certification peut être obtenu auprès d'INOCERT qui audit GererMesAffaires chaque année.

La marque NF203 CCFN atteste la conformité à :

- ISO 9001 : Systèmes de management de la qualité
- NF ISO/CEI 25051 : Ingénierie du logiciel
- NFZ42-020 : Spécifications fonctionnelles d'un composant Coffre-Fort Numérique

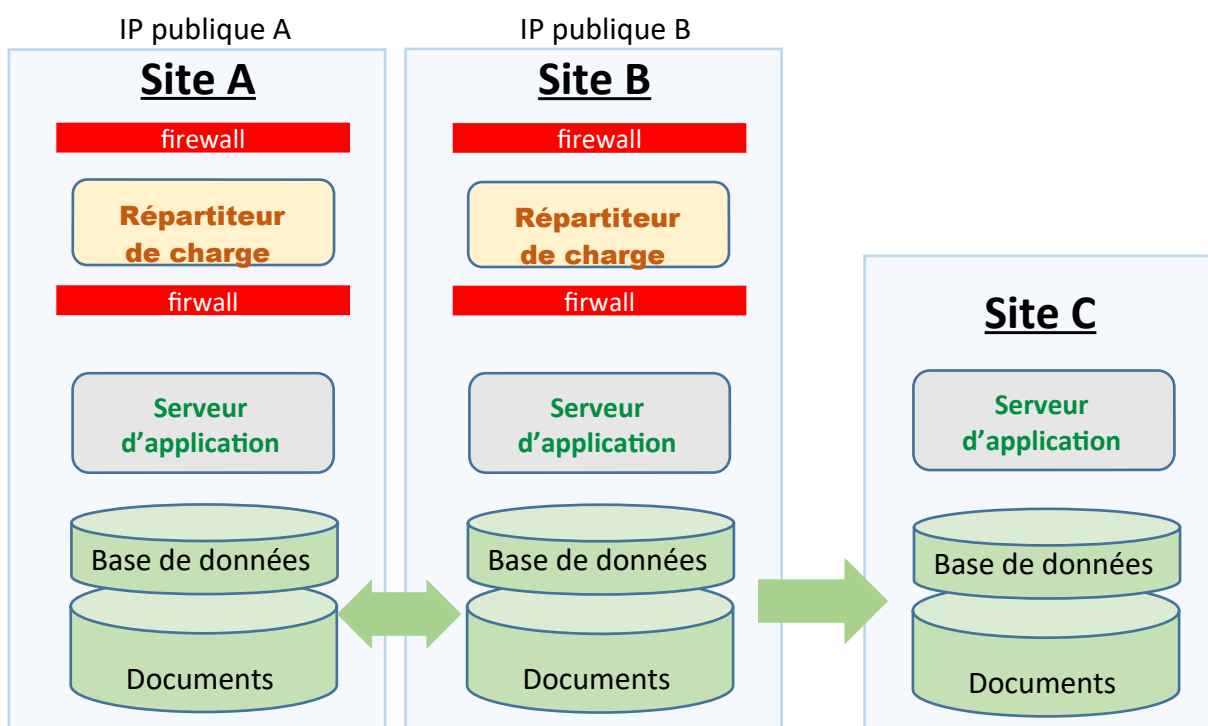
La continuité d'accès et la protection contre la perte de données.

Le but ici est de garantir que toutes les données restent accessibles à leur propriétaire, dans la durée, et quel que soit les événements qui peuvent survenir : crash de serveurs, incendie, vol.

Dans ce but le service *GererMesAffaires* est entièrement redondant. Le service est accessible par deux adresses IP distinctes. Toutes les fonctions du service sont dédoublées dans deux *Datacenters* sur deux sites A et B différents.

Toutes les données et tous les documents sont synchronisés entre les deux *Datacenters*. Lorsque vous téléversez un document ou quand vous saisissez des données sur l'un des *Datacenter*, ce document et ces données sont immédiatement dupliqués dans l'autre *Datacenter*.

En plus de cette redondance, les bases de données et les documents sont sauvegardés, en ligne, dans un troisième *Datacenter* sur un troisième site C sans aucun accès externe.



Tous les tiers de stockage possèdent un RAID pour parer au crash disque. Les serveurs sont sauvegardés régulièrement et peuvent donc être restaurés très rapidement.

Le plan de reprise d'activité (PRA) comprend un ensemble de procédures allant de la simple restauration d'un serveur en quelques minutes, au démarrage du service sur le site de sauvegarde C en cas d'indisponibilité des deux sites A et B quel qu'en soit la cause : une simple coupure d'alimentation prolongée ou une destruction complète par un incendie.

A propos des Datacenter

Les Datacenter que nous retenons pour héberger nos services et donc vos coffres, répondent aux plus hautes exigences de sécurité et disposent des certifications suivantes :

- SAE 3402 –Contrôle des activités externalisées.

- ISO 27001:2005 -Gestion de la sécurité de l'information
- ISO 9001:2008 -Gestion des systèmes de qualité
- ISO 14001:2004 -Gestion environnementale
- ISO 50001:2011 –Gestion de l'énergie
- ISO 22301 :2012 -Gestion de crise
- OHSAS 18001:2007 -Gestion de la santé et de la sécurité au travail

Les *Datacenters* sont en tiers III+. Ils sont habilités pour héberger des données de santé (HDS) et les données de cartes de paiement (PCI DSS).

Ils sont situés en dehors des zones à risques en application des articles L125-5 et R 125-26 du code de l'environnement :

- Pas de risque sismique
- Pas de risque Seveso
- Pas de risque d'inondation (point haut)
- Pas de risque de foudre
- Pas de couloir aérien

Solution souveraine

Nos datacenters sont tous situés en France et nous choisissons nos prestataires pour être des sociétés françaises non contrôlées par des capitaux américains et donc non concernées par l'extraterritorialité du droit américain (Cloud act, Patriot act, FISAA etc.). Nous rappelons que le stockage en France n'est pas une condition suffisante pour que les données ne partent pas aux Etats unis.

Le contrôle d'accès et la confidentialité.

Nous exposons ici les mesures de sécurité prises pour assurer aux propriétaires des coffres la maîtrise de l'accès à leurs données et à leurs documents.

L'ensemble de nos serveurs sont dans un réseau privé indépendant dont seul *GererMesAffaires* a la maîtrise.

Les contrôles d'entrées-sorties

Le seul protocole autorisé en entrée, par les multiples barrières mises en œuvre, est le protocole https sur le port standard avec un certificat étendu. Tout autre protocole est bloqué en entrée (la maintenance et l'administration passent par un VPN).

Les sorties sont également rigoureusement contrôlées et limitées aux services externes (envoi de mails, envoi de SMS, ...)

Les contrôles d'identité

Les membres de *GererMesAffaires* s'inscrivent avec leur véritable identité. Aucun alias n'est autorisé. Nous vérifions le N° de téléphone mobile et l'adresse mail.

Lorsqu'un membre s'inscrit, il reçoit un mot de passe par sms qu'il doit impérativement modifier par un mot de passe sécurisé à l'ouverture de la première session. Son identifiant est son adresse mail utilisée lors de son inscription, il est strictement personnel car il permet l'accès au coffre privé du membre. Il peut choisir de remplacer l'adresse mail par un identifiant anonyme généré aléatoirement donc plus sécurisé.

Chaque membre est :

- soit parraîné par un autre membre validé lors d'une invitation sur l'un de ses coffres,
- soit validé par *GererMesAffaires* après vérification de la concordance entre ses informations d'identification (nom, prénom, lieu et date de naissance) et celles de sa pièce d'identité.

GererMesAffaires recommande à ses membres l'usage de l'authentification via des *PassKey*. Ce mécanisme (MFA) est le plus simple et le plus fiable car il n'utilise plus de mot de passe.

Cas de l'API

Les accès via l'API se font sous la responsabilité d'un membre qui doit s'identifier via le protocole OAUTH2.

Il n'y a aucun passe-droit dans les règles de contrôle d'identité et d'autorisation d'accès aux données des coffres via l'API.

En l'absence d'identification d'une personne physique, le logiciel ne peut que téléverser des documents dans les coffres. Il ne peut accéder à aucune donnée.

Le chiffrement

Toutes les données et tous les documents de vos coffres sont chiffrés. Certaines données secrètes peuvent être chiffrées à l'aide du mot de passe de son propriétaire.

Le code source du service est lui aussi chiffré pour minimiser les risques de piratage.

Maintenance

Aucune personne externe à *GererMesAffaires* n'a accès aux serveurs. Parmi le personnel de *GererMesAffaires*, seules les personnes dûment habilités ont accès au réseau pour effectuer les tâches de maintenances indispensables.

Le personnel n'a aucun accès aux contenus des coffres. Si une opération de correction d'anomalie nécessite un accès à un coffre, la personne en charge demande à un administrateur du coffre un accès temporaire limité à l'analyse du problème.