Dossier d’Architecture Technique

Suivi du document

Version	Date	Auteurs	Objet de la mise à jour
1.2	Eté 2027	Nicolas MARCHAND	Mise à jour des éléments techniques
1.1	Nov 2021	Nicolas MARCHAND	Déplacement des chapitres Jet, FEC, Sauvegarde, Archives fiscales, RGPD vers le DCF
1.0	30/06/2021	Nicolas MARCHAND	Création du document

Définition du document

Ce document constitue le Dossier d'Architecture Technique (DAT) du progiciel LoGeAs. Il a pour objet de décrire en profondeur l'implémentation technique de la solution, dans le cadre de la démarche de certification NF203/NF552, en complément du Dossier de Conception Générale (DCG) et du Dossier de Spécifications Fonctionnelles (DSF).

Il couvre notamment :

- les technologies, langages et frameworks utilisés pour le développement et l'exécution de la solution ;
- l'architecture détaillée du système, incluant la nature et le sens des flux entre les différents composants (serveurs applicatifs, postes clients, outils de supervision) ;
- les protocoles de communication utilisés entre ces composants ;
- les algorithmes de signature et de hachage employés pour garantir l'intégrité, l'inaltérabilité et la traçabilité des données (enregistrements en base, fichiers, piste d'audit) ;
- l'architecture de supervision et son articulation avec la gestion des incidents (approche ITIL) ;
- l'historique versionné de ces éléments techniques, afin de tracer la conformité du logiciel aux marques NF successives (NF203, NF552) et au référentiel FIDELE (R19).

Les sujets relatifs à la sauvegarde des données, aux archives fiscales, au FEC et à la RGPD sont traités dans le DSF et ne sont pas repris ici.

Ce document s'adresse aux auditeurs en charge de la certification ainsi qu'aux équipes techniques internes chargées de la maintenance et de l'évolution de la solution. Il est mis à jour à chaque évolution significative de l'architecture technique.

Architecture globale de l'infrastructure

Vue d'ensemble des composants — serveur applicatif, postes clients, outils de supervision, prestataires (Prosoluce)

L'infrastructure physique de LoGeAs Informatique s'articule autour de trois sites. **Le site principal est hébergé à Saint Gaudens**, dans le datacenter de Prosoluce, au sein d'une demi baie dédié à notre activités. Il héberge les deux nœuds de virtualisation Proxmox — LOGEAS1 et LOGEAS2,

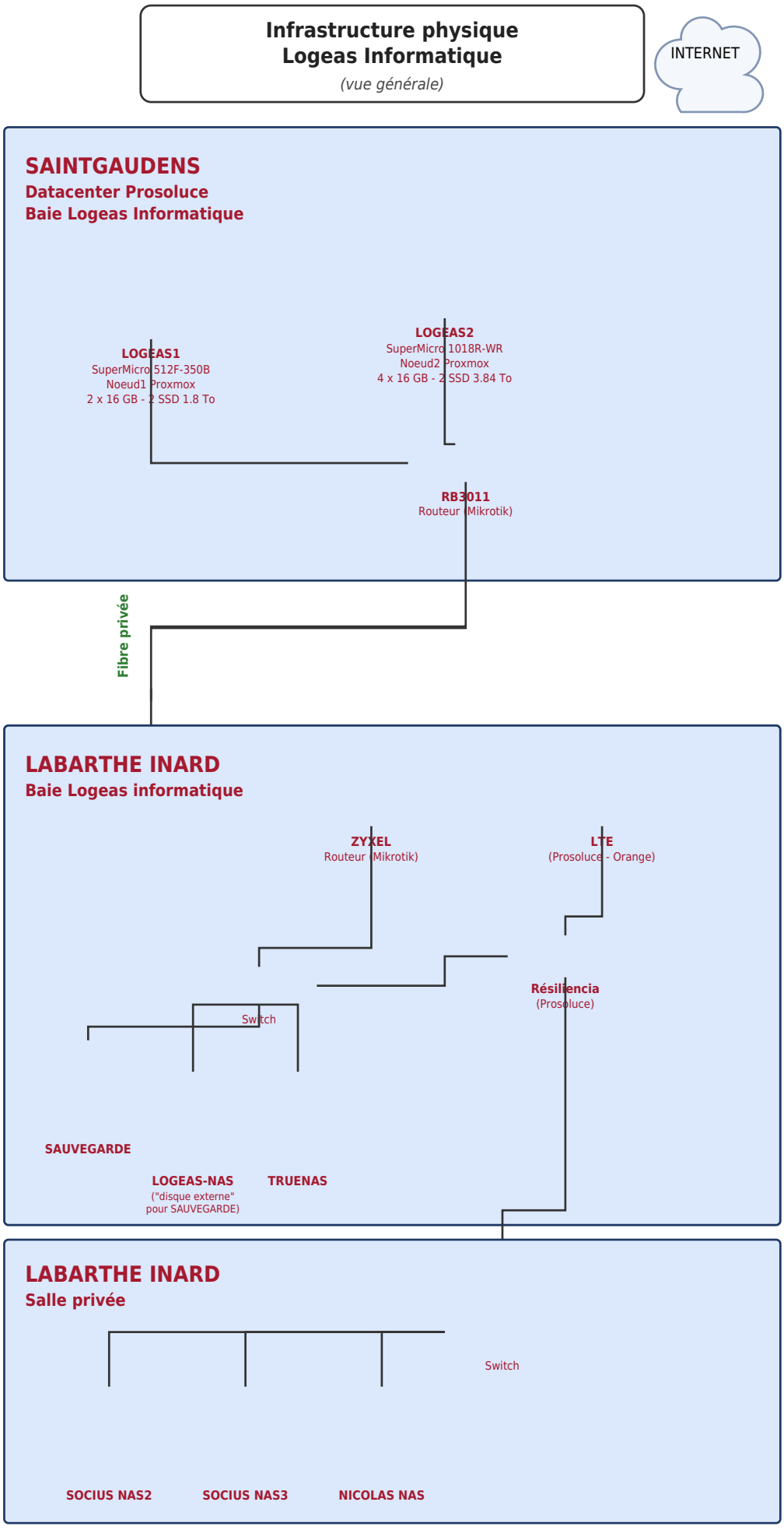
serveurs SuperMicro — qui portent l'ensemble des machines virtuelles applicatives. Ces deux serveurs sont reliés au routeur RB3011 (Mikrotik), point de sortie réseau du site.

Le site de Labarthe Inard héberge deux zones distinctes : la baie Logeas informatique et la salle privée. La baie Logeas informatique reçoit la connectivité du site de Saint Gaudens par deux voies complémentaires : une liaison Internet classique, via une fibre privée relie directement le site à notre baie dans le data-ceenter, et une liaison LTE de secours (Prosoluce/Orange), aboutissant au boîtier Résiliencia. Cette redondance des accès WAN vise à garantir la continuité de service en cas de défaillance de l'un des deux liens.

Enfin, la salle privée de Labarthe Inard, alimentée depuis la baie Logeas informatique via Résiliencia, héberge trois serveurs de stockage supplémentaires (SOCIUS NAS2, SOCIUS NAS3, NICOLAS NAS) raccordés à un commutateur dédié.

Schéma d'architecture globale

NB : SVG stocké sur le wiki éditable par exemple avec Inkscape



Architecture technique des serveurs applicatifs

Les serveurs web applicatifs sont hébergés sous forme de machines virtuelles sur les nœuds de virtualisation Proxmox du site de Saint-Gaudens (LOGEAS1 et LOGEAS2). Le serveur web utilisé est **Microsoft IIS**, qui a remplacé nginx sur ces environnements.

app.logeas.fr (VM sur LOGEAS1)

Ce serveur héberge deux sites, chacun exposé sur une adresse IP publique dédiée. Les deux sites sont exposés exclusivement en HTTPS. Le module Application Request Routing (ARR) et le proxy IIS sont installés sur ce serveur.

Site	Adresse IP	Port	Accès	Rôle
bases-ws.logeas.fr	185.61.118.200	443	Restreint (liste blanche IP)	Serveur des bases de données clients du logiciel LoGeAs
monespace.logeas.fr	185.61.118.198	443	Ouvert	Interface de gestion des utilisateurs et de leurs droits d'accès aux bases

NB : le site bases.logeas.fr, présent dans la configuration technique, est hors service et n'est pas documenté ici.

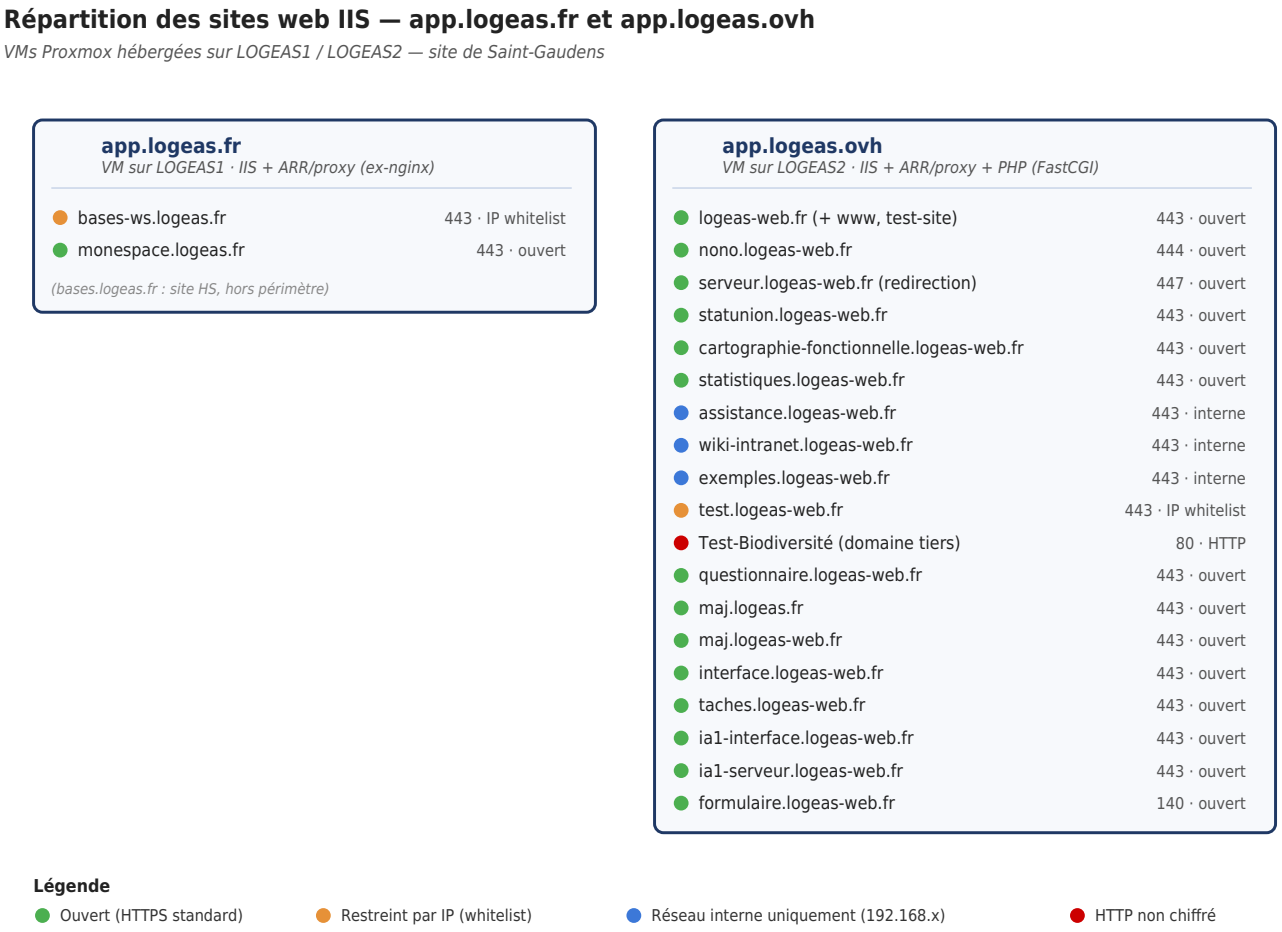
app.logeas.ovh (VM sur LOGEAS2)

Ce serveur héberge l'ensemble des sites secondaires de l'écosystème LoGeAs. Il intègre en complément un moteur PHP (FastCGI), notamment utilisé par le wiki intranet, ainsi que le module ARR/proxy.

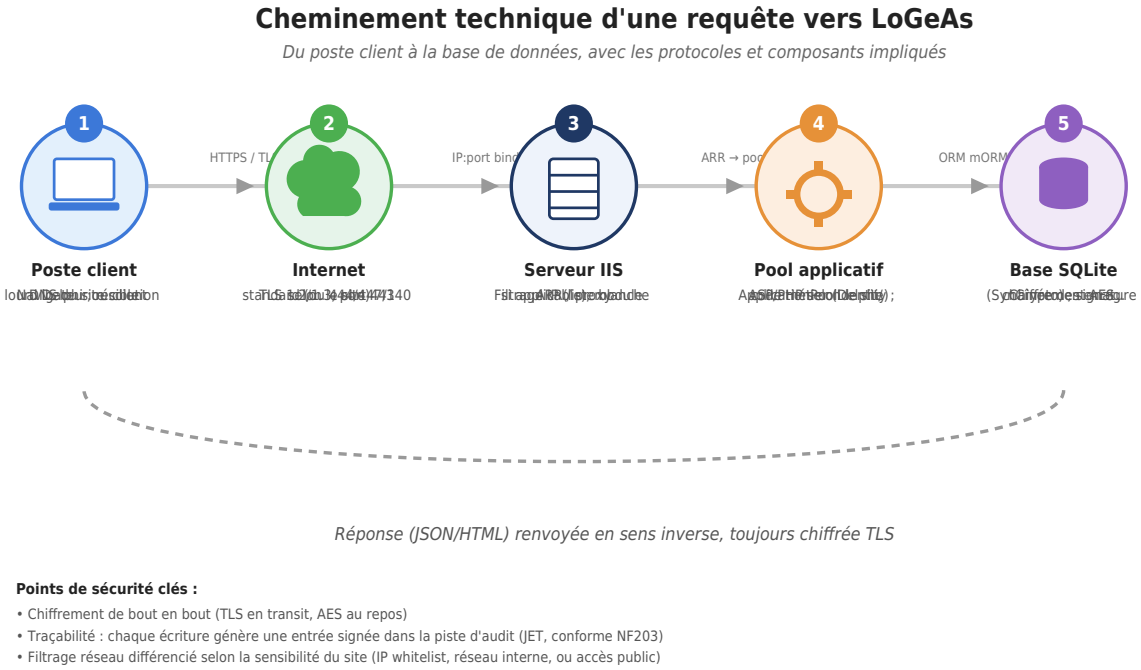
Site	Adresse IP	Port	Accès	Rôle
logeas-web.fr (+ www, test-site)	185.61.118.199	443	Ouvert	Site vitrine
nono.logeas-web.fr	185.61.118.199	444	Ouvert	Fonctions secondaires (tickets, aide, états)
serveur.logeas-web.fr	185.61.118.199	447	Ouvert	Redirection historique (héritage “app.logeas.fr”)
statunion.logeas-web.fr	185.61.118.199	443	Ouvert	Stat-Union (EPUdF)
cartographie-fonctionnelle.logeas-web.fr	185.61.118.199	443	Ouvert	Cartographie fonctionnelle
statistiques.logeas-web.fr	185.61.118.199	443	Ouvert	Statistiques
assistance.logeas-web.fr	192.168.88.100	443	Réseau interne uniquement	Assistance
wiki-intranet.logeas-web.fr	192.168.88.100	443	Réseau interne uniquement	Wiki intranet
exemples.logeas-web.fr	192.168.88.100	443	Réseau interne uniquement	Exemples
test.logeas-web.fr	185.61.118.199	443	Restreint (1 IP en liste blanche)	Environnement de test

Site	Adresse IP	Port	Accès	Rôle
Test-Biodiversité	185.61.118.199	80	Ouvert, **non chiffré (HTTP)**	Domaine tiers (les-vergers-retrouves-du-comminges.org)
questionnaire.logeas-web.fr	185.61.118.199	443	Ouvert	Questionnaire
maj.logeas.fr	185.61.118.199	443	Ouvert	Portail de mise à jour
maj.logeas-web.fr	185.61.118.199	443	Ouvert	Portail de mise à jour
interface.logeas-web.fr	185.61.118.199	443	Ouvert	Interface
taches.logeas-web.fr	185.61.118.199	443	Ouvert	Tâches
ia1-interface.logeas-web.fr	185.61.118.199	443	Ouvert	IA1 - interface
ia1-serveur.logeas-web.fr	185.61.118.199	443	Ouvert	IA1 - serveur
formulaire.logeas-web.fr	185.61.118.199	140	Ouvert	Formulaire

Schéma des sites hébergés



NB : SVG stocké sur le wiki, éditable par exemple avec Inkscape.



NB : SVG stocké sur le wiki, éditable par exemple avec Inkscape.

Architecture technique des postes clients

L'accès à LoGeAs depuis un poste client se fait selon deux modes complémentaires, décrits dans le Dossier de Conception Générale (DCG) :

- le **client lourd**, exécutable Delphi installé (ou exécuté directement) sur le poste, qui offre l'ensemble des fonctionnalités (fichier et comptabilité) ;
- la **version full-web**, accessible depuis un simple navigateur, qui permet de consulter et modifier le fichier, sans accès à la comptabilité ni aux états à ce jour (en constante évolution).

Cette distinction a une incidence directe sur l'architecture technique : le client lourd communique avec les serveurs applicatifs (app.logeas.fr / app.logeas.ovh) via l'ORM **mORMot**, en REST/JSON au travers d'une connexion HTTPS ; la version full-web utilise une connexion HTTP classique de navigateur à serveur.

Déploiement, portabilité et mise à jour

Pour répondre au mieux aux contraintes des installations sur les postes professionnels et sur les systèmes non gérés par LoGeAs, la version installée est livrée sous la forme d'un simple fichier exécutable (compressé ou non). Les fichiers secondaires utilisés pour le paramétrage (notamment les états) sont stockés en base de données et téléchargés à la demande, ce qui permet de les faire évoluer sans nécessiter de nouvelle version.

Il est ainsi possible de mettre l'exécutable de LoGeAs sur une clef USB 3 et de le transporter d'un ordinateur à l'autre : aucune donnée comptable n'est stockée localement, l'ensemble résidant sur les serveurs applicatifs.

La détection et la distribution des mises à jour du logiciel sont assurées par le portail dédié **maj.logeas.fr** (cf. section “Architecture technique des serveurs applicatifs”).

Utilisateur avancé

Lors du lancement, à côté de l'exécutable LoGeAs, est créé un dossier « LoGeAsUserData » dans lequel sont stockés :

- les informations de connexion (qui peuvent être régénérées facilement si besoin) ;
- des dossiers temporaires à LoGeAs, vidés régulièrement automatiquement ;
- les états « personnalisés » que vous ne partagez pas avec vos collègues (il est alors de votre responsabilité d'en faire des sauvegardes) ;
- des sauvegardes des états modifiés.

Ce dossier ne contient aucune donnée comptable ou métier : en cas de perte ou de vol du poste (ou de la clef USB), seuls les identifiants de connexion et les états personnalisés sont exposés — les premiers étant régénérables, les seconds relevant de la responsabilité de l'utilisateur.

Compatibilité et prérequis

Systèmes d'exploitation — le client lourd est développé et testé sur Windows 10 et Windows 11 (hors éditions "S", qui interdisent l'installation de logiciels tiers). La compatibilité avec Windows 8/8.1 n'est plus testée depuis la V8 mais reste visée dans la mesure du possible. Mac et Linux ne sont pas supportés nativement : leur usage n'est possible que via un émulateur (CrossOver, Parallels pour Mac ; Wine, PlayOnLinux pour Linux), non testé officiellement par nos équipes. La version full-web reste l'alternative recommandée sur ces systèmes, puisqu'elle ne dépend que d'un navigateur standard.

Réseau — un débit minimum de 2 Mbit/s et une latence inférieure à 40 ms sont requis pour un fonctionnement correct. Le port **8086** doit être ouvert ; les ports 8080 et 9000 peuvent être nécessaires en complément selon la configuration réseau du poste.

Machine — processeur x86/amd64, moins de 200 Mo d'espace disque requis, résolution minimale 1280×1024, mémoire 4 Go minimum (8 Go recommandés sous Windows 10 et supérieur).

Sauvegarde — bien qu'aucune donnée métier ne soit stockée localement, une sauvegarde du poste reste recommandée, de préférence externe au PC et aux locaux.

Architecture de supervision

Nous aborderons ici le thème de la supervision et son intégration dans le processus de gestion des incidents au sens ITIL du terme. Commençons tout d'abord par rappeler ce qu'est un incident dans un contexte ITIL. Un incident est une interruption inattendue d'un service. Il perturbe les opérations normales et affecte donc la productivité de l'utilisateur final. Un incident peut être provoqué par le mauvais fonctionnement d'un actif ou par une panne de réseau, en exemple : l'indisponibilité d'une imprimante.

Le lien entre la supervision et la gestion des incidents s'appuie particulièrement sur deux points :

- La génération automatique d'incident pour les alertes critiques fonctionnelles remontées par l'outil de supervision.
- La liaison directe avec la base de connaissance de la gestion des incidents.

Ainsi, la supervision permet de :

- Prévenir certains incidents par des systèmes de suivi d'indicateurs clefs et des alertes préventives adaptées.
- Ordonnancer les incidents selon une classification adaptée aux services ou aux besoins de l'entreprise.
- Optimiser la détection des incidents par un système d'alertes optimisées.
- Optimiser la résolution des incidents par la mise en place de procédure optimisées et en amélioration continue (mise à jour régulière de la base de connaissance afin de la faire correspondre aux nouvelles problématiques rencontrées).

Les bilans fournis par un outil de supervision sur l'état et la disponibilité des services permettent également de valider ou d'invalider une CNS (Contrats de Niveau de Service) ou SLA pour reprendre un terme ITIL (Service Level Agreement).

Le choix de l'entreprise s'est finalement porté sur Zabbix. En effet, outre la possibilité d'intégrer Zabbix à notre logiciel de support de façon simple, il s'avère que Zabbix dispose d'un template permettant de superviser les sauvegardes gérées par le logiciel Ipérius Backup, nous offrant ainsi la possibilité de nous alerter par sms, et de créer un ticket de support sur OTRS lorsqu'une sauvegarde est en statut d'échec ou terminée avec des erreurs, en sus des courriels. De plus, la possibilité de créer et de customiser simplement les déclencheurs et donc d'affiner la supervision des services déterminés comme étant critique est un réel avantage.

Robustesse

Dans le cadre de la certification NF552 un audit de robustesse à été réalisé sur le progiciel en octobre 2021. On trouvera les grandes lignes et les points d'évolution ainsi que les actions mené à la page Constat de l'audit de robustesse 2021

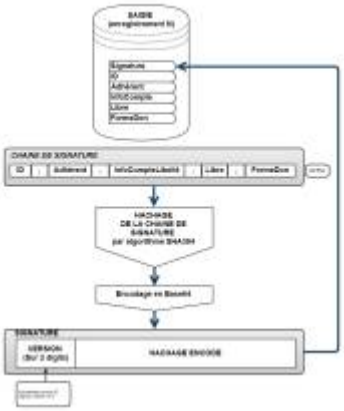
Signature des fichiers

On trouvera sur le page Partie cryptologie de LoGeAs (chaine aléatoire, cryptage, signature...) l'ensemble des informations liées à la signature des fichiers dans LoGeAs (FEC, Sauvegarde, Archive fiscale)

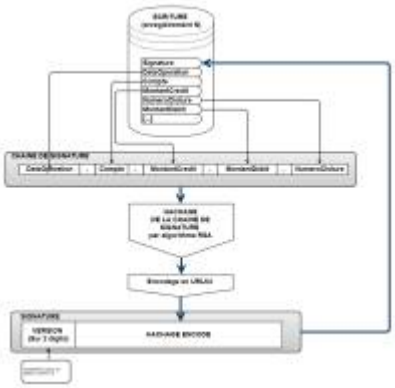
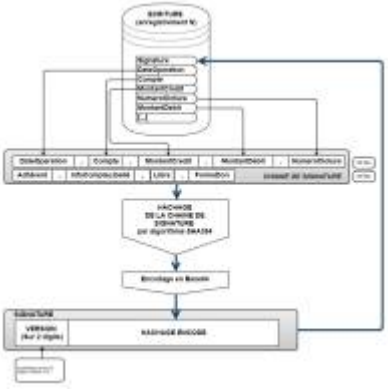
Signature des enregistrements dans la base

On pourra ce reporter à la page Partie cryptologie de LoGeAs (chaine aléatoire, cryptage, signature...) pour avoir des informations sur la technique utilisée par LoGeAs pour signer les fichiers et les enregistrements

Signature des enregistrements de la table "Saisie"

N°	Version initiale du logiciel	Schéma explicatif	Commentaires
01	A partir de la version 10.0		

Signature des enregistrements de la table "Ecriture"

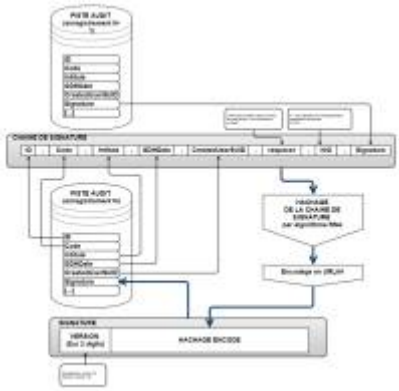
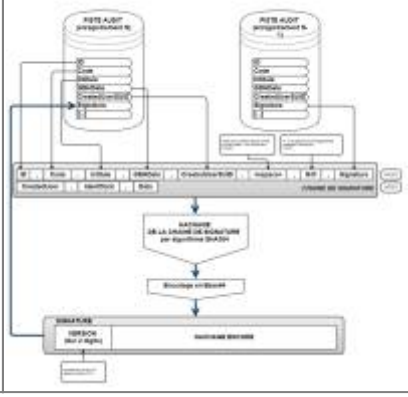
N°	Version initiale du logiciel	Schéma explicatif	Commentaires
01	Non référencé (buggée)		
02	A partir de la version 9.5		Mise en place de la nouvelle marques NF203
03	A partir de la version 10.0		Pour répondre à la marque NF552, la signature évolue avec la version 10 pour permettre la signature des champs contenant potentiellement des informations personnelles.

Signature des enregistrements de la table "PisteAudit"

Formatage de la signature

A partir de la version 9.5, la structure de la piste d'audit évolue pour se mettre en conformité avec la nouvelle version 4.0 du du R19.

N°	Version initiale du logiciel	Schéma explicatif	Commentaires
01	Non référencé (buggée)		

N°	Version initiale du logiciel	Schéma explicatif	Commentaires
02	A partir de la version 9.5		la structure de la piste d'audit évolue pour se mettre en conformité avec la nouvelle version 4.0 du du R19 La signature de chaque enregistrement est constituée avec la suite des champs : * “ID” : Identifiant de l'événement * “Code” : Code de l'événement * “Intitule” : Intitulé du code / Description de l'événement * “GDHDate” : Horodatage GDH (sous la forme AAAAMMJJHHMMSS) * “CreatedUserSUID” : Code opérateur * “Champ vide” correspondant au code de caisse (non utilisé dans LoGeAs) * “N” s'il existe une signature sur l'enregistrement précédent “O” sinon * “Signature de l'enregistrement précédent”
03	A partir de la version 10.0		

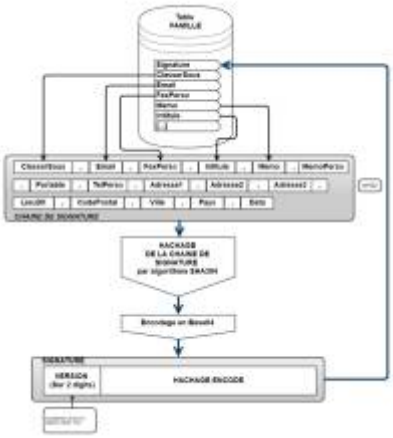
Correspondance des champs entre les labels FIDELE et le format historique de LoGeAs

Champ	Label FIDELE	Champ LoGeAs	Ajout 9.5
Identifiant de l'événement	JET-NID	ID	
Code de l'événement	JET-EVT-NUM	Code	
Intitulé du code / Description de l'événement	JET-EVT-LIB	Intitule	
Code opérateur	JET-OPE-NID	CreatedUserSUID	X
Horodatage GDH	JET-GDH	GDHDate	X
Information complémentaire contextuelle à l'événement	JET-INF	Data	
Signature Electronique	JET-TAG-SIG	Signature	X
Type d'action enregistrée sur la piste d'audit		Action	
Identifiant du lot de données pour la piste d'audit		Batchid	
Date de création de l'enregistrement pour la piste d'audit		CreatedDate	
Code opérateur sous forme de son adresse courriel		CreatedUser	
Description de l'enregistrement pour la piste d'audit		Description	
Exercice de référence de l'enregistrement		Exercice	
Indique la table et l'enregistrement concernés		Identifiant	

Champ	Label FIDELE	Champ LoGeAs	Ajout 9.5
Blocage de l'information par exemple suite à une demande RGPD (à venir)		IsDataConsultable	
Interne à mORMot		Version	

Bien que complétée par un texte en clair, chaque ligne d'entrée dans ce journal (JET) est taguée, conformément à la NF203, par un code dont vous trouverez la signification ci-dessus.

Signature des enregistrements de la table "Famille"

N°	Version initiale du logiciel	Schéma explicatif	Commentaires
01	A partir de la version 10.0		

Signature des enregistrements de la table "Personne"

N°	Version initiale du logiciel	Schéma explicatif	Commentaires
01	A partir de la version 10.0