Caisse.Enregistreuse

Dossier de Maintenance

Dossier de Maintenance

1. Gestion des versions

La gestion du code source de caisse.enregistreuse.fr est assurée via un dépôt SVN privé (svn://…/wwwCaisseEnregistreuse).

- **Versions majeures** : Tout changement impactant le périmètre fiscal génère une version majeure (exemple : passage de 1.x à 2.x).
- **Versions mineures** : Évolutions fonctionnelles n'impactant pas la conformité fiscale (exemple : passage de 1.0.1 à 1.0.2).
- **Révision** : Corrections de bugs
- **Politique de déploiement** : Mise à jour contrôlée et validation interne obligatoire avant toute mise en production.

2. Suivi des vulnérabilités

- **Veille sécurité** : Surveillance continue des vulnérabilités PHP, MySQL et Linux.
- **Correction** : Déploiement des correctifs critiques.
- **Gestion d'incidents** : Procédure de traitement et d'escalade.

3. Mise à jour du système

- **Méthode** : Mise à jour par déploiement contrôlé via SSH sécurisé.
- **Traçabilité** : Chaque mise à jour est enregistrée (numéro de version, description des changements, date de déploiement).
- **Information client** : Notification aux clients de la disponibilité de nouvelles versions majeures.

4. Système de management de la conformité

L'organisme met en place un système de management de la conformité (SMC).

Le responsable du SMC devra être désigné dans ce présent document et mise à jour en cas de modification.

Le SMC sera responsable du contrôle des exigences applicables au système d'encaissement.

Lorsqu'une nouvelle version de l'application est poussée sur le serveur SVN de gestion de fichiers, une procédure supplémentaire devra être appliquée dans l'hypothèse ou la révision contient des modifications qui portent sur des fichiers qui appartiennent au périmètre

fiscal. Dans un tel cas, le SMC (système de management de la conformité) devra effectuer un audit interne des modifications apportées à ces fichiers afin de s'assurer que celles-ci n'auront pas d'impact négatif sur la conformité du système d'encaissement. Les contrôles devront s'appuyer directement sur le référentiel de certification des systèmes d'encaissement mis à disposition par l'organisme de certification.

Cet audit interne donnera lieu à l'émission d'un rapport qui sera inclus dans le dossier de maintenance.

En cas de non conformité l'analyse de la cause et les actions prises afin de corriger la non-conformité seront enregistrées dans le document de maintenance, et la mise à jour ne sera déployée qu'après l'application d'un correctif, et un nouveau cycle de mise à jour avec audit interne.

Ces contrôles pourront s'appuyer sur des politiques, procédures ou processus documentés mais également des approbations ou revues de code, des plans et rapport de test.

Durant le contrôle, il sera nécessaire de vérifier la signature cryptographique du périmètre fiscal, la conformité des signatures numériques attachées aux transactions.

Responsable SMC : Simon Cabotse

5. Conception et développement du système d'encaissement

Conception est le développement de nouvelles versions pour le système d'encaissement suit un processus strict systématique :

- évaluation des besoins, estimation de l'impact technique des nouvelles évolutions fonctionnelles, basé sur une liste de recommandations ou de suggestions provenant soit des utilisateurs finaux, soit de l'équipe interne.

- à partir de cette évaluation des besoins sélection des évolutions fonctionnelles les plus pertinentes pour le logiciel

- pour chaque évolution fonctionnelle une nouvelle étude plus détaillée sera effectuée sur l'impact de la modification sur la conformité du système d'encaissement

- Si l'évolution présente un impact sur la conformité, l'évolution fonctionnelle du système d'encaissement devra être validé par le SMC en interne

- Une fois les évolutions fonctionnelles sélectionnées, analyser, éventuellement valider par le SMC, l'équipe chargée du développement pourra procéder à la réalisation sur sa propre branche du code source.

- Si des fichiers appartenant au périmètre fiscal sont modifiés ou que le périmètre fiscal est modifié, la documentation réglementaire devra être mise à jour, et incluse dans le Commit sur la branche principale

- Tout commit ou push ou merge sur la branche principale SVN devra donner lieu à l'établissement d'un contrôle de conformité de mise à jour si des fichiers concernés appartiennent au périmètre fiscal où que le périmètre fiscal est modifié (cf châpitre “Contrôles de conformité”).

- Une fois des évolutions fonctionnelles envoyées sur le serveur SVN, sur la branche principale, le code source pourra être déployé sur des serveurs de test. Ceci permettra de procéder au processus de test de ces nouvelles évolutions sur un environnement isolé factice et accessible uniquement en interne.

- Une fois la phase de test réalisée avec succès, la procédure de déploiement sur les serveurs de production pourra débuter. Celle-ci consiste en l'exécution d'un script permettant le déploiement simultané du code source sur tous les serveurs. Dès l'exécution du script terminée, la liste des évolutions fonctionnelles sera publiée sur la page d'accueil de l'application dans un encart intitulé “News” (changelog + actualités), permettant d’informer les utilisateurs des modifications apportées.

6. Gestion documentaire

Toutes les modifications sont documentées et intégrées aux dossiers techniques existants.

7. Périmètre du code source

L'entreprise effectue la tenue d'une liste mise à jour des fichiers ayant un impact sur la certification ou les fonctionnalités liées ou impactées par la certification.

Fichier “includes/coreCert.php”

Contient le numéro de version majeur et mineur, toutes les fonctions liées aux signatures : Fonction de création du sceau cryptographique ; Fonction de validation d’une commande ; Fonction de génération de la clé cryptographique associée à la boutique

Fichier “includes/article_add_check.php”

Contient les fonctions de vérification des conditions de création d’une nouvelle commande, édition de commande

Fichier “includes/shouldStartNewOrder.php”

Contient les fonctions de vérification des conditions de modification d’une commande

Fichier “includes/textes.php”

Contient les informations de révision

Fichier “includes/perfStat.php”

Contient les fonctions d’accès aux données

Les fichiers sont stockés dans un logiciel de gestion de versions de fichier (SVN).

L'historique des modifications apportées à ces fichiers y est clairement consultable, avec les dates de ces modifications, et les commentaires associés décrivant la modification apportée.

L'intégralité du code source étant d'ailleurs disponible par ce biais.

8. Maîtrise des sous traitants

Afin de limiter les risques sur la conformité du système d'encaissement, la sous-traitance des activités de conception, développement, test, intégration, fabrication, support ne seront pas possibles et seront uniquement effectuées en interne.

Liste des sous-traitants

Les seules activités dans la sous-traitance pourra être confiée à une entreprise tierce sera :

- la création de certificats de sécurité SSL sécurisé par des tiers

Les certificats de sécurité sont gérés par GoDaddy

- la mise en place est là maintenant d'infrastructure d'hébergement sécurisé (Cloud)

L'hébergement est réalisé par OVH, Digital Ocean

- la fabrication de matériel de caisse

Matériel de caisse fabriqué par Starmicronics, Sunmi, Pax, SumUp

- impression et expédition postale de factures

Réalisé par Esker

Sous traitance critique

La seule sous-traitance pouvant être considérée comme critique étant l'hébergement sécurisé. Il sera donc indispensable de s'assurer que chaque élément de matériel sur lequel le code source sera déployé soit bien un environnement contrôlé uniquement par l'équipe interne au système d'encaissement, et qu'aucun accès administrateur ne pourra être confié à aucune personne externe au système d'encaissement.

La personne responsable de la conservation et de la sécurisation des clés SSH permettant l'accès au serveur de production et au serveur de test devra être une seule et unique personne, interne à la société. Celle-ci devra être désignée dans le présent document et mise à jour en cas de modification.

Responsable de la conservation et de la sécurisation des clés d'accès : Simon Cabotse

9. Communication avec les clients

Le système prévoit la transmission à tous les clients chez qui le système d'encaissement est installé de tous les documents nécessaires au bon fonctionnement de celui-ci, des procédures de support et de formation, les engagements de responsabilité vis-à-vis de la loi des finances pour 2016, une description du moyen d'accès aux données d'encaissement par l'administration fiscale ainsi que d'un manuel utilisateur à destination de l'administration fiscale décrivant le moyen d'accès aux données d'encaissement, une description du format présenté, et la manière de procéder à la vérification d'intégrité des données.

Les documents précités seront disponibles pour les équipes internes et pour les utilisateurs pendant 3 ans après la date de fin de distribution de chaque version majeure du système d'encaissement.

10. Évaluation et amélioration des performances du SMC

L'organisme met en œuvre une surveillance du SMC, qui consiste en la collecte et l'analyse d'information dans le but d'évaluer et améliorer l'efficacité du SMC.

Cette surveillance comprend l'évaluation de l'efficacité :

- des contrôles définis par exemple par l'analyse des résultats de test par échantillonnage
- du traitement des non-conformités précédemment identifiés
- des actions mises en œuvre pour réduire les risques liés à la conformité des systèmes d'encaissement distribués
- des prestataires externes

L'organisme tire ainsi parti de la surveillance du système de SMC afin de déterminer, mettre en œuvre et enregistrer toute action jugée pertinente permettant l'amélioration du SMC et la réduction des risques de non-conformité.

11. Traitement des anomalies

Il ne peut exister aucune dérogation aux exigences du référentiel de certification des systèmes d'encaissement. L'organisme doit s'assurer que le système d'encaissement est bien conforme afin d'éviter la distribution et l'utilisation de système non conforme. En cas de détection d'anomalie au moment des contrôles, l'organisme doit réagir de la manière suivante : analyser l'anomalie en identifiant ses causes, mettre en œuvre des actions permettant de corriger l'analyse ou d'empêcher l'utilisation du système concerné évaluer l'efficacité des actions mises en œuvre, mettre à jour les risques identifiés, mettre à jour le SMC si nécessaire.

L'organisme enregistre les informations concernant la nature de l'anomalie, son analyse et les actions mises en œuvre avec leurs résultats dans le document si présent.

12. Historique des irrégularités corrigés dans le logiciel, identifiées par le SMC

12 avril 2025

Il a été identifié une irrégularité dans la génération des rapports qui permettait de générer des rapports portant sur une plage de date supérieure à un an. Un patch correctif a été appliqué au logiciel et celui-ci ne permet désormais plus de télécharger des rapports sur une plage de date supérieure à un an.

12 avril 2025

Il a été identifié une irrégularité dans la traçabilité des opérations concernant les opérations d'archivage. Le système de caisse enregistrait bien les documents d'archive générés en base de données mais il n'enregistrait pas l'identifiant de l'utilisateur ayant effectué la génération de l'archive (enregistrait l'identifiant de boutique). Le logiciel a été mis à jour et l'identifiant de l'utilisateur est désormais également enregistré dans la base de données, dans une table dédiés aux trace des opérations, pour permettre une traçabilité plus précise des opérations d'archivage

---

13. Conformité au Référentiel de Certification

Politique de versionnage (Exigence IV.10 - Exigence 21)
La gestion des versions majeures et mineures est rigoureuse et traçable via SVN.

Gestion des mises à jour (Exigence III.6)
Chaque modification du code est vérifiée pour garantir la conformité continue avant déploiement.

Traçabilité des évolutions (Exigence III.13)
Chaque évolution est documentée, archivée et accessible pour consultation.

Surveillance des vulnérabilités (Exigence III.4)
Un processus de veille de sécurité garantissant la correction rapide des failles détectées.