



Certification LNE

RÉFÉRENTIEL DE CERTIFICATION DES SYSTÈMES D'ENCAISSEMENT

- Référence de document : **Encaissement LNE**
- Réf. rédacteur : **BYCYB/CERTIFICATION/NK**
- 1^{ère} mise en application : **01/01/2018**
- Révision n° 1.8 – **14 octobre 2025 corrigée le 11 décembre 2025**
- Approbation LNE le **12/12/2025**

RÉVISIONS DU DOCUMENT

Version	Date	Raison de modification
1	29/11/2016	Version initiale
1.1	07/12/2016	<ul style="list-style-type: none"> Précisions apportées aux chapitres I.3/ domaine d'application (exclusion de la monétique) et V.4 / comité de marque (suppression du président et ajout de l'impossibilité de droit de veto conformément à la norme NF X50-067) suite au 1^{er} comité de marque du 06/12/2016.
1.2	12/12/2016	<ul style="list-style-type: none"> Ajustement de la composition du comité de marque (V.4). Ajustement de la procédure de recours et de plainte (VI).
1.3	PROJET	<p>Ensemble du document : Prise en compte de la FAQ de la DGFIP sur les logiciels de caisse sécurisés datée du 28/07/2017</p> <p>§ I.3 : précisions apportées au domaine d'application du référentiel</p> <p>§II.2 : prise en compte du retour d'expérience pour la rédaction des conditions</p> <p>§ III : précisions apportées sur la marque LNE Système de caisse et sur les engagements des titulaires de certifications</p> <p>§ IV : précisions apportées sur les modalités d'évaluation initiale et de surveillance.</p> <p>Glossaire : ajout de définitions</p>
1.4	24/01/2019	<ul style="list-style-type: none"> Prise en compte des changements de la version mise à jour du 04/07/2018 du BOI-TVA-DECLA-30-10-30 <p>Inclusion des précisions issues de la FAQ du 28 juillet 2017</p> <p>Utilisation d'un format d'archives ouvert</p> <p>Obligation de proposer 3 niveaux de clôture</p> <p>Redéfinition du système d'encaissement</p> <p>Précisions sur les données concernées</p> <p>Obligation de tracer les opérations du purge/archivage</p> <ul style="list-style-type: none"> Réorganisation des différentes parties du référentiel Clarification sur la différence certification/attestation Précisions sur le processus de certification Refonte des exigences qualité Réorganisation des exigences techniques

		<ul style="list-style-type: none"> • Ajout de l'identifiant de l'établissement dans les données concernées • Ajout de la sécurisation des justificatifs • Mise à jour des exemples de solutions acceptables dans les mécanismes garantissant l'inaltérabilité des données
1.5	PROJET	<ul style="list-style-type: none"> • Correction de coquilles • Clarifications vocabulaire évaluation / audit • Ajout des critères de classification des NC majeures/mineures pour le SMC • Ajout des cas de résiliation, suspension et retrait de certificat dans le processus de suivi des certificats • Mise en cohérence des activités liées au système d'encaissement (chap III) • Remise en forme des données à enregistrer listées à l'exigence n°3 et suppression dans la liste des données à enregistrer de « Toute donnée permettant la production de justificatifs (définitifs ou provisoires) » • Précision tirée du BOI ajoutée dans le corps de l'exigence 18 • Précisions sur les notes spécifiques des exigences 3, 13, 21 • Précisions sur les vérifications des exigences 1, 2, 7, 8, 12, 15 • Contenus déplacés entre le corps de l'exigence et la note spécifique : exigences 6, 7, 8 • Mise en cohérence de toutes les mentions aux données d'encaissement définies dans les différentes exigences du référentiel • Suppression de la notion d'environnement de recette/pre-prod et autres dans l'exigence n°5 sur le mode école
1.6	16/06/2021	<ul style="list-style-type: none"> • Remplacement des références au BOI-TVA-DECLA-30-10-30- 20180704 par BOI-TVA-DECLA-30-10-30-20210519 • Ajout note de bas de page pour « logiciel de facturation » dans la section domaine d'application • Prise en compte des certifications ISO 9001 dans la durée d'audit organisationnel • Prise en compte des changements de la version mise à jour du 19/05/2021 du BOI-TVA-DECLA-30-10-30

		<ul style="list-style-type: none"> • Exigence 3 : Ajout d'une indication sur la non-obligation des logiciels de facturation d'enregistrer l'identifiant du TPV • Exigence 6 : Ajout d'une indication sur la non-obligation des logiciels de facturation de réaliser les 3 clôtures sous réserve de la fourniture du total du chiffre d'affaires enregistré pour une période déterminée • Exigence 8 : Précision ajoutée dans la section « Exemples de solutions acceptables » • Exigence 11 : Ajout de la précision sur le fait que les archives doivent être réalisables sur toute période inférieure à 7 ans + ajout d'un exemple de solution acceptable • Exigence 12 : Ajout de la notion de serveur distant dans les exemples de solutions acceptables • Exigence 13 : Ajout d'une précision indiquant que les données cumulatives et récapitulatives ne doivent jamais être purgées • Exigence 18 : Exclusion de la notion de traçabilité dans l'exigence et dans les vérifications documentaires et fonctionnelle • Exigence 20 : Précision ajouté dans « Notes spécifiques » et « Exemples de solutions acceptables » • Exigence 21 : ajout d'un exemple de solution acceptable • Chapitre III.2 : suppression du chapitre sur les engagements de l'éditeur + renumérotation des chapitres • Chapitre 5 SMC : Renommage du titre du chapitre en "Veille juridique et réglementaire" • Chapitre 5 SMC : Suppression de la mention : être destinataire des bulletins d'information du LNE • Chapitre 8 SMC : Suppression de l'engagement des sous-traitants à respecter le présent référentiel • Chapitre 8 SMC : Réorganisation du chapitre (dernier paragraphe déplacé en premier • Ajout définition logiciel de facturation dans la section « lexique » • Précision exigence n°7 pour le cas d'un système d'encaissement utilisé par plusieurs assujettis • Modification de l'exigence n°3 concernant le moment à partir duquel les données de transaction doivent être
--	--	---

		<p>enregistrées</p> <ul style="list-style-type: none"> • Modification de l'exigence n°6 concernant les cas d'exercices fiscaux décalés • Assouplissement de l'exigence n°18 sur la déconnexion des terminaux • Intégration de la nouvelle marque de certification • Page 66 : suppression du tableau de correspondance • Mise en page
1.7	30/05/2024	<ul style="list-style-type: none"> • Ajout des modalités de certification des produits certifiés hors LNE. • Chapitre III.2 : ajout de l'identification de la responsabilité relative à la veille réglementaire. • Chapitre III.8 : ajout de la vérification de la disponibilité de la dernière version majeure certifiée. • Chapitre III.8 : ajout de la vérification de la communication de l'éditeur avec les clients finaux de la disponibilité de la dernière version majeure certifiée dans le cas de la non mise à jour automatique des systèmes chez les clients finaux • Chapitre III.8 : ajout d'un exemple de solution acceptable avec la possibilité d'utiliser un système de licences pour vérifier le parc de systèmes d'encaissements chez les utilisateurs finaux. • Exigence 3 : ajout de l'identification et l'inaltérabilité des champs et de leurs valeurs lorsque la conformité à la réglementation française est paramétrable (documentaire et fonctionnel). • Exigence 8 : ajout d'une meilleure formalisation des gestions des clés. • Exigence 9 : ajout de la gestion et l'identification des mode hors- ligne en base de données. • Exigence 9 : ajout de solution acceptable pour l'identification de l'utilisation du mode hors-ligne ainsi que sa durée maximale. • Exigence 9 : ajout de l'identification des justificatifs au format dématérialisé. • Exigence 9 : ajout des vérifications effectuées sur le ticket.

		<ul style="list-style-type: none"> Exigence 10 : remonté de la note 36 dans le corps de l'exigence. Exigence 18 : ajout de l'identification et la justification d'un délai maximum pour l'utilisation du mode hors-ligne. Exigence 18 : ajout de la vérification documentaire de l'enregistrement du délai maximum pour le mode hors-ligne. Exigence 18 : ajout de la vérification de la durée et des causes des déconnexion et mode hors-ligne. Exigence 18 : ajout de la vérification de l'identification des opérations réalisées en mode hors-ligne. Exigence 19 : ajout de la vérification documentaire des champs, leurs valeurs et l'intégrité des paramétrages pour que le système soit conforme à la réglementation française. Exigence 19 : ajout de la vérification de l'intégration et la sécurisation des paramétrages du mode hors-ligne. Exigence 19 : Vérifier le nombre de licences identifiées pour les clients finaux dans le cas d'utilisation de licence. Exigence 19 : Vérifier que les paramètres (champs et valeurs) de conformité française sont joints aux exports à destination de l'administration fiscale. Modification des modalités de fonctionnement du comité de marque. <p><u>Contexte de l'évolution 1.7 :</u></p> <p>La mise à jour du référentiel LNE ver 1.7 répond aux objectifs suivants :</p> <ul style="list-style-type: none"> - Améliorer la robustesse dans le contexte de nouveaux types de fraude comme la fraude à la caisse fantôme. <ul style="list-style-type: none"> Paramétrage de la conformité à la réglementation française. Modalités relatives au mode hors ligne. - Préciser les modalités de certification des produits certifiés hors LNE - Précisions diverses en particulier concernant : <ul style="list-style-type: none"> Traçabilité de la distribution des versions certifiées. Gestion des clés. Justificatifs en format dématérialisé.
--	--	--

		<p>Information dans le ticket</p> <p>- Corrections éditoriales.</p> <p><u>Modalités de transition pour le référentiel en version 1.7 :</u></p> <p>Le référentiel en version 1.7 entre en application à la date de sa publication. Le référentiel en version 1.7 a une période de transition qui prend fin au 30/09/2025. A partir du 30 septembre 2024, tous les audits seront réalisés selon la version 1.7. Tout écart relatif à ces exigences mises à jour devra faire l'objet d'une mise en conformité constatée avant le 30 septembre 2025 au plus tard. Tous les certificats devront avoir été passé en version 1.7 au 1er octobre 2025.</p> <p>A cette date, tous les certificats en version 1.6 seront retirés.</p> <p>Note : d'ici au 30 septembre 2024, les nouvelles exigences pourront être revues lors de l'audit. Tout écart constaté fera l'objet d'un point d'attention dans le rapport. Il n'y aura pas de non-conformités concernant les nouvelles exigences durant cette période.</p>
1.8	01/08/2025	<p>Evolutions de la version 1.8</p> <ul style="list-style-type: none"> • Prendre en compte la mise à jour du BOI-TVA-DECLA-30-10-30-20250416 et la fin de l'auto-attestation • Prendre en compte les rôles et responsabilités du LNE et de BYCYB dans la certification des systèmes de caisse • Clarifier la formulation de certaines mentions sur les tickets de caisse

TABLE DES MATIÈRES

RÉVISIONS DU DOCUMENT	2
CHAPITRE I : GÉNÉRALITÉS	11
I.1) Objet & assujettis à la TVA concernés.....	11
I.2) Domaine d'application : définition du système d'encaissement.....	12
CHAPITRE II : PROCESSUS D'ATTRIBUTION ET DE SUIVI DES CERTIFICATS.....	13
II.1) Processus de commande.....	13
II.2) Processus de certification	13
II.2.1) Examen de recevabilité documentaire	13
II.2.2) Planification de l'évaluation initiale	14
II.2.3) Réalisation de l'évaluation initiale	14
II.2.3.1) Audit organisationnel.....	15
II.2.3.2) Evaluation de la robustesse.....	15
II.2.3.3) Evaluation documentaire.....	15
II.2.3.4) Evaluation fonctionnelle	16
II.2.4) Réponse aux fiches de non-conformité.....	16
II.2.5) Avis du Responsable d'évaluation et revue du rapport.....	17
II.2.6) Décision du comité de lecture.....	17
II.2.7) Modalités de certification des produits certifiés hors marque LNE	18
II.3) Surveillance du certificat	18
II.4) Résiliation, suspension et retrait du certificat.....	19
CHAPITRE III : EXIGENCES APPLICABLES AU SYSTÈME DE MANAGEMENT DE LA CONFORMITÉ (SMC)	21
III.1) Contexte.....	21
III.2) Rôles et responsabilités.....	21
III.3) Objectifs et mise en œuvre du SMC.....	22

III.4) Veille juridique et réglementaire	23
III.5) Etablissement des contrôles de conformité	23
III.6) Conception et développement du système d'encaissement.....	24
III.7) Maîtrise des sous-traitants	25
III.8) Identification et traçabilité de la distribution.....	25
III.9) Communication avec les clients	26
III.10) Usage de la marque LNE – Système de caisse	27
III.11) Evaluation et amélioration des performances du SMC	27
III.12) Traitement des anomalies	28
III.13) Gestion des enregistrements.....	28
CHAPITRE IV : EXIGENCES TECHNIQUES APPLICABLES AU SYSTÈME D'ENCAISSEMENT CERTIFIÉ	30
IV.1) Documentation	30
IV.2) Enregistrement des données	33
IV.3) Clôtures.....	37
IV.4) Sécurisation & Inaltérabilité des données.....	39
IV.5) Archivage des données d'encaissement	44
IV.6) Purges	48
IV.7) Traçabilité des opérations	50
IV.8) Conservation des données.....	50
IV.9) Accès de l'administration fiscale aux données d'encaissement.....	55
IV.10) Identification du périmètre fiscal et des versions majeures et mineures	57
CHAPITRE V : ÉLABORATION ET VALIDATION DU RÉFÉRENTIEL	61
V.1) Comité de marque	61
V.1.1) Modalités, rôle, et engagements de fonctionnement	61
V.1.2) Composition du comité.....	62
V.1.3) Groupe de travail	62

V.2) Modalités d'élaboration et de validation du référentiel	62
V.3) Normes et documents de référence	63
CHAPITRE VI : RECOURS ET TRAITEMENT DES PLAINTES	64
VI.1) Recours contre décision	64
VI.2) Traitement des plaintes	64
CHAPITRE VII : ANNEXES	65
VII.1) Lexique	65

CHAPITRE I : GÉNÉRALITÉS

Introduction

Pour donner suite à l'évolution du BOI, une mise à jour du référentiel 1.7 voit le jour afin de se conformer.

Modalités d'application de la version 1.8 :

- Le référentiel en version 1.8 entre en application à la date de sa publication.
- Le référentiel en version 1.8 n'introduit aucune nouvelle exigence pour les systèmes déjà certifiés.
- L'impact concerne uniquement les certificats qui seront actualisés à la version supérieure sous un délai de 02 mois après la publication du référentiel. De ce fait il n'y a pas de période de transition.

I.1) Objet & assujettis à la TVA concernés

Afin de lutter contre la fraude à la TVA liée à l'utilisation de systèmes permettant la dissimulation de recettes, la loi de finances pour 2016 a instauré l'obligation pour tous les professionnels assujettis à la TVA, qui effectuent des livraisons de biens et des prestations de service à destination de clients particuliers, enregistrant les paiements reçus en contrepartie au moyen d'un système de caisse, que celui-ci soit sécurisé. Ce système doit ainsi être certifié par un organisme indépendant accrédité¹.

La certification est une procédure par laquelle une tierce partie, l'organisme certificateur, donne une assurance écrite qu'un système d'organisation, un processus, une personne, un produit ou un service est conforme à des exigences spécifiées dans une norme ou un référentiel. Elle est encadrée par le Code de la Consommation.

Cette obligation touche tous les secteurs d'activités, étant rappelé que la loi de finances pour 2018 a exclu du dispositif les assujettis à la TVA bénéficiant du régime de la franchise en base, ceux soumis au régime du remboursement forfaitaire de TVA agricole, ceux effectuant exclusivement des opérations exonérées de TVA² et ceux qui réalisent l'intégralité de leurs opérations entre professionnels uniquement (B to B).

Le présent référentiel décrit les modalités de certification des systèmes d'encaissement. Il s'appuie principalement sur l'article 88 de la loi n° 2015-1785 du 29 décembre 2015 de finances pour 2016 et le bulletin officiel des finances **BOI-TVA-DECLA-30-10-30-20250416**, qui définit les conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données de transaction auxquelles le système doit se satisfaire. Le

¹ **BOI-TVA-DECLA-30-10-30-20250416**

² BOI-TVA-DECLA-30-10-30-20250416: point 25.

référentiel vise à certifier ces 4 caractéristiques, la caractérisation du périmètre fiscal du système et des versions du système, la documentation afférente au système, et l'organisation (SMC³) mise en place pour assurer la production et la livraison de systèmes d'encaissement conformes à la version certifiée.

I.2) Domaine d'application : définition du système d'encaissement

Un système d'encaissement est un système informatique (quelle que soit sa qualification : gestion, CRM, comptabilité, de caisse, de facturation⁴, etc.) doté d'une fonctionnalité de caisse.

Une fonctionnalité de caisse consiste à mémoriser et à enregistrer extra-comptablement des paiements reçus en contrepartie d'une vente de biens ou de prestations de services, et ce quel que soit le moyen de paiement. On entend par enregistrer extra-comptablement que le paiement enregistré par le système **ne génère pas simultanément, automatiquement, obligatoirement et sans intervention humaine** une écriture comptable dans le système de comptabilité⁵.

Certaines exclusions spécifiques existent. Il convient de se référer au **BOI-TVA-DECLA-30-10-30-20250416**.

BYCYB n'a pas vocation à trancher sur l'applicabilité de ce BOI quant au système concerné.

³ SMC : Système de Management de la Conformité

⁴ Un logiciel de facturation, c'est-à-dire un système informatique permettant d'émettre des factures entre assujettis à la TVA, contenant les mentions obligatoires prévues à l'article 242 nonies A de l'annexe II au CGI et respectant les conditions de l'article 289 du CGI, doit être considéré comme un logiciel ou système de caisse tel que défini au I-B § 30, s'il dispose d'une fonctionnalité de caisse.

⁵ **BOI-TVA-DECLA-30-10-30-20250416**: point 30.

CHAPITRE II : PROCESSUS D'ATTRIBUTION ET DE SUIVI DES CERTIFICATS

II.1) Processus de commande

Après une première prise d'informations et d'échanges, le service commercial de **BYCYB** fait parvenir le questionnaire initial au demandeur de la certification qui doit être retourné rempli afin de pouvoir établir le devis. Le service commercial fait alors parvenir l'offre de certification au demandeur. Une fois la commande enregistrée, le processus de certification peut démarrer.

II.2) Processus de certification

Le processus de certification se découpe en plusieurs étapes successives. Les principales sont :

1. l'instruction du dossier de demande : l'examen de recevabilité documentaire ;
2. la réalisation de l'évaluation initiale :

Elle se découpe en 4 opérations d'évaluation d'une durée minimale d'un jour chacune :

- l'audit organisationnel destiné à s'assurer de la conformité du SMC mis en place aux exigences du chapitre III ;
- l'évaluation de la conformité documentaire du système aux exigences du chapitre IV ;
- l'évaluation de la conformité fonctionnelle du système aux exigences du chapitre IV ;
- l'évaluation de la conformité robustesse du système aux exigences du chapitre IV ;

3. le retour sur les fiches de non-conformité le cas échéant ;
4. la prise de décision de certification en comité de lecture ;
5. l'émission du certificat une fois la décision de certification entérinée.

II.2.1) Examen de recevabilité documentaire

Une fois la prise de commande enregistrée, **BYCYB** envoie au demandeur de la certification le formulaire de recevabilité documentaire.

Ce formulaire doit être retourné à **BYCYB**, rempli, et accompagné du dossier technique constitué de la documentation relative au système. Cette documentation doit être complète et décrire précisément l'ensemble des fonctionnalités et mécanismes mis en œuvre dans le cadre de la mise en conformité, permettant de répondre aux exigences techniques du référentiel LNE⁶.

⁶ CF : Chapitre IV : exigences techniques applicables au système d'encaissement certifié (Exigence 1 et 2)

L'examen de recevabilité documentaire n'est pas équivalent à l'évaluation documentaire effectuée lors de l'audit de certification ni même équivalent à l'audit dans son ensemble.

L'examen de recevabilité documentaire consiste à déterminer si l'évaluation de la conformité du système d'encaissement est possible compte tenu du degré d'aboutissement du dossier technique transmis par le demandeur. Pour ce faire il est constaté :

- si des documents demandés à l'exigence n° 1 du chapitre IV sont manquants ;
- si tout ou partie de la documentation réglementaire n'est pas en français ;
- si le périmètre fiscal et la gestion des numéros de version sont bien définis ;
- si le principe des méthodes proposées pour répondre aux exigences du chapitre IV est pertinent.

A l'issue de l'examen de recevabilité documentaire, **BYCYB** informe le demandeur du résultat.

Dans le cas où cette étape conclue à l'irrecevabilité du dossier, il appartient au demandeur de la certification de répondre à **BYCYB** en fournissant les documents manquants. Un devis complémentaire sera adressé par le service commercial du **BYCYB** si un second examen de recevabilité documentaire est nécessaire.

II.2.2) Planification de l'évaluation initiale

Dans le cas où l'examen de recevabilité documentaire est satisfaisant, le dossier est recevable et **BYCYB** prend contact avec le demandeur, afin de définir les lieux et dates des différentes étapes de l'évaluation.

La durée de l'audit organisationnel peut être augmentée s'il est nécessaire de se déplacer sur plusieurs sites, si des sous-traitants interviennent dans la conception, le développement, les tests, l'intégration, la fabrication, le déploiement/ la distribution, la configuration, l'installation et/ou le support du système à certifier et ne sont pas suivis par le titulaire de la certification, ou encore s'il est nécessaire de faire appel à un interprète. Elle est fixée par défaut à une journée. Elle peut être diminuée sous réserve de justifier que le demandeur de la certification dispose d'un SMQ certifié ISO 9001 pour les activités couvertes par le référentiel (conception, développement, tests, intégration, fabrication, déploiement/distribution, configuration, installation, support).

La durée des évaluations documentaire, fonctionnelle et de robustesse d'un système d'encaissement est liée à sa complexité ; elle est fixée par défaut à une journée par évaluation. Elle peut être augmentée, notamment à l'issue de l'examen de recevabilité documentaire, selon la complexité du système d'encaissement (plusieurs interfaces homme/machine, configurations et/ou flux de données à tester, architecture du système etc.).

II.2.3) Réalisation de l'évaluation initiale

Plusieurs opérations d'évaluation peuvent avoir lieu en même temps en fonction de la composition de l'équipe d'évaluation.

Il est rappelé que les opérations d'évaluation sont basées sur un échantillonnage des informations disponibles. L'absence de non-conformité constitue une présomption et non une preuve de conformité aux exigences.

II.2.3.1) *Audit organisationnel*

Le demandeur de la certification doit mettre en œuvre un Système de Management de la Conformité (SMC) destiné à s'assurer que chaque système d'encaissement, ou mise à jour, déployé répond aux exigences du chapitre IV.

Les exigences applicables à ce SMC sont définies au chapitre III et leur bonne application est vérifiée lors de l'audit organisationnel.

L'audit organisationnel du SMC a lieu chez le demandeur, de préférence sur le site où ont lieu les activités de conception, développement et tests concernant le système à certifier. Lorsqu'un titulaire souhaite certifier plusieurs systèmes d'encaissement, l'audit organisationnel, est mutualisé pour l'ensemble des systèmes **si et seulement si les documentations SMC sont communes**. Dans le cas où un demandeur ou titulaire de la certification dispose d'une certification ISO 9001 couvrant les activités et sites de conception et développement/production des systèmes d'encaissement, la durée de l'audit organisationnel pourra être réduite. Le demandeur de la certification doit s'assurer de la disponibilité d'un interlocuteur maîtrisant le SMC mis en place, l'organisation de la société et ses processus, ainsi que de toute autre personne jugée pertinente.

II.2.3.2) *Evaluation de la robustesse*

L'évaluation de la robustesse du système d'encaissement a pour objectif de vérifier le respect des exigences définies au chapitre IV du point de vue de la robustesse. Le demandeur de la certification doit s'assurer de la disponibilité d'un :

- expert technique maîtrisant la conception, le développement/fabrication (connaissant le code source), la configuration et l'utilisation du système d'encaissement à certifier ;
- système d'encaissement fonctionnel dans un environnement de test (pour pouvoir notamment modifier la date du système facilement) avec tous les périphériques associés (Imprimantes, afficheurs, télécommande...), raccordés et fonctionnels, et des éventuelles connexions ou configurations possibles (à un PC, serveur ou tout autre système centralisé) ;
- système d'encaissement dans un environnement de développement (avec accès intégral au code source, accès direct aux bases de données, serveurs etc.) ;
- accès aux documentations utilisateur et technique.

II.2.3.3) *Evaluation documentaire*

L'évaluation documentaire du système d'encaissement a pour objectif de vérifier le respect des exigences définies au chapitre IV du point de vue documentaire. Le demandeur de la certification doit s'assurer de la disponibilité de :

- un interlocuteur maîtrisant la documentation et la conception du système d'encaissement à certifier ;

- la documentation réglementaire⁷ en français ;
- la documentation complémentaire⁸ en français ou en anglais ;
- l'ensemble de la documentation à destination de l'évaluateur, ainsi que d'un moyen de transfert pertinent. Ces documents seront conservés par BYCYB comme preuves d'audit.

II.2.3.4) Évaluation fonctionnelle

L'évaluation fonctionnelle du système d'encaissement a pour objectif de vérifier le respect des exigences définies au chapitre IV du point de vue fonctionnel. Le demandeur de la certification doit s'assurer de la disponibilité d'un :

- interlocuteur maîtrisant la conception, le développement/fabrication, la configuration et l'utilisation du système d'encaissement à certifier ;
- système d'encaissement fonctionnel dans un environnement de test (pour pouvoir notamment modifier la date du système facilement) avec tous les périphériques associés (Imprimantes, afficheurs, télécommande...), raccordés et fonctionnels, et des éventuelles connexions ou configurations possibles (à un PC, serveur ou tout autre système centralisé) ;
- jeu de données d'encaissement suffisamment fourni pour pouvoir réaliser les cas de test du référentiel : clôtures périodiques (journalière, mensuelle et annuelle), synchronisation des données, archivage, etc.

Il est rappelé qu'il appartient à l'éditeur de prouver la conformité de son produit. Une absence de réponse ou une absence de démonstration permettant de prouver la conformité est enregistrée comme une non-conformité.

II.2.4) Réponse aux fiches de non-conformité

Dans le cas où une non-conformité est constatée durant une des opérations d'évaluation, une fiche décrivant la NC⁹ est rédigée par l'évaluateur¹⁰ /auditeur¹¹. Celle-ci est transmise par le RE¹² au demandeur de la certification, lors de la réunion de clôture de l'évaluation.

On distingue 2 catégories de NC :

1. NC 'système' du SMC (chapitre III)

Elles peuvent être mineures ou majeures.

Une NC majeure est bloquante pour la certification : elle devra être corrigée avant la certification.

⁷ CF : Chapitre IV exigence 1

⁸ CF : Chapitre IV exigence 2

⁹ NC : Non-conformité

¹⁰ Evalueur pour les étapes 2/3/4 : évaluations du système d'encaissement (chapitre IV)

¹¹ Auditeur pour l'étape 1 : audit organisationnel sur le système de management de la conformité (chapitre III)

¹² RE : responsable d'évaluation

Une NC mineure n'est pas bloquante pour la certification mais devra être corrigée avant le prochain audit de suivi, sous peine de suspension de certificat.

La non-conformité est classée **majeure** lorsque, sur la base d'évidences objectives :

- La non-conformité met en cause la conformité du système d'encaissement ou
- Il y a présence d'un risque important pour la capacité du SMC à maîtriser la conformité du système d'encaissement ou
- Il y a non-satisfaction systématique ou répétée d'une exigence (relative au système de caisse ou au SMC)

2. NC 'produit' du système d'encaissement (chapitre IV)

Toute NC produit est bloquante pour la certification : elle devra être corrigée avant la certification.

Si la NC est uniquement documentaire, le RE ou **BYCYB** peuvent la lever après transmission des documents appropriés.

Le demandeur de certification a alors un délai fixé avec le RE (de 3 à 5 semaines) pour lui retourner chaque fiche complétée par l'analyse de la NC et l'action engagée.

Après analyse des actions proposées par le demandeur de la certification, le RE se prononce sur sa pertinence et préconise le type de suivi nécessaire à la NC.

II.2.5) Avis du Responsable d'évaluation et revue du rapport

Après réception des éventuelles fiches de NC complétées par le demandeur de la certification et le RE, le **BYCYB** analyse le rapport d'évaluation et l'avis du responsable d'évaluation. A la lecture du rapport il peut demander des informations complémentaires au demandeur de la certification, avant le passage en comité de lecture.

II.2.6) Décision du comité de lecture

Le comité de lecture est chargé de rendre un avis sur la décision de certification dans le processus d'attribution, de surveillance, de retrait ou de suspension des certificats. Il est composé au minimum :

- d'un représentant de la direction de **BYCYB** (qui ne peut intervenir en tant que chef de projet certification et n'ayant pas participé à l'évaluation) ;
- d'un chef de projet certification n'étant pas en charge du dossier ;
- d'un chef de projet certification en charge de présenter le dossier.

Le comité est présidé par le représentant de la direction de **BYCYB** et a pour mission :

- d'examiner les rapports d'évaluation et de formuler un avis et une recommandation sur les décisions à prendre, notamment sur le type et la durée du suivi d'une NC ;
- le cas échéant, d'examiner dans un premier temps les appels contre les décisions de **BYCYB** et de formuler un avis sur les suites à donner ;
- d'évaluer la qualité des rapports d'évaluation.

La décision de certification s'appuie sur l'examen des éléments du dossier et du rapport de l'évaluation. Chaque décision de certification est matérialisée par l'enregistrement et le cas échéant l'émission d'un certificat.

Les certificats sont émis sans date limite de validité et restent valides tant qu'aucune modification portant sur les caractéristiques certifiées (périmètre fiscal) n'est apportée. Il appartient à l'entreprise de signaler à **BYCYB** les modifications afin de faire réaliser les évaluations nécessaires à la révision du certificat.

II.2.7) Modalités de certification des produits certifiés hors marque LNE

A la réception d'une demande de certification d'une société disposant déjà d'une certification selon un référentiel basé sur les exigences du BOI 30-10-30 et accrédité selon le référentiel 17065 par un organisme d'accréditation reconnu, des modalités de certification spécifiques peuvent être mise en place.

L'audit initial des entreprises déjà certifiées hors marque LNE sera allégé en les exonérant de l'étape de revue par **BYCYB** de la recevabilité documentaire. Néanmoins un document « vérification documentaire migration de certificat » devra être rempli par la société en particulier concernant la référence aux documents de conformité afin de permettre la réalisation de l'évaluation dans les durées évoquées ci-dessous. La durée de l'évaluation initiale pour les entreprises déjà certifiées hors marque LNE pourra être réduite.

Pour le reste des modalités de l'audit initial tout sera identique aux dispositions déjà établies dans le présent référentiel.

II.3) Surveillance du certificat

Il est procédé à une évaluation de surveillance annuelle. Le contenu de l'évaluation annuelle varie selon les cas ; sa durée ne peut être inférieure à une journée.

Afin de planifier cette surveillance, **BYCYB** envoie un questionnaire à l'entreprise dont le système est certifié afin de connaître les évolutions depuis l'évaluation précédente. Une fois le questionnaire retourné, **BYCYB** établit une offre de surveillance en fonction des modifications effectuées.

Les modalités d'évaluation en fonction des modifications lors du suivi sont les suivantes :

- **Si le système certifié n'a subi aucune modification :**

L'évaluation de suivi annuelle porte sur l'audit du SMC du titulaire et des vérifications destinées à s'assurer de l'absence de modification du système (comparaison de l'empreinte). Il dure 1 journée. Le but de l'évaluation est de s'assurer que le SMC est maintenu, afin de produire des systèmes d'encaissement identiques à celui certifié et que la traçabilité des systèmes distribués est assurée.

- **Si le système certifié a subi une modification de son périmètre fiscal** (et donc un changement de version majeure) :

L'évaluation de suivi annuelle est considérée par défaut comme une évaluation initiale avec examen de l'ensemble des exigences documentaires, fonctionnelles et de robustesse, listées au chapitre IV ainsi que les exigences organisationnelles liées au SMC, listées au chapitre III. Sa durée est fonction des modifications apportées au système.

Note : en cas de modification sur le périmètre fiscal, l'entreprise doit informer **BYCYB** des modifications effectuées avant de pouvoir distribuer cette version. En effet le certificat ne couvre le système que pour une version majeure donnée.

- **Si le système certifié a subi une modification mineure** (donc sans changement sur le périmètre fiscal) :

L'évaluation de suivi annuelle porte sur l'audit du SMC du titulaire et des vérifications fonctionnelles permettant de s'assurer que les versions mineures ultérieures du système d'encaissement continuent de répondre aux 4 conditions sur les données d'encaissement définies par le BOI¹³, et sur l'absence de modification du périmètre fiscal du système (comparaison de l'empreinte). Sa durée est fonction des modifications apportées au système.

Une fois la commande passée, les étapes ci-dessous sont identiques à celles de l'évaluation initiale :

1. planification de l'évaluation de suivi ;
2. réalisation de l'évaluation de suivi (selon les modalités d'évaluation précédentes) ;
3. réponses aux éventuelles fiches de NC ;
4. revue du rapport ;
5. décision du comité de lecture.

II.4) Résiliation, suspension et retrait du certificat

Les motifs de résiliation, suspension ou de retrait d'un certificat par **BYCYB** sont les suivants :

- le non-respect des exigences contractuelles,
- le refus par l'entreprise de réaliser l'évaluation de suivi dans le délai imparti notifié par **BYCYB**
- le refus de mise en œuvre d'actions correctives requises dans le délai imparti notifié par le **BYCYB**,
- la demande d'annulation de tout ou partie de la certification par l'entreprise.

¹³ **BOI-TVA-DECLA-30-10-30-20250416**: point 330.

BYCYB notifie alors formellement la suspension ou le retrait au titulaire par lettre recommandée avec accusé de réception, en indiquant dans le premier cas les conditions de levée de la suspension, notamment les mesures correctives à prendre le cas échéant.

Afin de lever une suspension, **BYCYB** procède aux vérifications nécessaires pour rétablir la certification. Si tel est le cas, la suspension est levée et la certification remise en vigueur avec notification au titulaire.

Lorsque la certification est retirée ou suspendue, l'ex-titulaire de la certification se doit de cesser toute utilisation de la marque sous peine de poursuites.

CHAPITRE III : EXIGENCES APPLICABLES AU SYSTÈME DE MANAGEMENT DE LA CONFORMITÉ (SMC)

Le demandeur/titulaire de la certification doit mettre en œuvre, évaluer et maintenir à jour un Système de Management de la Conformité (SMC) destiné à s'assurer que chaque système d'encaissement ou mise à jour mis sur le marché répond en permanence aux exigences du présent référentiel.

Ce SMC doit respecter les exigences définies ci-dessous.

Note : toute mention future à l'action d'enregistrer une information ou de produire un enregistrement fait référence aux exigences du III.13) du présent chapitre.

III.1) Contexte

L'organisme doit déterminer et enregistrer les enjeux internes et externes ainsi que les risques (juridiques, réputation, financiers, etc.) liés à la conformité des systèmes d'encaissement mis sur le marché.

Pour ce faire, l'organisme doit notamment prendre en compte les contextes externes réglementaires, économiques mais aussi le contexte interne de l'organisme (ressources, processus, fournisseurs, sous-traitants etc.). Cela peut par exemple être fait en mettant en œuvre un processus de management des risques, en établissant une cartographie des risques ou une analyse SWOT.

III.2) Rôles et responsabilités

L'entreprise doit pouvoir démontrer que la direction a confié et communiqué la responsabilité et l'autorité à la fonction en charge de la conformité pour :

- a. s'assurer que le système de management de la conformité est conforme au présent chapitre III ;
- b. analyser les exigences techniques définies au chapitre IV ;
- c. les décliner en spécifications fonctionnelles, pouvant être mises en œuvre ;
- d. assurer ou organiser des sessions de formation/information pour les employés concernés afin de s'assurer qu'ils soient conscients des exigences de conformité qui les concernent ;
- e. définir des indicateurs de performance de la conformité ;
- f. contrôler et mesurer ces indicateurs ;
- g. analyser les résultats pour identifier si des actions correctives sont nécessaires ;
- h. identifier et gérer les risques liés à la conformité relatifs aux tierces parties telles que fournisseurs, agents, distributeurs, consultants et sous-traitants ;

- i. superviser les conditions d'externalisation, afin de s'assurer qu'elles tiennent compte des exigences de conformité définies dans le présent référentiel.
- j. assurer une veille légale et réglementaire.

La direction doit s'assurer que les responsabilités et autorités, pour chaque activité en lien avec les systèmes d'encaissement (conception, développement, tests, intégration, fabrication, déploiement/distribution, configuration, installation, support), soient définies de façon à assurer que les exigences définies dans le présent référentiel sont, systématiquement, et de façon permanente, mises en œuvre.

III.3) Objectifs et mise en œuvre du SMC

L'objectif principal du SMC est de s'assurer que chaque système d'encaissement ou mise à jour mis sur le marché répond en permanence aux exigences du présent référentiel.

L'entreprise doit déterminer et justifier quelles sont les activités qui peuvent avoir un impact sur la conformité du système d'encaissement (conception, développement, tests, intégration, fabrication, déploiement/distribution, configuration, installation, support et évaluation de l'efficacité du SMC).

Pour chaque activité qui peut avoir un impact sur la conformité, l'entreprise doit définir des objectifs de conformité qui doivent être :

- pertinents ;
- cohérents avec les objectifs du SMC ;
- mesurables ;
- communiqués aux personnes concernées ;
- compris et appliqués ;
- surveillés régulièrement par une personne en charge de la conformité ;
- mis à jour si nécessaire ;
- enregistrés.

L'organisme doit s'assurer que le SMC peut atteindre les résultats attendus et prévenir ou réduire les risques. Pour cela, il doit notamment prévoir :

- les actions pertinentes à mettre en œuvre en corrélation avec
 - les enjeux ;
 - les risques ;
 - les exigences ;
- l'intégration de ces actions au sein des activités concernées ;
- l'évaluation (et son enregistrement) de l'efficacité de ces actions.

III.4) Veille juridique et réglementaire

L'organisme doit être en mesure d'identifier les nouveautés et changements de législation, directives, réglementations, exigences de conformité afin d'assurer la pérennité de la conformité des systèmes d'encaissement.

L'organisme pourra par exemple :

- être destinataire des bulletins d'information des organismes de réglementation (DGFIP, ministères, etc.);
- suivre ou participer à des groupes de travail professionnels ;
- s'abonner aux newsletters appropriées ;
- participer aux événements professionnels du secteur ;
- consulter régulièrement les sites internet des organismes de réglementation et de certification ;
- faire appel à des conseillers juridiques ;
- etc.

L'impact de ces changements doit être évalué et les actions (et modifications du SMC) qui en découlent doivent être effectuées, suivies et enregistrées. En cas de modification des exigences, les spécifications fonctionnelles devront clairement les identifier.

III.5) Etablissement des contrôles de conformité

Pour les activités qui peuvent avoir un impact sur la conformité du système d'encaissement (définies au chapitre III. 3), l'organisme doit planifier mettre en œuvre et enregistrer des contrôles efficaces pour chaque activité liée au système d'encaissement afin de s'assurer que les exigences sont respectées et que les non-conformités sont évitées ou détectées et corrigées.

Pour cela, l'entreprise doit :

- désigner des personnes compétentes, maîtrisant les exigences du référentiel pour effectuer ces contrôles ;
- définir l'objet du contrôle ;
- définir une fréquence de contrôle adapté ;
- enregistrer les résultats de ces contrôles ;
- en cas de non-conformité, enregistrer l'analyse de la cause et les actions prises afin de corriger la NC ;
- s'assurer que les contrôles définis ont bien été réalisés aux étapes opportunes et que les résultats démontrent la conformité du système d'encaissement au présent référentiel.

Ces contrôles peuvent s'appuyer sur :

- des politiques, procédures, processus et instructions de travail opérationnels documentés, clairs, pratiques et faciles à suivre ;

- des systèmes et des rapports d'anomalies ;
- des approbations ou revues de code ;
- des plans et rapports de test ;
- une séparation des rôles et des responsabilités incompatibles ;
- des processus automatisés ;
- des plans annuels de conformité ;
- des audits de la conformité.

III.6) Conception et développement du système d'encaissement

L'organisme doit mettre en œuvre, de façon maîtrisée, et enregistrer un processus de conception et un processus de développement du système d'encaissement ou de sa mise à jour approprié pour assurer la fourniture de systèmes d'encaissement conformes aux exigences du présent référentiel.

Les éléments de sortie du processus de conception qui doivent être enregistrés sont, a minima, l'ensemble des spécifications fonctionnelles liées à la conformité au présent référentiel et les plans de tests associés.

L'élément de sortie du processus de développement est un prototype ou une mise à jour d'un système d'encaissement, conforme au présent référentiel ainsi qu'à minima l'enregistrement des rapports des tests de conformité.

Les éléments suivants du processus de développement qui doivent être définis et enregistrés (voir IV. 1 dossier organisationnel et dossier de maintenance) doivent être appliqués tels que définis :

- la méthode de développement suivie (cycle en V, W, méthode agile, méthode propre à l'organisme, etc.) ;
- la gestion du code source : explication de l'organisation des répertoires, fichiers de code source, classes, packages, librairies, dll, etc. ;
- la gestion de la nomenclature des versions (et notamment la gestion des numéros de versions majeures et mineures)¹⁴.

Ces processus doivent prendre en compte :

- les exigences de conformité du présent référentiel ;
- la revue des spécifications fonctionnelles et des rapports de tests par la fonction en charge de la conformité.

La maîtrise de ces processus doit notamment s'appuyer sur l'atteinte et l'enregistrement des objectifs et contrôles de conformité définis au préalable et sur la mise

¹⁴ CF : exigence technique n° 21

en œuvre, le suivi et l'enregistrement de toute action jugée nécessaire pour remédier aux problèmes identifiés lors des contrôles.

En cas de modification des processus de conception et/ou de développement, l'organisme doit s'assurer, et enregistrer les preuves, que la modification n'a pas d'impact négatif sur la conformité du système d'encaissement au présent référentiel.

III.7) Maitrise des sous-traitants

La sous-traitance de certaines activités (conception, développement, tests, intégration, fabrication, déploiement/distribution, configuration, installation, support) liées au système d'encaissement est possible à condition qu'elle, ainsi que les risques sur la conformité du système d'encaissement, soient maîtrisés.

L'organisme doit identifier ses fournisseurs/sous-traitants critiques, analyser les risques sur la conformité du système d'encaissement liés à la sous-traitance et mettre en œuvre toutes les actions jugées nécessaires afin de réduire ces risques. Ces informations doivent être enregistrées.

Les conditions de sous-traitance doivent être formalisées et enregistrées (définition du sous-traitant, exigences, objectifs et contrôles de conformité, communication des résultats, procédure à suivre en cas de non-conformité).

L'organisme doit surveiller les conditions de sous-traitance ainsi que les résultats (et les enregistrer) de l'activité externalisée en mettant en œuvre des contrôles afin de s'assurer du maintien de la conformité du système d'encaissement. Il doit communiquer ces modalités de contrôle/évaluation au sous-traitant concerné.

Il est par exemple possible de suivre ces conditions via un audit du système de management de la qualité du sous-traitant par **BYCYB** ou de tenir compte d'une certification ISO 9001 par un organisme accrédité sur les activités précitées liées aux systèmes d'encaissement et les sites concernés.

III.8) Identification et traçabilité de la distribution

Chaque système d'encaissement distribué doit être identifié de manière unique (ainsi que la version distribuée). Cette identification doit permettre :

- d'assurer si applicable¹⁵ la traçabilité des systèmes distribués sur le marché ;
- de pouvoir faire une mise à jour ou une nouvelle installation le cas échéant (vulnérabilité majeure détectée, correctif lié à la conformité à appliquer, etc.).
- de s'assurer que la dernière version majeure certifiée est disponible pour être déployée chez les clients finaux.

¹⁵ Un logiciel en mode SAAS avec une seule instance n'est pas concerné

- de s'assurer que l'éditeur a notifié les clients finaux de la disponibilité de la dernière version majeure certifiée dans le cas de la non mise à jour automatique des systèmes chez les clients finaux.

L'organisme doit enregistrer et mettre continuellement à jour un registre des systèmes et versions distribués à ses clients.

Exemple de solution acceptable : Il est possible de mettre en place un système de licence pour suivre le nombre de système de caisse déployé chez chaque client final.

III.9) Communication avec les clients

L'organisme doit prévoir la transmission à tous les clients chez qui le système d'encaissement certifié est installé :

- tous les documents nécessaires au bon fonctionnement du système d'encaissement (mode d'emploi, prérequis matériel, etc.), que ceux-ci soient fournis par l'éditeur/fabricant ou un distributeur ;
- les procédures de support et de formation le cas échéant ;
- les engagements de responsabilité des clients vis-à-vis de la loi des finances pour 2016 (obligation de réaliser les clôtures, conservation des données, etc.) ;
- 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 données¹⁶ ;
- le certificat correspondant.

Par ailleurs, il doit s'assurer de la disponibilité des documents précités pour les équipes internes et les utilisateurs pendant 3 ans après la date de fin de distribution de chaque version majeure du système d'encaissement certifié.

La communication concernant la certification du système d'encaissement ne doit pas :

- être ambiguë pour le client quant au nom et à la version du système d'encaissement bénéficiaire de la certification ;
- porter à confusion sur le fait que la certification concerne un système d'encaissement et non une entreprise, un système de management ou une prestation de service.

La liste des systèmes de caisse certifiés est disponible sur le site internet **BYCYB** soit via une recherche dans le moteur dédié, soit sur demande auprès de **BYCYB** qui fournit les informations relatives à la validité d'un certificat donné.

¹⁶ CF : exigence technique n° 19

III.10) Usage de la marque LNE – Système de caisse

Le LNE est propriétaire de la marque de certification LNE numérique. Le LNE confie la gestion de la certification LNE relative aux systèmes de caisse à BYCYB. BYCYB, en qualité d'organisme de certification, est responsable vis-à-vis du LNE de toutes les opérations qui lui sont confiées conformément au présent référentiel.

Seules les entreprises titulaires de la certification « LNE système de caisse » pour un ou plusieurs de leurs systèmes de caisse certifiés peuvent utiliser la marque « LNE système de caisse » sur ses produits et supports de communication. La marque de certification devra être utilisée conformément à la charte graphique, publiée par le LNE **et repris sur le site de BYCYB** en vigueur.

Lorsque le titulaire prévoit l'apposition du marquage LNE (marque LNE – système de caisse), il doit respecter les dispositions destinées à s'assurer du bon usage de la marque :

- ne pas utiliser la certification obtenue d'une manière qui puisse nuire au LNE, ni faire de déclaration ou de communication sur la certification de ses produits qui puisse être considérée comme trompeuse ou non autorisée ;
- toute référence à la certification avant la notification de celle-ci est interdite ;
- en cas de retrait de certification, la référence à cette certification retirée est interdite : tout moyen de communication qui y fait référence doit cesser d'être utilisé ;
- faire des déclarations sur la certification en cohérence avec le certificat émis par **BYCYB** ;
- reproduire les certificats dans leur intégralité, avec les annexes le cas échéant, en cas de fourniture à un tiers ;
- toute référence à la certification LNE systèmes de caisse dans la publicité, la présentation de tout service, ainsi que sur les documents commerciaux de toute nature qui s'y rapportent doit reprendre au minimum les informations suivantes :
 - le numéro du certificat ;
 - l'adresse du site internet de BYCYB

Tout usage ou référence abusif de la marque « LNE systèmes de caisse », qu'il soit l'objet du titulaire du certificat ou d'un tiers, fera l'objet de poursuites en application de la réglementation en vigueur concernant la publicité mensongère et la propriété intellectuelle.

III.11) Evaluation et amélioration des performances du SMC

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

Cette surveillance comprend l'évaluation de l'efficacité :

- des contrôles définis en III.5, par exemple par analyse des résultats de tests par échantillonnage ;
- du traitement des non-conformités précédemment identifiées ;

- des actions mises en œuvre pour réduire les risques liés à la conformité des systèmes d'encaissement distribués ;
- des prestataires externes.

L'organisme doit tirer parti de la surveillance de 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 NC.

III.12) Traitement des anomalies

Il ne peut exister aucune dérogation aux exigences du présent référentiel. L'organisme doit s'assurer que les systèmes d'encaissement non-conformes produits soient identifiés et maîtrisés afin d'éviter leur distribution et utilisation.

En cas de détection d'anomalies au moment des contrôles définis au III.5, l'organisme doit réagir (même après distribution éventuelle) de la manière suivante :

- analyser l'anomalie: identifier ses causes afin de déterminer s'il est nécessaire de mener une action pour les éliminer afin que l'anomalie ne se reproduise pas ;
- mettre en œuvre les actions permettant :
 - de corriger l'anomalie;
 - ou d'empêcher l'utilisation du ou des systèmes d'encaissement concernés, de prévenir ses clients, et procéder au rappel des produits ou à leur mise à jour ;
- évaluer l'efficacité des actions mises en œuvre ;
- mettre à jour les risques identifiés en III.1 si nécessaire ;
- mettre à jour le SMC si nécessaire.

L'organisme doit enregistrer les informations concernant la nature de l'anomalie, son analyse, les actions mises en œuvre ainsi que leurs résultats.

III.13) Gestion des enregistrements

L'organisme doit maîtriser les enregistrements cités dans le présent référentiel ainsi que tous ceux jugés pertinents afin qu'ils soient disponibles, accessibles et conviennent à l'utilisation, quand et là où ils sont nécessaires. L'organisme doit s'assurer, du stockage, de la protection, de la durée de conservation et de l'élimination de ces enregistrements.

Les enregistrements concernés sont à minima les suivants :

- risques (juridiques, réputation, financiers, etc.) liés à la conformité des systèmes d'encaissement (III.1) ;
- objectifs de conformité de chaque niveau et fonction pour les activités concernées (III.3) ;
- action pertinente pour atteindre les résultats attendus ou prévenir les risques et l'évaluation de son efficacité (III.3) ;

- action pertinente suite à une modification du contexte et/ou du SMC et l'évaluation de son efficacité (III.4) ;
- contrôles de conformité mis en œuvre et leurs résultats (III.5 & III.6) ;
- analyse de la cause d'une NC et des actions prises suite à celle-ci (III.5 & III.6) ;
- processus de conception (III.6) ;
- spécifications fonctionnelles liées à la conformité (III.2 & III.6) ;
- plans de test (III.6) ;
- processus & méthode de développement (III.6) ;
- rapports de test (III.6) ;
- gestion du code source (III.6) ;
- définition du périmètre fiscal (III.6) ;
- gestion de la nomenclature des versions (III.6) ;
- preuve de non impact sur la conformité d'une modification des processus de conception et développement (III.6) ;
- conditions de sous-traitance (III.7) ;
- résultats des processus externalisés (III.7) ;
- identification des fournisseurs/sous-traitants critiques (III.7) ;
- analyse de risques sur la conformité de la sous-traitance (III.7) ;
- action pertinente pour réduction du risque lié à la sous-traitance (III.7) ;
- registre des systèmes et versions distribués (III.8) ;
- informations sur les NC, leur analyse et les actions mises en œuvre (III.12).

Lorsqu'il enregistre et met à jour des informations enregistrées, l'organisme doit s'assurer que les éléments suivants sont définis et corrects :

- identification et description : titre, date, numéro de version du document ;
 - dans le cas d'un enregistrement électronique : nom du fichier et extension (word, pdf, jpg, etc.) ;
- que la revue/approbation du caractère approprié et pertinent des informations est effectuée par les personnes pertinentes avant leur diffusion.

L'organisme doit s'assurer que les documents d'origine externe sont identifiés et empêcher toute utilisation de documents périmés.

CHAPITRE IV : EXIGENCES TECHNIQUES APPLICABLES AU SYSTÈME D'ENCAISSEMENT CERTIFIÉ

Ce chapitre présente les exigences techniques, auxquelles le système d'encaissement certifié doit satisfaire. Le demandeur de la certification est libre de démontrer comment il y répond. Des exemples de solution acceptables sont présentés pour certaines exigences.

Les méthodes de contrôle sont basées sur l'évaluation de la documentation liée au système d'encaissement, des vérifications fonctionnelles et de robustesse sur le système d'encaissement à certifier.

Pour chaque exigence, sont décrites, lorsque c'est applicable : l'intitulé de l'exigence, des indications ou exemples de solution(s) acceptable(s) et les modalités de vérification documentaires, fonctionnelles et de robustesse.

IV.1) Documentation

La documentation du système d'encaissement doit décrire l'ensemble des fonctionnalités et mécanismes mis en œuvre dans le cadre de la certification permettant de répondre à l'ensemble des exigences techniques définies dans le présent chapitre. L'organisation de cette documentation doit être décrite dans un document chapeau¹⁷.

L'ensemble de cette documentation doit être :

- conservée sur support papier ou informatique ;
- conservée jusqu'à l'expiration de la 3^e année suivant celle au cours de laquelle le système a cessé d'être diffusé¹⁸ ;
- identifiée de façon claire et unique :
 - titre pertinent, en anglais ou en français ;
 - numéro de version du document et/ou date d'approbation du document.

Note : Il est rappelé, pour chaque exigence technique, la documentation attendue dans la case « vérification documentaire ».

Le demandeur de la certification est libre de répondre à chacune de ces exigences dans la documentation réglementaire ou dans la documentation complémentaire tout en respectant les contraintes de celles-ci (langues de rédaction notamment).

¹⁷ CF : IV.1) Exigence 2.

¹⁸ CF : III.10) communication avec les clients

Exigence 1 : documentation réglementaire¹⁹

Le système d'encaissement doit faire l'objet d'une documentation décrivant sa conception, son exploitation, sa maintenance et son utilisation.

Les 7 documents listés ci-dessous sont visés par le droit de communication de l'administration fiscale, ils doivent être rédigés en français, séparément et intitulés comme suit :

1. Dossier de conception générale,
2. Dossier de spécifications fonctionnelles,
3. Dossier d'architecture technique,
4. Dossier organisationnel,
5. Dossier de maintenance,
6. Dossier d'exploitation,
7. Dossier utilisateur

Indications concernant les éléments attendus :

Ces indications ne sont pas exhaustives, leur seul but est d'avoir une meilleure compréhension des attendus de chaque document.

Dossier de conception générale : Décrit le système et ses grands principes de fonctionnement dans leur ensemble, le matériel associé au système pour permettre l'encaissement. Cartographie des différents modules et de leurs interactions. Quels sont les OS et langages utilisés, les caractéristiques du réseau, description succincte des bases de données éventuelles et de la manière dont elles sont interfacées (modèles conceptuels & logiques de données : MCD/MLD). Doit également permettre d'identifier de façon non ambiguë le système : périmètre fiscal, versions mineures/majeures.

Dossier de spécifications fonctionnelles : Description des cas d'usage identifiés, des points d'attention et demandes particulières inhérents au système, définis pendant la phase de conception afin de valider que la solution répondra bien à des besoins expressément identifiés. On doit notamment retrouver les spécifications liées aux exigences du référentiel LNE.

Dossier d'architecture technique : décrit en profondeur l'implémentation technique de la solution : technologies, algorithmes (notamment de signature et hashes utilisés pour la sécurisation des données), frameworks, protocoles utilisés ; architecture détaillée du système (schéma avec nature des flux et les différents composants du système). Ce dossier doit couvrir tous les traitements effectués sur les données à sécuriser, notamment leur transport, sauvegarde, export, impression et affichage.

¹⁹ BOI-CF-COM-10-80-20160803 : point 200.

Dossier organisationnel : Décrit quels sont les processus et l'organisation mis en place pour la conception, le développement, la configuration / déploiement du système ? RACI, organigrammes etc.

Dossier de maintenance : destiné à identifier le suivi des évolutions/corrections du produit, les processus et l'organisation en place pour la gestion des vulnérabilités, la gestion des licences, les méthodes de mises à jour d'une version (corrective ou évolutive) et de sa livraison chez le client, politique de versionning du code mentionnant la gestion des versions majeures/mineures au sens de la réglementation.

Description de l'architecture du code source (organisation des différents fichiers de code, branches sur le gestionnaire de code) et identification des portions concernées par la certification entrant dans le périmètre fiscal.

Politique de gestion de versions du code (si applicable l'outil utilisé : git, SVN, etc.) identifiant les portions de code impactant le périmètre fiscal, lié aux fonctions de sécurisation, de conservation, d'inaltérabilité et d'archivage au sens du BOI TVA 30-10-30. Ce code, dit « version majeure » ou périmètre majeur/fiscal ne peut faire l'objet de modification sans information du LNE et dans ce cas il fera l'objet d'une évaluation supplémentaire afin d'en vérifier l'impact sur la conformité.

Dossier d'exploitation : Description des configurations et paramétrages possibles du système, de son installation, des prérequis matériels, des modalités de sauvegarde des données, de la gestion des droits utilisateurs, de l'utilisation et de la supervision du système par le ou les administrateurs du système ainsi que le remplacement du système.

Dossier utilisateur : Manuel utilisateur à destination de l'utilisateur final décrivant les fonctionnalités du système, son mode d'emploi.

Manuel utilisateur à destination de l'administration fiscale décrivant précisément et simplement l'accès aux données dédié à l'administration fiscale (avec description des éventuels champs de tables, fichiers XML, CSV, etc.), notamment les méthodes de calcul des données cumulatives et récapitulatives²⁰, les méthodes de vérification d'intégrité des données dans le système²¹ et de vérification d'intégrité des archives²² ainsi que de preuve de l'exhaustivité du transfert des données vers le système centralisateur²³. Il peut être inclus dans le manuel utilisateur ou séparé.

Vérification documentaire :

Vérifier que la documentation réglementaire existe, est correctement identifiée (titres, n° de version et/ou date d'approbation) et est bien rédigée en français.

²⁰ Voir totaux de période et total perpétuel : CF exigence n°7

²¹ CF exigence n°8

²² CF exigence n°12

²³ CF exigence n°18

Vérification fonctionnelle :

Vérifier qu'un échantillon de documents relatifs à un système en cours de diffusion est disponible. Dans le cas d'un système certifié qui a cessé d'être diffusé depuis moins de 3 ans, vérifier que sa documentation est disponible.

Vérification de robustesse :

Vérifier que la documentation technique des méthodes de sécurisation est cohérente avec ce qui est implémenté.

Exigence 2 : documentation complémentaire

La documentation complémentaire est composée de toute la documentation permettant de répondre aux exigences techniques du présent référentiel et ne faisant pas partie de la documentation réglementaire. Elle doit être rédigée en français ou en anglais.

L'organisme doit fournir un document chapeau décrivant l'organisation de la documentation et récapitulant pour chaque exigence technique quels sont les documents, les paragraphes et les numéros de page concernés.

Vérification documentaire :

Vérifier que la documentation complémentaire est correctement identifiée (titres, n° de version et date d'approbation) et est bien rédigée en français ou en anglais.

Vérification fonctionnelle :

Vérifier qu'un échantillon de documents relatifs à un système en cours de diffusion est disponible. Dans le cas d'un système certifié qui a cessé d'être diffusé depuis moins de 3 ans, vérifier que sa documentation est disponible.

Vérification de robustesse :

Vérifier que la documentation technique des méthodes de sécurisation est cohérente avec ce qui est implémenté.

IV.2) Enregistrement des données

Exigence 3 : Données à enregistrer²⁴

Le système d'encaissement doit enregistrer toutes les données liées à la réalisation d'une transaction et à son règlement. Ces données doivent être enregistrées dès que l'émission d'un justificatif (provisoire, définitif ou duplicata) est possible. Ces données comprennent à minima :

²⁴ BOI-TVA-DECLA-30-10-30-20250416: point 50-75-130

- le numéro de justificatif (de transaction le cas échéant),
- l'identifiant du TPV²⁵ (dans le cas d'un logiciel de facturation, cette donnée n'est pas obligatoire),
- un identifiant unique de l'établissement d'utilisation du système d'encaissement,
- la date et l'heure de la transaction (année, mois, jour, heure, minute),
- le montant total TTC de la transaction,
- les détails des articles ou prestations, soit pour chaque ligne de la transaction :
 - libellé,
 - quantité,
 - prix unitaire,
 - total HT de la ligne,
 - taux de TVA associé, toute autre donnée élémentaire²⁶ nécessaire au calcul du total HT de la ligne.

Exigence 3 : Données à enregistrer

- le mode de règlement (et les détails des montants réglés par mode de paiement si le règlement a lieu via plusieurs modes de paiement),
- la date de règlement (si différente de la date de transaction),
- toute donnée permettant d'assurer la traçabilité de la transaction et de garantir l'intégrité des données d'encaissement²⁷.

Note spécifique :

Ces données doivent être enregistrées telles quelles, en tant que données élémentaires, dans la base de données et/ou le système de fichier et pas seulement pouvoir être retrouvées sur la base d'un calcul, **notamment le total HT de la ligne**.

Le libellé de l'article ou de la prestation doit être enregistré. Un code article, identifiant article n'est pas suffisant.

Toute référence future aux « données d'encaissement » correspond aux données requises dans cette exigence plus celles générées par les corrections (exigence n°4), celles requises pour l'exigence 5 relative au mode école/test ainsi que les données

²⁵ TPV : Terminal Point de Vente identifié par un numéro unique (n° de terminal, de caisse, de balance, etc.). Un terminal assure l'enregistrement des données d'encaissement localement, temporairement (en attendant le transfert des données vers un système centralisateur) ou dans le respect avec l'exigence n° 16 concernant la conservation des données pendant la durée de 6 ans à partir de la date de la dernière transaction enregistrée sur l'exercice fiscal courant.

²⁶ Donnée élémentaire : donnée qui n'est pas obtenue par calcul à partir d'autres données

²⁷ CF exigence n°8

cumulatives et récapitulatives requises pour l'exigence 7, les données de traçabilité d'impression/réimpression de justificatifs définies dans l'exigence n°9, les données définies dans l'exigence n°15 de traçabilité des opérations de purge, d'archivage et de restauration des données ainsi que les données définies dans l'exigence n°18 de traçabilité de la remontée des données des TPV vers le système centralisateur le cas échéant.

Il peut notamment être considéré que les données sont enregistrées lorsqu'elles sont stockées dans la mémoire dure, non volatile du système d'encaissement (type EEPROM), c'est-à-dire qu'elles ne s'effacent pas si le système d'encaissement n'est plus alimenté en électricité.

Exemples de solutions acceptables :

L'identifiant unique de l'établissement d'utilisation peut être le n° de SIRET de l'établissement ou les coordonnées de l'établissement (adresse complète).

Vérification documentaire :

Description de la méthode utilisée pour enregistrer toutes les données de manière exhaustive. Lorsque les paramètres peuvent affecter la conformité à la réglementation française, il convient que les paramètres et leurs valeurs soient explicitement identifiés dans la documentation.

Vérification fonctionnelle :

Réaliser un ensemble échantillonné d'opérations. Vérifier que l'ensemble des opérations réalisées préalablement apparaît dans les données enregistrées.

Les cas de test suivants sont à réaliser s'ils sont possibles : application des remises, application des promotions, application des avantages fidélités ou équivalent, réimpressions de ticket, etc.

Lorsque les paramètres peuvent affecter la conformité à la réglementation française, il convient de vérifier qu'avec les paramètres et leurs valeurs paramétrées conformément à la documentation, la conformité à la réglementation française est effective, ainsi que la vérification de l'impossibilité de modifier ces paramètres sauf après réinitialisation.

Exigence 4 : corrections²⁸

Si des corrections (modifications ou annulations) sont apportées à des transactions, par quelque moyen que ce soit, ces corrections doivent s'effectuer par un enregistrement des données d'encaissement correctives par le biais d'opérations de « plus » et de « moins », et non par modification directe des données d'encaissement enregistrées.

²⁸ BOI-TVA-DECLA-30-10-30-20250416: point 90 & 100.

Vérification documentaire :

Vérifier à partir de la description complète des méthodes de correction des transactions comment la donnée modifiée est liée à la donnée originale et que la traçabilité des modifications est assurée.

Vérification fonctionnelle :

Tester le fonctionnement du système pour vérifier que les corrections s'effectuent par des opérations de "plus" et de "moins" et non par des modifications directes des données d'origines enregistrées.

Vérifier par examen de la base de données ou du fichier que les données sont effectivement enregistrées, en cas de correction.

Des cas de test doivent inclure les cas suivants : modification de quantité, suppression d'un article, suppression d'un ticket, ajout d'un article à un ticket déjà finalisé avant paiement, application des remises, application des promotions, application des avantages fidélités ou équivalent, etc.

Exigence 5 : Mode école-test²⁹

Les données générées, ou simulées, par le biais d'un mode ou d'une fonction « école », « test », permettant l'enregistrement de transactions fictives, doivent être enregistrées et sécurisées au **même titre que les données citées à l'exigence 3** mais explicitement identifiées comme étant issues de ce mode.

L'identifiant du responsable de l'opérateur enregistrant les transactions, ainsi que toutes les opérations enregistrées lors de l'utilisation de ce mode font partie des données de transaction. A ce titre ces données doivent **respecter les mêmes exigences que les données de l'exigence 3** (enregistrement, sécurisation, archivage).

Toute pièce justificative émise lors de l'utilisation de ce mode doit être identifiée comme telle en y apposant en trame de fond la mention « factice », « simulation » ou toute autre mention pertinente.

L'utilisation du mode école doit être visible depuis l'affichage du système d'encaissement.

Si aucun mode de ce type n'est présent dans le système ceci doit être indiqué dans la documentation.

Exemples de solutions acceptables :

Afin d'identifier les données d'encaissement générées par des simulations de transactions, il est par exemple possible d'utiliser un champ spécifique en base de données ou une base de données différente des données réelles de production, à condition que les mêmes

²⁹ BOI-TVA-DECLA-30-10-30-20250416: point 90 & 150.

mécanismes de sécurisation interviennent et que ces données soient bien intégrées dans les archives.

Vérification documentaire :

Vérifier à partir de la description complète du mode concerné que :

les données générées sont bien enregistrées et sécurisées comme toute donnée d'encaissement,

l'identifiant du responsable et toutes les opérations effectuées sont bien enregistrées et sécurisées, les données d'encaissement fictives font l'objet d'une identification claire, les pièces justificatives font l'objet d'une identification claire, l'affichage du système identifie le mode de façon appropriée.

Vérifier que si aucun mode ne permet de simuler ou générer des données liées à une transaction fictive, ceci est explicite et argumenté le cas échéant dans la documentation.

Vérification fonctionnelle :

Entrer dans le mode "école" ou "factice" ou similaire.

Vérifier dans la base de données et sur les pièces justificatives émises que le fonctionnement est conforme à l'exigence et est cohérent avec la documentation.

Vérifier que les données permettant d'identifier l'usage de ce mode école sont bien sécurisées en essayant de les modifier **et en vérifiant la bonne détection de l'erreur d'intégrité.**

IV.3) Clôtures

Exigence 6 : clôtures annuelles, mensuelles et journalières²⁶

Le système d'encaissement doit prévoir des fonctionnalités de clôture journalières, mensuelles et annuelles. La clôture annuelle doit pouvoir se baser sur l'exercice fiscal lorsque celui-ci ne coïncide pas avec l'année civile.

Le système d'encaissement ne doit pas permettre d'enregistrer de nouvelles transactions, de modifier ou d'annuler une transaction sur une période clôturée. Si la clôture doit être réalisée par l'utilisateur, celui-ci doit être informé de cette possibilité et de la responsabilité qui lui incombe.

Les logiciels de facturation n'ont pas l'obligation de réaliser les clôtures journalière, mensuelle et annuelle sous réserve de pouvoir fournir via une fonctionnalité, à la demande de l'administration, le total du chiffre d'affaires enregistré pour une période déterminée.

Note spécifique :

Ces clôtures peuvent être réalisées automatiquement par le système d'encaissement ou faites par l'utilisateur.

Dans le cas de la clôture réalisée par l'utilisateur, il reste de la responsabilité de l'utilisateur du système d'encaissement de réaliser les clôtures périodiques.

Exemples de solutions acceptables :

Il est possible d'avertir l'utilisateur de la nécessité de réaliser les clôtures par tout moyen adéquat (affichage sur l'interface du système, notice d'utilisation, contrat, etc.).

Vérification documentaire :

Vérifier à partir de la description de la fonctionnalité de clôture si les 3 fonctions de clôture (journalière, mensuelle et annuelle) sont bien présentes, que la fonctionnalité est conforme aux exigences, que si la fonctionnalité n'est pas automatique l'utilisateur est averti de l'obligation qui lui incombe de réaliser les clôtures.

Dans le cas d'un logiciel de facturation, vérifier s'il existe une fonctionnalité de clôture journalière, mensuelle et annuelle ou bien une fonctionnalité permettant de fournir à la demande le total du chiffre d'affaires enregistré pour une période déterminée.

Vérification fonctionnelle :

Enregistrer des transactions et réaliser les clôtures (au moins 1 clôture de chaque niveau) et vérifier la bonne génération des clôtures.

Vérifier également qu'il est impossible d'enregistrer une nouvelle transaction ou de modifier/annuler une transaction sur la période clôturée.

Dans le cas d'un logiciel de facturation ne réalisant pas les clôtures journalière, mensuelle et annuelle, vérifier que le logiciel est en mesure de fournir, via une fonctionnalité à la demande le total du chiffre d'affaires enregistré pour une période déterminée.

Exigence 7 : Données cumulatives et récapitulatives³⁰

Pour chaque clôture, le système d'encaissement doit enregistrer et sécuriser³¹ le total cumulatif de la période et le total perpétuel comme toute autre donnée d'encaissement.

En cas de changement de système d'encaissement tous les compteurs repartent de zéro. Les compteurs de l'ancien système doivent alors être archivés³².

Dans le cas d'une mise à jour du système, tous les compteurs doivent continuer à être incrémentés sans être remis à 0.

Dans le cas d'un système d'encaissement utilisé par plusieurs assujettis, les données cumulatives et récapitulatives doivent être générées séparément pour chaque assujetti.

³⁰ BOI-TVA-DECLA-30-10-30-20250416: point 170.

³¹ CF exigence n°8

³² CF exigence n°10

Note spécifique :

Le total cumulatif de la période est le cumul du chiffre d'affaires décompté depuis l'ouverture de la période concernée. Il s'agit d'un compteur initialisé à 0 à l'ouverture de la période (journalière, mensuelle ou annuelle) et dont la valeur est stockée à la clôture.

Le total perpétuel est le cumul de chiffre d'affaires décompté depuis le début de l'utilisation du système d'encaissement. Il s'agit d'un compteur ne se remettant jamais à 0 et dont la valeur est stockée périodiquement à chaque clôture.

Vérification documentaire :

Vérifier à partir de la documentation sur les données cumulatives et récapitulatives que la méthode de calcul de ces totaux se base sur le chiffre d'affaires, est précisément décrite et que ces données sont bien enregistrées pour chaque clôture (journalière, mensuelle et annuelle).

Vérification fonctionnelle :

Vérifier sur la base d'un échantillon de données de test représentatives que le système d'encaissement calcule correctement et enregistre bien les totaux cumulatifs de période et total perpétuel pour chacune des périodicités de clôture.

Vérification de robustesse :

Vérifier que l'intégrité et l'authenticité des données cumulatives et récapitulatives repose sur un mécanisme robuste.

IV.4) Sécurisation & Inaltérabilité des données

Exigence 8 : Inaltérabilité des données³³

Le système d'encaissement doit prévoir un mécanisme permettant de garantir et de démontrer l'absence d'altération de toutes les données d'encaissement définies dans les exigences précédentes³⁴, et ce depuis leur enregistrement initial. Ce mécanisme doit permettre de détecter et mettre en évidence toute modification ou suppression de données d'encaissement. Les modalités de gestion des clés et/ou des certificats doivent être documentées, comprenant au moins les aspects suivants : la méthode de génération des clés et/ou des certificats, les durées de validité, la portée (qu'il s'agisse d'une clé/certificat par caisse ou partagée entre plusieurs caisses), les modalités de renouvellement et

³³ BOI-TVA-DECLA-30-10-30-20250416: point 80 & 100.

³⁴ Définies dans l'exigence n°3, les données d'encaissement correctives définies dans l'exigence n°4, les données du mode école-test définies dans l'exigence n°5, les données cumulatives et récapitulatives définies dans l'exigence n°7, les données de traçabilité d'impression/réimpression de justificatifs définies dans l'exigence n°9, les données définies dans l'exigence n°15 de traçabilité des opérations de purge, d'archivage et de restauration des données, les données définies dans l'exigence n°18 de traçabilité de la remontée des données des TPV vers le système centralisateur le cas échéant.

les mécanismes de révocation.

Exemples de solutions acceptables :

L'inaltérabilité des données peut être garantie par :

1) la preuve de l'authenticité et de l'intégrité des données qui peut être un chainage d'empreintes à clé, ou un chainage des signatures de chaque enregistrement.

L'authentification et l'intégrité peuvent être garanties par un mécanisme de signature (tels que RSA-SSA-PSS, ECDSA) ou un mécanisme d'empreinte avec clé (HMAC). La clé doit être générée par un procédé fiable et l'utilisateur final (le professionnel assujetti) ne doit pas pouvoir en avoir connaissance ou être aisément devinable. La signature (ou l'empreinte avec clé) d'une transaction doit inclure des éléments authentifiant la transaction précédente ainsi que la dernière transaction enregistrée (via un compteur ou tout autre élément unique) pour garantir qu'aucune transaction n'ait été supprimée.

Concernant le choix des algorithmes utilisés, il convient de se référer au Référentiel général de sécurité de l'ANSSI. Au-delà du choix de l'algorithme, son implémentation est tout aussi importante (gestion des clés pour signature, taille des clés, gestion du bourrage ou padding, etc.).

Les exemples de mécanismes d'empreinte à clé suivants sont acceptables : HMAC-SHA-256, HMAC-SHA3.

Les exemples de fonctions de hachage suivants sont non acceptables : SHA-1, MD5, CRC16, CRC32 et toutes autres formes de sommes de contrôles non cryptographiques y compris un CRC32 d'une empreinte SHA256.

Les exemples d'algorithmes de signatures de données suivant sont acceptables : RSA-SSA-PSS, ECDSA. Pour l'algorithme RSA, il est nécessaire d'utiliser une clé d'au minimum 1024 bits. Il est recommandé d'utiliser une clé de 2048 bits ou plus. Pour les courbes elliptiques, leur ordre doit être d'au moins 256 bits. Les exemples de courbes elliptiques suivantes sont acceptables : ed25519, Brainpool, P-256, ed448.

2) La signature ou la prise d'une empreinte à clé de l'ensemble des données enregistrées. Dans ce cas, à chaque transaction, la nouvelle signature ou l'empreinte à clé doit être calculée sur l'ensemble des données après leur vérification avec l'ancienne valeur.

3) Une parfaite maîtrise de l'accès en écriture des données peut être acceptable. Le professionnel assujetti ne doit en aucun cas pouvoir obtenir un accès en écriture aux données. Il est possible que le système s'appuie sur une base de **données chiffrée et signée** (par exemple, avec le mécanisme « encryption at rest » sous MongoDB) pour laquelle la clé cryptographique n'est pas aisément accessible par l'utilisateur (emploi de principes d'enfouissement de clés par exemple, ou de dongle USB externe avec mécanisme de type protection de licence).

Quelle que soit la solution choisie, dans le cas d'un système d'encaissement déployé sur un poste pour lequel l'utilisateur dispose des droits administrateurs il est nécessaire de se

prémunir d'une restauration des données dans un état antérieur. L'opération doit être détectée ou rendue impossible. Il est possible d'enregistrer, hors d'accès de l'utilisateur du système d'encaissement, la preuve d'intégrité (signature, empreinte à clé) du dernier enregistrement (dans le cas d'un chaînage des données) ou de l'ensemble de la base si le système le permet.

Ces solutions ne sont pas exhaustives et peuvent être utilisées conjointement, d'autres solutions peuvent être acceptées.

Exigence 8 : Inaltérabilité des données³³

Vérification documentaire :

Vérifier que les mécanismes assurant l'inaltérabilité des données sont décrits précisément, incluant les algorithmes de cryptographie utilisés. Vérifier que les données concernées par ces mécanismes comprennent bien l'ensemble des données d'encaissement à sécuriser :

Toutes les données d'encaissement définies à l'exigence 3,

Toutes les données correctives définies à l'exigence 4,

Toutes les données du mode école-test définies à l'exigence 5

Les données cumulatives et récapitulatives définies à l'exigence 7

Les données de traçabilité d'impression/réimpression définies à l'exigence 9

Les données de traçabilité des opérations de purge, archivage et restauration des données définies à l'exigence n°15.

Les données définies à l'exigence n°18 de traçabilité de la remontée des données des TPV vers le système centralisateur le cas échéant.

Vérification fonctionnelle :

Vérifier la présence d'un moyen de contrôle de l'intégrité des données ainsi que son efficacité en les modifiant directement sur disque ou en base des données d'encaissement.

Exigence 8 : Inaltérabilité des données³³

Vérification de robustesse :

Réaliser un ensemble d'opérations d'encaissement.

Se connecter sur le dispositif avec l'ensemble des moyens d'accès autorisés, et essayer de modifier les données d'opérations déjà enregistrées.

Vérifier, notamment par un audit de code, que les données d'encaissement enregistrées sont protégées contre leur altération (modification, insertion, suppression ou remplacement) en :

- cas 1) : Vérifier que le secret (la clé) est généré de façon aléatoire et qu'il n'est pas

accessible par un attaquant.

Vérifier que chaque enregistrement est cryptographiquement lié à l'enregistrement qui le précède chronologiquement, en incluant dans le calcul de l'empreinte cryptographique de l'enregistrement courant des éléments authentifiant l'enregistrement précédent, ainsi que la date et l'heure.

Vérifier que l'algorithme de signature ou d'empreinte à clé est conforme. Vérifier sur le dispositif, et par échantillonnage, la cohérence d'une chaîne pour un ensemble d'enregistrements contenant des corrections (modifications et des annulations).

Vérifier la sécurité des éléments en bout de chaîne, notamment contre leur suppression.

- cas 2) : Vérifier que le secret (la clé) est généré de façon aléatoire et qu'il n'est pas accessible par un attaquant. Vérifier qu'à chaque enregistrement, la précédente signature de l'ensemble des données est vérifiée avant son écrasement.

- cas 3) :

Vérifier que les moyens de protection apportant le même niveau de sécurisation que les exemples précédents sont bien mis en œuvre. Dans le cas d'une maîtrise se basant sur un tiers de confiance vérifier les dispositions et SLA prises concernant ces moyens de protection à partir des contrats, termes et conditions, descriptifs de la gestion des droits et du contrôle d'accès, des RACI des équipes intervenant sur les données, des preuves de traçabilité des opérations de maintenance ainsi que de tout autre document jugé pertinent.

Réaliser une analyse de robustesse sur le mécanisme assurant la sécurisation des enregistrements (exemples de tests à réaliser : validation de la chaîne des certificats électroniques, utilisation et implémentation correctes des mécanismes cryptographiques employés et conformité vis-à-vis de l'état de l'art, etc.).

Vérifier que la sécurité des flux de données repose sur des canaux sécurisés (par exemple HTTPS/TLS).

Vérifier que la restauration d'une base ou d'un dossier contenant les données protégées est empêchée ou détectée.

Vérifier que toutes les données d'encaissement concernées par les exigences 3, 4, 5, 7, 9, 15 sont couvertes par les mécanismes de sécurité.

Conclure sur la capacité du système à garantir l'intégrité et l'authenticité des données.

Exigence 9 : sécurisation des justificatifs

Le système d'encaissement doit permettre de distinguer et identifier sans ambiguïté les justificatifs émis avant paiement des justificatifs émis après paiement.

Tout justificatif réimprimé doit porter la mention « duplicata ».

Le système doit assurer la traçabilité des impressions et réimpressions de justificatifs (définitifs ou provisoires) de manière sécurisée, mais également des envois de justificatif

au format électronique.

Les informations présentes sur les justificatifs doivent être cohérentes avec les données d'encaissement enregistrées par le système d'encaissement.

Les tickets doivent mentionner le fait que le système de caisse soit certifié par le LNE.

Pour les systèmes centralisateurs, dans le cas où le système est en mode hors-ligne, cet état doit figurer sur les exports.

La procédure d'émission de justificatifs au format électronique doit être clairement documentée, incluant les protocoles d'envoi et les modalités de gestion des originaux et des duplicatas.

Il est recommandé que toute absence d'impression ou d'envoi de justificatif au format numérique soit enregistrée de manière sécurisée.

Note spécifique :

Facture, note, reçu, ticket, billets sont des justificatifs.

Ces justificatifs peuvent être sous forme papier ou sous forme dématérialisé (PDF...).

La présence de la signature de l'opération sur le ticket est recommandée, afin de démontrer la capacité à établir un lien certain et infalsifiable entre chaque ticket et la transaction correspondante enregistrée en base de données.

Exemples de solutions acceptables :

Il est possible de faire apparaître une mention « valable pour encaissement », « provisoire », « pro- forma », « non payé » sur le justificatif avant encaissement et faire apparaître une mention « paiement réalisé », « paiement reçu », sur le justificatif de reçu d'encaissement.

Dans les cas où une même note est partagée entre plusieurs clients, il est possible d'émettre un premier justificatif identifié comme provisoire, puis d'émettre des justificatifs après paiement dont la somme des totaux correspond au total du justificatif provisoire.

Il est possible d'assurer la traçabilité des impressions/réimpressions de justificatifs en enregistrant et en sécurisant le nombre de d'impressions de chaque justificatif ou de tracer chaque impression/réimpression en enregistrant la date, l'heure et le n° du justificatif (ou de la transaction le cas échéant) dans un journal de logs/d'évènements sécurisé avec le même niveau de sécurité que celui défini à l'exigence n°8.

Il est possible d'ajouter un champ en base de données pour identifier les opérations effectuées en mode hors-ligne.

Il est possible de mentionner sur le ticket le type de mode utilisé pour générer le ticket. Il est possible de mentionner sur le ticket la signature numérique de l'opération.

Il est possible de tracer l'utilisation du mode hors-ligne ainsi que sa durée maximale.

Il est possible de rajouter le n° de certificat LNE sur le ticket et/ou la facture.

Il est possible de ne pas indiquer le taux de TVA sur les justificatifs tant qu'il n'y a pas eu d'encaissement ou production du justificatif définitif

Afin d'assurer la traçabilité et la transparence des justificatifs délivrés, chaque ticket doit indiquer que le système d'encaissement est certifié. La mention « Système de caisse certifié LNE » est recommandée. Toutefois, la mention « Système certifié LNE » est recevable, sous réserve qu'elle ne génère aucune ambiguïté quant à la portée de la certification.

Vérification documentaire

Vérifier à partir de la description des méthodes d'impression des justificatifs que toutes les exigences sont prévues et documentées

Vérifier que la procédure d'émission de justificatifs au format électronique est clairement documentée, incluant les protocoles d'envoi et les modalités de gestion des originaux et des duplicatas.

Vérification fonctionnelle

Vérifier que les justificatifs émis avant et après paiement sont identifiables sans ambiguïté possible.

Vérifier suivant les différents cas d'usage du système la cohérence des justificatifs émis avec les transactions enregistrées et la mise à jour des compteurs.

Vérifier dans les cas de partage d'addition/note que la somme des montants des différents justificatifs est bien égale au montant TTC de la transaction initiale.

Vérifier la traçabilité des justificatifs physiques et dématérialisés générés.

Vérifier la présence sur le ticket de la signature de l'opération si appliqué par l'éditeur ou tout autre moyen permettant d'identifier de manière certaine quel ticket fait référence à quelle transaction en base de données.

Vérifier qu'il est possible d'identifier sur le ticket l'établissement d'émission du ticket (SIRET ...).

Vérifier le fait que le ticket mentionne que le système est certifié par le LNE.

IV.5) Archivage des données d'encaissement

Exigence 10 : Archivage des données

Le système d'encaissement doit prévoir une fonctionnalité d'archivage, à destination des utilisateurs, permettant l'export dans un format ouvert³⁵, des données d'encaissement

³⁵ Format ouvert : format de données interopérable, c'est-à-dire indépendant du logiciel utilisé pour le créer, le modifier ou le lire, et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre. Art 4 de la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

(Définies dans l'exigence n°3, les données d'encaissement correctives définies dans l'exigence n°4, les données du mode école-test définies dans l'exigence n°5, les données cumulatives et récapitulatives définies dans l'exigence n°7, les données de traçabilité d'impression/réimpression de justificatifs définies dans l'exigence n°9, les données définies dans l'exigence n°15 de traçabilité des opérations de purge, d'archivage et de restauration des données, les données définies dans l'exigence n°18 de traçabilité de la remontée des données des TPV vers le système centralisateur le cas échéant) figées et horodatées.

En cas de changement de système d'encaissement les données cumulatives et récapitulatives³⁶ doivent être archivées.

Note spécifique

La fonctionnalité d'archivage ne doit pas être confondue avec seulement une solution de sauvegarde à long terme des données. Il s'agit bien d'exporter du système, dans un format **ouvert et sécurisé, les données de transaction** figées, horodatées et sécurisées afin de se prémunir d'une perte des données suite à un problème matériel, une faille de sécurité, un changement de système d'encaissement ou tout autre raison. Il s'agit d'un moyen pour l'assujetti de pouvoir conserver indépendamment du système d'encaissement ses données d'encaissement et pouvoir les communiquer à l'administration fiscale en cas de contrôle.

Il n'est pas de la responsabilité de l'éditeur du système d'encaissement de réaliser l'archivage. Par contre, le système doit permettre à son utilisateur d'archiver les données. La réalisation de l'exécution de l'archivage reste de la responsabilité de l'utilisateur du système.

Exemple de solutions acceptables :

Les formats pour les données d'archivage suivants sont des formats ouverts acceptables: ods, xlsx, odb, csv, json, xml, txt. Si les données d'archivage sont compressées, les formats de compression suivants sont des formats ouverts acceptables : Zip, 7z, gz, bz2, tar, rar.

A contrario, les formats suivants sont des formats fermés ou propriétaires non acceptables : xls, mdb.

Vérification documentaire

Vérifier, à partir de la description de la fonctionnalité d'archivage que celle-ci est existante, qu'un utilisateur du système d'encaissement peut l'utiliser et en est averti, que le format est ouvert et que les données présentes dans l'archive sont bien figées, horodatées et complètes.

Vérifier, si nécessaire, la présence d'un engagement de l'éditeur du système d'encaissement, à fournir, aux utilisateurs, ainsi qu'à l'administration fiscale, les données

³⁶ CF exigence n°7

d'archivage, notamment dans le cas où l'utilisateur cesse d'utiliser le système d'encaissement.

Vérification fonctionnelle

Vérifier la disponibilité de la fonctionnalité d'archivage, que celle-ci fournit bien des archives dans un format ouvert et que les données présentes sont bien horodatées et complètes.

Vérifier **que** les totaux cumulatifs de période et totaux perpétuels figés à chaque période sont bien inclus dans l'archive.

Vérification de robustesse

Vérifier que l'intégrité et l'authenticité des données de la date de création de l'archive est protégée par un mécanisme robuste, tel que décrit à l'exigence n°8.

Exigence 11 : Périodicité d'archivage

Cette fonctionnalité d'archivage doit permettre à l'utilisateur, à toute date, d'avoir accès ou de pouvoir générer les archives pour toute période passée inférieure à 7 ans.

La période couverte par une archive ne doit pas pouvoir être supérieure à un an ou à un exercice fiscal.

Exemples de solutions acceptables

Il est acceptable de donner à l'utilisateur la possibilité de définir les bornes de la période dont il souhaite réaliser l'archivage (tout en respectant la contrainte maximale d'une année/exercice) ou de générer plusieurs fichiers d'archive périodiques (journalières, mensuelles et/ou annuelles).

Une fois les archives générées, il est de la responsabilité de l'utilisateur de les conserver pour la période légale de 7 ans.

Il est possible de laisser à l'utilisateur la possibilité d'avoir accès ou de pouvoir générer les archives pour des périodes passées supérieures à 7 ans mais l'obligation légale de conserver les données de transaction étant limitée à 6 ans à compter de la date de la dernière transaction de l'exercice fiscal, il est aussi acceptable de ne fournir cette possibilité que pour 7 ans.

Vérification documentaire

Vérifier, à partir de la description de la fonctionnalité d'archivage que l'utilisateur a la possibilité d'archiver toute période souhaitée sans toutefois pouvoir dépasser un an ou un exercice fiscal par archive.

Vérification fonctionnelle

Vérifier que l'utilisateur peut archiver toutes les données d'encaissement pour toute période souhaitée (en un ou plusieurs fichiers), à toute date, sans toutefois pouvoir

dépasser la limitation d'un an/exercice par archive.

Réaliser par exemple une ou des archives pour une période de plusieurs jours, 1 mois, plusieurs mois et/ou 1 an. Vérifier qu'il est impossible de faire un fichier d'archive dépassant une période d'un an ou d'un exercice fiscal.

Exigence 12 : Intégrité des archives

Les données contenues dans l'archive doivent être conformes aux données initiales figées dans le système d'encaissement et doit prévoir un mécanisme fiable, indépendant du support de conservation de l'archive, garantissant cette intégrité et permettant de la vérifier, y compris lorsque l'utilisateur a cessé d'utiliser le système d'encaissement.

Note spécifique

En cas de génération d'une archive sur une période contenant des données altérées/supprimées dans le système, ce mécanisme doit notamment le détecter et mettre en évidence que parmi les données archivées, certaines ne sont pas fiables.

Un assujetti décidant par exemple de changer de système d'encaissement ou d'arrêter l'utilisation d'un système d'encaissement reste concerné par l'obligation de conserver ses données d'encaissement pendant la durée légale³⁷. Pour ce faire il se doit de conserver les archives générées depuis le système d'encaissement avant d'avoir cessé de l'utiliser. En cas de contrôle par l'administration, il devra également pouvoir démontrer que ces archives sont intègres. L'éditeur du système d'encaissement doit donc prévoir que le contrôleur fiscal puisse vérifier l'intégrité des données d'archive générées avec son système d'encaissement indépendamment de celui-ci.

Le niveau de sécurité de ces mécanismes doit être au moins équivalent à celui utilisé pour répondre à l'exigence 8.

Exemples de solutions acceptables

Une archive peut par exemple être sécurisée par signature ou empreinte à clé et être stockée sur un dispositif externe (disque externe, clé USB, serveur distant, etc.).

Le mécanisme permettant de vérifier l'intégrité des archives peut par exemple être un outil téléchargeable ou directement accessible sur le site internet de l'éditeur/fabriquant du système d'encaissement. L'éditeur/fabriquant peut également prévoir et s'engager à le rendre accessible sur demande.

Vérification documentaire

Vérifier que les mécanismes assurant l'intégrité des archives sont décrits précisément, incluant les algorithmes de cryptographie utilisés.

Vérifier que le manuel à destination de l'administration fiscale précise comment accéder au

³⁷ CF exigence n°17

moyen permettant de vérifier l'intégrité des archives et que son fonctionnement est correctement décrit.

Vérification fonctionnelle

Vérifier la présence d'un moyen de contrôle de l'intégrité des archives ainsi que son efficacité en essayant de modifier directement l'archive.

Vérifier, en générant une archive comprenant des données altérées dans le système, qu'il est impossible de confondre dans les données de l'archive générée les données intègres et les données corrompues.

Vérifier que ce moyen de vérification est accessible y compris si l'utilisateur a cessé d'utiliser le système d'encaissement.

Vérification de robustesse

Vérifier que l'inaltérabilité des archives dans le temps repose sur un mécanisme robuste, garantissant un niveau de protection au moins équivalent à celui demandé à l'exigence n°8.

IV.6) Purges

Exigence 13 : Purge³⁸

Si le système d'encaissement dispose d'une fonctionnalité de purge des données d'encaissement, liée à la nécessité de libérer de l'espace mémoire, il doit garantir avant la mise en œuvre de la purge, la génération d'une archive contenant toutes les données d'encaissement à purger et sa conservation conformément à l'exigence n°17. Les données cumulatives et récapitulatives ne doivent jamais être purgées.

Note spécifique

N'est considérée comme une purge que la suppression des données du système d'encaissement (responsable de la conservation des données d'encaissement dans le respect des exigences du présent référentiel et notamment n°8 et n°16) intervenant avant la fin de la période légale de conservation³⁹. La conservation des archives devient alors le seul moyen pour un assujetti de conserver ses données d'encaissement en vue d'un éventuel contrôle fiscal⁴⁰.

Toute suppression des données antérieures à la période légale de conservation des données n'est pas considérée comme une opération de purge et n'est pas soumise aux exigences n°13, 14 et 15.

³⁸ BOI-TVA-DECLA-30-10-30-20250416 : point 250.

³⁹ CF exigence n°16

⁴⁰ CF exigence n°17

Vérification documentaire

Vérifier à partir de la description de la méthode de purge que celle-ci est systématiquement précédée de la génération d'une archive contenant bien toutes les données d'encaissement à purger.

Si aucune procédure de purge n'existe, vérifier que ceci est bien décrit dans la documentation.

Vérification fonctionnelle

Créer une archive fictive initiale contenant un échantillon de données d'origines et de modification, copier cette archive sur un autre support puis mettre en œuvre la procédure de purge. Vérifier la complétude de l'archive générée par la purge par rapport à l'archive initiale.

Vérification de robustesse

Vérifier que l'archive générée par ce biais est sécurisée avec le même niveau qu'à l'exigence n°12.

Créer une archive sur une période déterminée. Effectuer une purge des données de cette même période. Vérifier que l'archive est bien cohérente.

Exigence 14 : Purge partielle⁴¹

La fonctionnalité de purge ne doit pas supprimer du système d'encaissement les données cumulatives et récapitulatives⁴² ainsi que les données de traçabilité des opérations⁴³. Celles-ci doivent être conservées⁴⁴, sécurisées⁴⁵, dans le système d'encaissement.

Vérification documentaire

Vérifier à partir de la description de la méthode de purge que les données cumulatives, récapitulatives et de traçabilité sont toujours correctement conservées, sécurisées dans le système d'encaissement lui-même.

Vérification fonctionnelle

Sur un système de caisse représentatif, introduire des données connues, réaliser une purge et vérifier l'exactitude, et la bonne conservation, des données cumulatives et récapitulatives pour la période dont les données ont été purgées, contenues dans le système d'encaissement en les comparant avec les données initialement introduites.

Vérification de robustesse

⁴¹ BOI-TVA-DECLA-30-10-30-20250416 : point 260.

⁴² CF exigence n°7

⁴³ CF exigence n°15

⁴⁴ CF exigence n°16

⁴⁵ CF exigence n°8

Vérifier que le mécanisme de purge ne remet pas en cause l'intégrité des données cumulatives et récapitulatives conservées dans le système d'encaissement pour la période dont les données ont été purgées.

IV.7) Traçabilité des opérations

Exigence 15 : Traçabilité des opérations

Le système d'encaissement doit assurer de manière sécurisée la traçabilité des opérations d'archivage, de purge, de restauration des données applicative en enregistrant, dans le système, pour chacune de ces opérations son horodatage et l'identifiant du TPV depuis lequel l'opération est faite.

Exemples de solutions acceptables

Il est possible que la traçabilité de ces opérations soit assurée par un journal d'évènements ou de logs sécurisé selon le même niveau que défini dans l'exigence 8.

Les restaurations « système » ne pouvant être tracées par la couche applicative, les restaurations de données concernées sont les restaurations effectuées depuis l'application/le logiciel d'encaissement.

Vérification documentaire

Vérifier à partir de la description des moyens d'assurer la traçabilité de ces opérations que toutes les opérations de génération d'archive, de purge et de restauration des données sont concernées par le mécanisme.

Vérification fonctionnelle

Après avoir réalisé un ensemble d'opérations d'archivage, de purge et de restauration des données le cas échéant, vérifier sur le système :

- qu'il est possible de recenser l'ensemble des opérations réalisées ;
- qu'un horodatage est mis en place ;
- qu'une association existe entre l'opération et le dispositif qui l'a réalisée
- qu'une modification d'une donnée de traçabilité est détectée par le système.

Vérification de robustesse

Vérifier que les mécanismes de sécurisation des données de traçabilité mis en œuvre sont au moins équivalents en termes de niveau de sécurité que celui atteint dans l'exigence n°8. Vérifier que l'horodatage des opérations repose bien sur un mécanisme fiable et qu'il n'est pas possible de le modifier.

IV.8) Conservation des données

Exigence 16 : Conservation des données

Toutes les données d'encaissement, de traçabilité, ainsi que les preuves de leur inaltérabilité, doivent être conservées pendant 6 ans (à compter de la date de la dernière opération de l'exercice fiscal)⁴⁶.

Les données cumulatives et récapitulatives ainsi que les données de traçabilité⁴⁷ doivent être conservées dans le système⁴⁸.

Les données d'encaissement (hors données cumulatives et récapitulatives et les données de traçabilité) peuvent être conservées soit dans le système lui-même soit dans les archives.

Note spécifique

Les données d'encaissement concernées sont toutes celles définies dans l'exigence n°3, les données d'encaissement correctives définies dans l'exigence n°4, les données du mode école-test définies dans l'exigence n°5, les données cumulatives et récapitulatives définies dans l'exigence n°7 les données de traçabilité d'impression/réimpression définies à l'exigence 9, les données de traçabilité définies dans l'exigence 15 ainsi que les données définies à l'exigence n°18 de traçabilité de la remontée des données des TPV vers le système centralisateur le cas échéant.. Un assujetti ne conservant que le Z de caisse (total cumulatif de la journée) ne respecte pas ses obligations de conservation.

Les vérifications concernant la durée de conservation des données se basent une durée de 7 ans afin de simplifier les interprétations possibles du Livre des Procédures Fiscales et prendre en compte les cas exceptionnels de décalage d'exercice fiscal.

Le système doit permettre de se prémunir des défaillances matérielles d'un support de stockage ou explicitement prévenir l'utilisateur (assujetti) de sa responsabilité quant à l'obligation de conserver ses données conformément à la présente exigence.

Exemples de solutions acceptables :

Il est par exemple possible de mettre en œuvre des processus et/ou des outils de supervision de la capacité mémoire, de faire une estimation de la capacité mémoire nécessaire, d'avertir l'utilisateur de la nécessité de réaliser une purge, augmenter la capacité mémoire si nécessaire ou redonder des sauvegardes sur des supports physiques si possible distants.

Vérification documentaire

Vérifier à partir de la description de la méthode de conservation des données d'encaissement que toutes les données d'encaissement sont bien conservées pendant un délai de 7 ans.

Vérifier pour les données d'encaissement hors données cumulatives, récapitulatives et de

⁴⁶ CF article L.102 B du Livre des Procédures Fiscales

⁴⁷ CF exigence n°15

⁴⁸ CF exigence n°14

traçabilité si la conservation a bien lieu soit dans le système soit dans les archives.

Vérifier que l'éditeur a mis en place des dispositions pour prévenir le risque de saturation mémoire et que le système permet une conservation des données pendant au moins 7 ans.

Vérification fonctionnelle

Vérifier que les dispositions mises en place par l'éditeur pour réduire le risque de saturation mémoire fonctionnent efficacement.

Vérifier pour les données d'encaissement hors données cumulatives, récapitulatives et de traçabilité si la conservation a bien lieu soit dans le système soit dans les archives.

Vérifier que les données cumulatives, récapitulatives et de traçabilité sont bien conservées dans le système lui-même.

Vérification de robustesse

Dans le cas où la conservation des données est assurée par le système et non par les archives, vérifier l'aptitude du système d'encaissement à conserver les données d'encaissement pendant une durée de 6 ans.

Vérifier que cette aptitude repose, par exemple, sur l'utilisation d'un mécanisme assurant le niveau de disponibilité adéquat au niveau du système de stockage (RAID-1 matériel ou logiciel) ou au niveau du système de fichiers (redondance des fichiers sur plusieurs unités de stockage, journalisation et capacité d'autoréparation, etc.). Vérifier que la configuration des mécanismes mis en œuvre permet de s'assurer la bonne conservation et disponibilité des données d'encaissement pendant 7 ans.

Exigence 17 : Conservation des archives

Les archives doivent être conservées de manière à garantir l'intégrité et la disponibilité des données archivées en cas de contrôle pendant 6 ans (à compter de la date de la dernière opération de l'exercice fiscal).

Exemples de solutions acceptables :

Les archives peuvent être conservées, dans le système d'encaissement, en dehors, ou par un tiers archiveur qui se charge d'assurer la conservation des archives. Les mesures nécessaires doivent être prises pour garantir l'intégrité et la disponibilité des archives conformément aux exigences n°12 et 16.

La conservation des archives dans le cloud est possible dans le respect des règles de l'art.

Vérification documentaire

Vérifier à partir de la méthode de conservation des archives comment celles-ci sont conservées de façon à garantir leur intégrité et leur disponibilité avec le même niveau de confiance que pour les exigences n°12 et 16.

Vérification fonctionnelle

Vérifier comment les archives sont conservées de façon à garantir leur intégrité et leur disponibilité avec le même niveau de confiance que pour les exigences n°12 et 16.

Vérification de robustesse

Vérifier l'aptitude du système d'encaissement à conserver les archives intègres et disponibles avec le même niveau de confiance que pour les exigences n°12 et 16.

Exigence 18 : Système centralisateur⁴⁹

Lorsque la conservation des données⁵⁰ est assurée sur un système centralisateur, le système d'encaissement doit prévoir un mécanisme fiable de transfert des données et assurer l'exhaustivité du flux des données transférées, y compris en cas de déconnexion en cours ou passée.

Les déconnexions et modes hors-ligne doivent être paramétrées pour être utilisées pendant une durée réduite.

L'éditeur doit spécifier la durée maximale pour utiliser le système en mode hors ligne.

Le choix de la durée maximale doit être documenté et pertinent compte tenu des modalités d'utilisation du système de caisse.

L'utilisateur du système de caisse doit être notifié que le système fonctionne en mode hors-ligne.

Note spécifique

Un système est dit centralisateur si un ou des TPV qui assurent localement le stockage de l'information avant transmission transmettent les données d'encaissement vers un système central qui en assure la conservation dans le respect de l'exigence n°16 (cas des caisses autonomes remontant périodiquement les données ou qui remontent les données en temps réel tout en prévoyant un système de buffer en cas de déconnexion).

A contrario un système avec une architecture client-serveur où l'interface client n'est qu'une interface graphique, sans stockage temporaire des données, qui permet la communication vers un serveur (cas d'une application web ouverte dans un navigateur par exemple) n'est pas considéré comme un système centralisateur dans la mesure où l'utilisation autonome de l'interface sans connexion avec le serveur est impossible.

Si la conservation des données dans le respect des exigences n° 8 et 16 est assurée par les terminaux cette exigence est non-applicable.

La traçabilité de la remontée des données d'encaissement vise à s'assurer que l'ensemble des données de transaction sont bien remontées y compris en cas de problèmes de

⁴⁹ BOI-TVA-DECLA-30-10-30-20250416: point 210.

⁵⁰ CF exigence n°13

connectivité ou d'erreurs de transmission.

Exemples de solutions acceptables :

Afin de garantir l'exhaustivité du transfert de donnée, il est possible de mettre en place une numérotation incrémentale horodatée des envois et réceptions de données ou une référence au dernier enregistrement envoyé (comme par exemple l'empreinte ou la signature de l'enregistrement), couplé à une identification du TPV source afin de s'assurer qu'aucune donnée n'est manquante.

Afin de garantir l'intégrité des données transférées, il est possible d'utiliser une signature, une empreinte à clé, ou un protocole réseau sécurisé (comme par exemple TLS, IPsec).

Si le système prévoit que les TPV puissent effectuer des transactions de manière autonome en cas de perte de la connexion avec le système centralisateur, les données stockées localement doivent avoir un niveau de sécurité au moins équivalent à celui apporté en réponse à l'exigence 8. De plus, lors du rétablissement de la connexion, le système centralisateur doit s'assurer avoir récupéré toutes les données stockées localement et temporairement par les TPV.

En cas de perte de connexion entre le système centralisateur et les terminaux, il est acceptable que le système centralisateur identifie quels sont les terminaux concernés et depuis quand (date/heure) sans dépasser la durée maximale proposée par l'éditeur.

Vérification documentaire

Si la conservation des données est assurée par les terminaux, vérifier les éléments permettant de démontrer l'inapplicabilité de cette exigence.

Si la conservation des données est assurée par le système centralisateur vérifier à partir de la description complète de ce système que l'exhaustivité de la remontée des données est démontrée. Vérifier que l'éditeur fournit une déclaration explicite d'exhaustivité de la remontée des données d'encaissement.

Vérifier le paramétrage de la durée maximale du mode hors-ligne ainsi que la justification de ce délai.

Vérifier la documentation de la présence sur le système d'un moyen d'information pour l'utilisateur final qu'il est en mode hors-ligne.

Vérification fonctionnelle

Si la conservation des données est assurée par les terminaux, vérifier les éléments permettant de démontrer l'inapplicabilité de cette exigence.

Vérifier la bonne remontée dans le système centralisateur d'un ensemble échantillonné de données d'encaissement.

Vérifier la durée et les causes des déconnexions liées au mode hors-ligne.

Vérifier la présence sur le système d'un moyen d'information pour l'utilisateur final qu'il est en mode hors-ligne.

Vérifier l'identification des opérations réalisées en mode hors-ligne.

Vérifier le nombre de licences identifiées pour les clients finaux dans le cas d'utilisation de licence.

Vérification de robustesse

Dans le cas d'un chiffrage ou d'une signature des envois de données vérifier que le niveau de sécurité est au moins équivalent à celui apporté en réponse à l'exigence n° 8.

Vérifier que l'ensemble des données d'encaissement sont bien stockées et conservées sur le système centralisateur. Vérifier qu'une défaillance dans la transmission des données ou dans la réception des données n'engendre pas un manque ou une donnée erronée dans le système centralisateur.

Vérifier que le mécanisme de protection contre l'altération des envois est d'un niveau de sécurité au moins équivalent à celui permettant de répondre à l'exigence n° 8.

Vérifier qu'en cas de perte de connexion il n'est pas possible d'effectuer indéfiniment des transactions sur les TPV et que le mécanisme est suffisamment robuste pour contrôler que tous les éléments sont bien remontés lors du rétablissement de la connexion.

IV.9) Accès de l'administration fiscale aux données d'encaissement

Exigence 19 : Accès de l'administration fiscale aux données⁵¹

Le système d'encaissement doit prévoir un accès pour l'administration fiscale à l'ensemble des données d'encaissement⁵² enregistrées.

L'éditeur doit fournir un moyen automatisé pour que l'administration fiscale puisse vérifier l'intégrité des données d'encaissement.

L'éditeur doit fournir un manuel utilisateur à destination de l'administration fiscale, en français, détaillant la procédure permettant d'accéder aux données, ainsi qu'un descriptif clair du fonctionnement des outils utilisés pour accéder aux données et en vérifier l'intégrité.

Cet accès ne doit pas remettre en cause la sécurité des données d'encaissement.

Note spécifique :

⁵¹ BOI-TVA-DECLA-30-10-30-20250416 : point 60 & 100.

⁵² Définies dans l'exigence n°3, les données d'encaissement correctives définies dans l'exigence n°4, les données du mode école-test définies dans l'exigence n°5, les données cumulatives et récapitulatives définies dans l'exigence n°7, les données de traçabilité d'impression/réimpression de justificatifs définies dans l'exigence n°9, les données définies dans l'exigence n°15 de traçabilité des opérations de purge, d'archivage et de restauration des données, les données définies dans l'exigence n°18 de traçabilité de la remontée des données des TPV vers le système centralisateur le cas échéant.

Le manuel utilisateur à destination de l'administration fiscale doit être clair et compréhensible par un non-informaticien. Il doit, par ailleurs, détailler la procédure permettant de vérifier que les données n'ont pas été altérées.

Exemples de solutions acceptables :

Il peut être possible d'exploiter le compte gérant, ou un compte dédié à l'administration, pour accéder à l'ensemble des données de l'entreprise, qui peuvent être sous une forme native (fichiers à plat, fichiers XML, etc.) ou une forme interprétée pour des fins de visualisation.

Il est possible de détailler le processus de contact et d'escalade auprès du support si nécessaire dans le manuel à destination de l'administration fiscale. Celui-ci peut être inclus dans le manuel utilisateur ou être un manuel distinct. La structure de la présentation des données (les différents champs) doit être décrite de façon explicite. L'interface utilisateur, les menus, fenêtres et autres fonctionnalités à destination de l'administration fiscale peuvent être décrits dans le manuel à sa destination.

Le manuel à destination de l'administration fiscale peut être inclus dans les archives générées.

Vérification documentaire

Vérifier à partir de la description du moyen d'accès de l'administration fiscale que toutes les données d'encaissement sont accessibles.

Vérifier l'existence et la pertinence du manuel à destination de l'administration fiscale décrivant les moyens et procédures permettant l'accès aux données d'encaissement.

Dans le cas de système de caisse avec des paramètres permettant de modifier/activer/désactiver la conformité française, vérifier la présence des champs, leurs valeurs et l'intégrité des paramétrages pour que le système soit conforme à la réglementation française.

Vérifier l'intégration et la sécurisation des paramétrages du mode hors-ligne.

Vérification fonctionnelle

Vérifier que moyen permettant d'accéder aux données pour l'administration fiscale fonctionne correctement et que toutes les données d'encaissement sont accessibles.

Vérifier que ce moyen ne permet pas de modifier ou supprimer des données d'encaissement. Vérifier que le moyen fourni à l'administration fiscale permet la bonne détection de l'altération (modification, insertion, suppression) des données. Par exemple, modifier une donnée et vérifier que la détection de cette erreur est aisée et immédiate en utilisant le moyen d'accès de l'administration fiscale.

Vérifier que les paramètres de conformité français sont joints aux exports à destination de l'administration fiscale.

Vérifier le nombre de licences identifiées pour les clients finaux dans le cas d'utilisation de licence.

Vérification de robustesse

Vérifier que les modalités d'accès par l'administration ne remettent pas en cause le niveau de sécurité du système d'encaissement.

IV.10) Identification du périmètre fiscal et des versions majeures et mineures

Exigence 20 : Identification du périmètre fiscal

L'éditeur doit définir clairement le périmètre fiscal de son système d'encaissement et lister de façon exhaustive tous les fichiers du code source, des librairies, pilotes et modules impactant les fonctionnalités et exigences énoncées dans le présent référentiel.

Notes spécifiques :

Les fichiers de code source intégrant les fonctionnalités fiscales (sécurisation & inaltérabilité, conservation, archivage, clôture, fonction école, chainage ou signature des données, accès à l'administration fiscale, purge) doivent être listés et une empreinte de ces fichiers sera prise afin de vérifier leur non-modification.

Si une partie du périmètre fiscal est protégé par une configuration spécifique du système d'exploitation, les fichiers de la configuration considérée doivent avoir une identification additionnelle.

Le périmètre non fiscal est dit « périmètre mineur ». Le code source du périmètre mineur doit être disponible aux évaluateurs lors de l'évaluation de robustesse afin de vérifier la cohérence de la définition des périmètres fiscal et mineur.

Exemples de solutions acceptables

La définition exhaustive du périmètre fiscal peut prendre la forme d'un tableau de corrélation entre les 21 exigences du présent référentiel et la liste tous les éléments du code source impliqués.

Sont par exemple inclus dans le périmètre fiscal toutes les fonctions d'enregistrement des données d'encaissement ; de correction/annulation d'une transaction ; les fonctions liées à l'enregistrement et à la sécurisation des données générées par le mode école ; les fonctions de clôture (journalière, mensuelle et annuelle) ; de calcul, d'enregistrement et de sécurisation des données cumulatives et récapitulatives ; de sécurisation et d'inaltérabilité des données d'encaissement ; de sécurisation des justificatifs ; d'archivage ; de sécurisation des archives ; de purge ; de traçabilité des opérations (archivage, purges, clôtures) ; de conservation des données et des archives ; d'accès de l'administration fiscale et de toute autre fonctionnalité/module/pilote/librairie impactant le respect des exigences du présent référentiel.

Il est possible de définir le périmètre fiscal comme étant l'entièreté du code source du système d'encaissement.

Vérification documentaire

Vérifier à partir de la liste des composants du périmètre fiscal que celle-ci est complète afin que l'organisme de certification et l'éditeur n'aient aucun doute sur les portions de code source dont la modification entraîne un changement de version majeure.

Vérification de robustesse

Vérifier par analyse du code source que l'ensemble des fonctionnalités réglementaires (i.e. en lien avec la certification et les exigences du présent référentiel) sont implémentées dans des fichiers de code source inclus dans le périmètre fiscal.

Vérifier par échantillonnage du code source qu'il n'y a pas de fonctionnalités réglementaires dans le périmètre non fiscal (mineur)

Exigence 21 : Identification des versions majeures et mineures

Le système d'encaissement doit être clairement identifié par un numéro de version majeure et un numéro de version mineure inextricablement liés au système d'encaissement.

Ces numéros de version doivent être aisément accessibles depuis l'interface utilisateur standard du système d'encaissement.

Toute modification de code dans le périmètre fiscal ou paramétrage impactant le respect des exigences du présent référentiel doit entraîner une incrémentation du numéro de version majeure.

L'éditeur doit générer et fournir l'empreinte de chaque version majeure.

Note spécifique :

Le numéro de version majeure du système d'encaissement est l'identification du numéro de version du périmètre fiscal du système d'encaissement.

Le numéro de version mineure du système d'encaissement est l'identification du numéro de version du code non inclus dans le périmètre fiscal n'impactant donc pas le respect des exigences du présent référentiel.

Si des fonctions du système d'encaissement peuvent être désactivées par des paramétrages spécifiques, chaque fonction ou variante doit être identifiée séparément.

Le certificat délivré par **BYCYB** porte sur la version majeure du système d'encaissement évaluée et demeure valable pour attester du respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données pour les versions mineures ultérieures à la version mineure évaluée par **BYCYB**.

Il est possible de présenter à la certification un système d'encaissement dont les versions majeure et mineure seraient fixes.

Exemples de solutions acceptables

Les algorithmes suivants sont à l'état de l'art pour réaliser les empreintes des logiciels ou

sous- parties des logiciels dans un but d'identification précise : SHA-2, SHA-3, Whirlpool, Blake.

A contrario les algorithmes suivants sont non acceptables : SHA-1, MD5, CRC16, CRC32 et toutes autres formes de sommes de contrôles non cryptographiques.

Il est possible de faire les empreintes utilisées pour l'identification des versions à partir du binaire ou du code source. L'empreinte peut être stockée à côté du code source.

Le format de numérotation des versions majeures et mineures est libre. Il appartient à l'éditeur de le définir et de l'appliquer.

Dans le cas des systèmes accessibles directement par les clients finaux (e-commerce par exemple), l'affichage du numéro de version du système d'encaissement peut être limité à un profil spécifique (contrôleur fiscal ou administrateur par exemple).

Vérification documentaire

Vérifier à partir de la documentation comment l'identification du système par les numéros de version est créée et comment est inextricablement liée au système lui-même. Vérifier dans la documentation quelles sont les mesures prises pour protéger l'identification du système d'encaissement d'une quelconque falsification.

Vérifier qu'il est décrit dans le manuel utilisateur comment afficher l'identification des versions majeures et mineures du système depuis l'interface utilisateur.

Vérifier que les règles de nomenclature des versions majeures et mineures sont clairement établies et conformes à l'exigence.

Vérifier à partir de la documentation que l'éditeur a fourni le numéro de version majeure et le numéro de version mineure du système d'encaissement évalué.

Vérification fonctionnelle

Vérifier que l'identification du logiciel est visualisée conformément à sa description dans la documentation. Vérifier que l'identification présentée est correcte.

Vérification de robustesse

Vérifier que le mécanisme permettant de générer l'identification du système via les numéros de version majeure et mineure a intégré toutes les parties du système concernées et que celui-ci est fiable, c'est-à-dire qu'il suit les critères de l'annexe B1 du RGS, ou, a minima, est résistant à une attaque par collision (c'est-à-dire qu'il n'est pas possible de forger deux sources distinctes produisant la même empreinte).

Vérifier que les mesures prises pour éviter la falsification sont appropriées par rapport à l'état de l'art.

Vérifier par échantillonnage à partir du journal des versions (« changelog ») ou au différentiel en termes de code entre deux versions que les modifications mineures n'ont pas d'impact sur le respect des exigences du présent référentiel.

Vérifier qu'une empreinte réalisée par l'évaluateur sur le code certifié produit la même

empreinte que celle délivrée par l'éditeur.

CHAPITRE V : ÉLABORATION ET VALIDATION DU RÉFÉRENTIEL

V.1) Comité de marque

V.1.1) Modalités, rôle, et engagements de fonctionnement

Il est constitué un comité de marque des experts et les différentes parties intéressées pour donner un avis sur les règles de certification.

Les attributions du comité de marque sont de:

- donner un avis sur les règles de certification et ses évolutions,
- donner un avis sur les projets d'actions de communication ou de promotion relatifs à la marque.
- donner un avis sur la synthèse de l'ensemble des contrôles et vérifications effectuées.

Le comité de marque se réunit au minimum une fois par an.

Tout membre du comité s'engage :

- à contribuer par son expertise au bon fonctionnement **de la certification LNE système de caisse, à l'élaboration et la mise à jour du référentiel établi par BYCYB.**
- à garder la confidentialité sur l'ensemble des informations à caractère individuel qui lui sont communiquées, et ceci jusqu'à leur publication par **BYCYB**,
- à participer régulièrement aux réunions, et le cas échéant à informer régulièrement son suppléant et lui communiquer les documents,
- à contribuer au développement du référentiel système de caisse **BYCYB**, c'est-à-dire promouvoir les produits ou services certifiés sous la marque.

Le mandat des membres est renouvelable par tacite reconduction.

Afin de préserver la crédibilité et l'efficacité du travail du comité, **BYCYB**, se réserve la possibilité de mettre fin au mandat d'un membre dans les cas suivants :

- non-respect de l'engagement de confidentialité,
- absences répétées aux réunions sans justification,
- non-respect, en général, des engagements précités.

BYCYB assure l'animation et le secrétariat du comité, et recherche le consensus des avis des membres du comité de marque.

L'exercice des fonctions de membre du comité de marque est strictement personnel. Toutefois, en cas d'absence, un suppléant est désigné et nommé dans les mêmes conditions que les titulaires.

BYCYB rédige le compte rendu de la réunion du comité, faisant apparaître les observations et propositions formulées, ainsi que toute position contraire à l'avis émis par le comité. Ce compte rendu est adressé à tous les membres du comité de marque.

Dans le cadre de la révision du présent référentiel de certification, **BYCYB** organise la consultation et la validation du référentiel de certification avec notamment consultation de la DGFIP en tant que partie prenante.

V.1.2) Composition du comité

Le comité de marque est composé d'une représentation des parties intéressées associées à la certification des systèmes d'encaissement. La liste des membres du comité détaillée ci-dessous est indicative, non exhaustive et peut être modifiée autant que de besoin.

Le LNE est membre de droit du comité.

La liste des membres du comité de marque est tenue et mise à jour par **BYCYB**. Le comité est composé comme suit :

Organisme certificateur

- Le(s) représentant(s) **de BYCYB** – Département certification produits et technologies de l'information.

Organisme certifié :

- Au moins 3 représentants des éditeurs des systèmes d'encaissement et de facturation.

Utilisateurs

- Au moins 2 représentants des utilisateurs.

V.1.3) Groupe de travail

Pour la conduite de certains travaux ponctuels, d'ordre technique et ne nécessitant pas la convocation de l'ensemble des membres du comité de marque, il peut être créé un groupe de travail dont les membres sont désignés nominativement et choisis parmi ceux du comité de marque. Dans le cas d'un groupe de travail, il peut être fait appel à des professionnels ou des personnalités extérieures au comité.

Les missions de ce groupe de travail sont précisées par le comité de marque ; ses attributions seront généralement limitées à l'élaboration de projets, de propositions ou à la fourniture de compléments d'information sur un sujet donné pour le compte du comité de marque.

V.2) Modalités d'élaboration et de validation du référentiel

Le présent référentiel a été élaboré par **BYCYB** et approuvé par le LNE.

Sa rédaction a été faite conformément aux exigences de la loi du 4 août 2008 et du décret du 19 décembre 2008 régissant la certification des produits et des services. À ce titre et d'après l'article L433-3 et suivants et R433-1 et -2 du code de la consommation, le référentiel de certification est un document technique définissant les caractéristiques que doit présenter un produit, un service ou une combinaison de produits et de services, et les modalités de contrôle de la conformité à ces caractéristiques.

Pour la validation de ce référentiel, **BYCYB** a la responsabilité :

- d'identifier les parties intéressées concernées ;
- de s'assurer de la pertinence des parties intéressées sélectionnées ;
- de s'assurer de leur représentativité, sans prédominance de l'une d'entre elles ;
- de recueillir leur point de vue.

Sur la base du retour d'expérience, le référentiel est passé en revue au sein d'un comité de marque spécifiquement constitué, intégrant l'ensemble des parties intéressées. Son approbation est effectuée selon la même méthodologie que la première version.

V.3) Normes et documents de référence

- Norme NF EN ISO 9001:2015 : Systèmes de management de la qualité – Exigences.
- Norme NF EN ISO 19600:2014 : Systèmes de management de la conformité – Lignes directrices
- Loi n° 2015-1785 du 29 décembre 2015 de finances pour 2016 – Article 88, modifiée par la loi n° 2017-1837 article 105
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
- Code de la consommation – version du 1^{er} janvier 2019 – articles L433-3 à L433-11, articles R433-1 et R433-2
- Code général des impôts – version du 1^{er} janvier 2019 – articles 286, 1770 duodecimes
- Livre des procédures fiscales – version du 1^{er} janvier 2019 – articles L 16-0 BA, L47 A, L80 O, L96 J, L102 B, L102 D
- Arrêté du 29 juillet 2013 portant modification des dispositions de l'article A. 47 A-1 du livre des procédures fiscales relatif aux normes de copies des fichiers sur support informatique
- **BOI-TVA-DECLA-30-10-30-20250416** : Obligation d'utilisation de logiciels ou systèmes de caisse certifiés et Suppression de la possibilité de justifier du respect de l'obligation prévue au 3° bis du I de l'article 286 du CGI par la production d'une attestation individuelle délivrée par l'éditeur (loi n° 2025-127 du 14 février 2025 de finances pour 2025, art. 43)
- BOI-CF-COM-10-80-20160803 : Droit de communication auprès de diverses personnes
- BOI-BIC-DECLA-30-10-20-40-20131213 : Conservation et représentation des livres, documents et pièces comptables dans le cadre d'une comptabilité informatisée
- BOI-CF-IOR-60-40-20131213 : Contrôle des comptabilités informatisées
- Référentiel général de sécurité version 2.0 –Annexe B1 – Mécanismes cryptographiques – version 2.03 du 21 février 2014

CHAPITRE VI : RECOURS ET TRAITEMENT DES PLAINTES

VI.1) Recours contre décision

Le titulaire de la certification peut contester la décision prise par courrier avec accusé réception.

Dans un premier temps, **BYCYB** procède au réexamen du dossier au vu des éléments factuels motivant le recours. Il notifie le maintien ou la nouvelle décision au demandeur dans un délai de 15 jours ouvrés à réception du recours.

Dans le cas où le demandeur désire maintenir son recours contre décision, il le notifie à **BYCYB** par lettre recommandée avec accusé réception dans un délai de 15 jours ouvrés. Ce recours, non suspensif de la décision de **BYCYB**, doit être motivé. Il est instruit par **BYCYB** dans les 21 jours ouvrés suivant sa réception et donne lieu, lorsqu'il concerne la décision de certification, à examen par le comité de lecture. **BYCYB** informe l'auteur du recours, du maintien ou non de sa décision.

En cas de maintien du recours après instruction et soumission au comité de marque pour avis, le recours est présenté au Comité de Certification et de Préservation de l'Impartialité de **BYCYB**, qui après examen, propose ses conclusions. La décision finale est notifiée par **BYCYB** à L'Entreprise.

Toute contestation ultérieure peut être soumise à l'arbitrage de la direction compétente du Ministère chargé de l'Industrie ou est portée devant les tribunaux compétents.

VI.2) Traitement des plaintes

Toute plainte concernant des produits fait l'objet d'un examen par **BYCYB** afin de confirmer si la plainte concerne effectivement des produits certifiés. L'entité formulant une plainte doit étayer celle-ci en fournissant des preuves factuelles.

A réception de celles-ci, **BYCYB** les examine et le cas échéant contacte l'entreprise concernée.

L'Entreprise concernée doit alors informer **BYCYB** des suites apportées et tenir à disposition de **BYCYB**, les enregistrements relatifs à la plainte ainsi qu'aux actions entreprises pour la résoudre. La vérification de la mise en place des actions annoncées peut faire l'objet d'examens supplémentaires à la charge de l'Entreprise.

Dans le cadre du suivi de l'Entreprise, **BYCYB** examine les enregistrements relatifs aux plaintes et réclamations et vérifie que les corrections et actions correctives appropriées ont été entreprises.

CHAPITRE VII : ANNEXES

VII.1) Lexique

Archivage	La fonctionnalité d'archivage, à destination des utilisateurs, a pour objet d'exporter, en garantissant la date de création de l'archive, les données d'encaissement figées dans un format ouvert afin de se prémunir d'une perte des données suites à un problème matériel, une faille de sécurité, un changement de système d'encaissement. Elle ne doit pas être confondue avec seulement une solution de sauvegarde à long terme des données. Il s'agit d'un moyen pour l'assujetti de pouvoir conserver indépendamment du système d'encaissement ses données d'encaissement et pouvoir les communiquer à l'administration fiscale en cas de contrôle.
Archive	Fichier au format ouvert généré par la fonctionnalité d'archivage contenant les données d'encaissement d'une période définie. L'archive ne peut contenir de données d'encaissement sur une période supérieure à un an ou un exercice fiscal.
Authenticité	Caractéristique d'une donnée dont le système est en mesure de vérifier l'identité de l'auteur. Elle peut être assurée grâce aux mécanismes d'empreinte à clé ou de signature.
Chainage	Algorithme consistant à faire dépendre la preuve d'intégrité d'une donnée, de la preuve d'intégrité de la donnée précédente, constituant ainsi une preuve de l'intégrité de l'ensemble des données. Ce mécanisme ne garantit pas l'intégrité du dernier élément et ne permet pas de compter le nombre d'éléments (maillons) manquants lorsque la chaîne est rompue. La preuve d'intégrité peut également être une preuve d'authenticité afin de garantir en plus l'authenticité de la chaîne.
Chiffrage	Évaluation financière, ou action d'écrire ou transcrire en chiffres. À ne pas confondre avec chiffrement.
Chiffrement	Mécanisme cryptographique permettant de garantir la confidentialité de données, en utilisant un chiffre (dans le sens de code secret). Le chiffrement des données n'est pas requis par ce référentiel. À ne pas confondre avec chiffrage.
Clés privées et publiques	Une signature numérique est générée à partir d'une clé privée, qui est un secret cryptographique, et d'un document à signer. La vérification d'une signature est effectuée à partir du document originel et de la clé publique associée au signataire. Connaître une clé publique ne permet pas de retrouver la clé privée correspondante.

Clôture	Fonctionnalité, manuelle ou automatique, offerte par le système d'encaissement qui pour objet de clôturer une période journalière, mensuelle ou annuelle, c'est-à-dire rendre impossible l'enregistrement de nouvelles transactions, de modifier ou d'annuler une transaction sur une période clôturée.
Confidentialité	Caractéristique d'une information ou d'un système visant à s'assurer que leur accès n'est strictement possible qu'aux personnes autorisées. La confidentialité n'est pas requise dans le cadre du référentiel. Elle peut être assurée grâce au chiffrement.
Cryptage	Insérer ou masquer un sens caché dans un texte ou propos, volontairement ou non. Exemple : « décrypter un discours politique ». Pour l'anglicisme, voir chiffrement.
Données d'encaissement	Les données d'encaissement correspondent à toutes les données définies à l'exigence n°3, les données d'encaissement correctives définies dans l'exigence n°4, les données du mode école-test définies dans l'exigence n°5 ainsi que les données cumulatives et récapitulatives définies dans l'exigence n°7 ainsi que les données de traçabilité des impressions et réimpressions de justificatifs définies dans l'exigence n°9
Donnée élémentaire	Donnée qui n'est pas obtenue par calcul à partir d'autres données. Toute donnée élémentaire qui concourt à la constitution d'une écriture comptable, à la justification d'un événement ou d'une situation transcrite dans les livres, registres, documents, pièces et déclarations est visée par le droit de contrôle de l'administration fiscale.
Editeur	Personne qui détient le code source du système d'encaissement et qui a la maîtrise de la modification des paramètres impactant les conditions de sécurisation, conservation et archivage des données d'encaissement de celui-ci.
Empreinte / hash / condensat	Résultat d'une fonction qui associe à une donnée de taille arbitraire une donnée de taille fixe. Lorsque l'empreinte est de qualité cryptographique, il n'est pas faisable de calculer l'inverse de cette fonction.
Empreinte à clé	Empreinte cryptographique réalisée en combinant les données sources à un secret d'authentification. Cela permet d'assurer que seul le détenteur du secret peut générer et vérifier une empreinte. Une empreinte à clé permet de garantir l'intégrité d'un document et d'en assurer l'authenticité, sans pouvoir distinguer les identités des détenteurs du secret.

Fonctionnalité de caisse	Fonctionnalité qui consiste à mémoriser et à enregistrer extra-comptablement des paiements reçus en contrepartie d'une vente (de produits ou de services). Si le paiement déclenche concomitamment, automatiquement, obligatoirement, instantanément et sans intervention humaine la passation d'une écriture comptable la fonctionnalité n'est pas considéré comme une fonctionnalité de caisse mais comme une fonctionnalité d'écriture comptable.
Horodatage	Valeur de temps unique croissante monotone indiquant la date et l'heure à laquelle un événement s'est produit. Ces données sont présentées dans un format cohérent, facilitant la comparaison de deux enregistrements différents et le traçage dans le temps.
Imputabilité	Possibilité d'attribuer la responsabilité d'un fait à une personne.
Inaltérabilité	Caractéristique d'un système dont rien ne peut changer les données enregistrées sans traçabilité (i.e. sans que le système ne le détecte). Une altération des données constitue une atteinte à leur intégrité et à leur authenticité.
Intégrité	Caractéristique de données n'ayant subi aucune modification ou destruction, volontaire ou accidentelle.
Journalisation	Enregistrement séquentiel d'événements affectant un processus particulier. C'est un moyen d'assurer la traçabilité des événements.
Justificatif / pièce justificative	Document regroupant des données permettant de justifier le détail de la commande, des ventes, des achats et du mode de paiement d'un produit ou d'une prestation.
Logiciel de facturation	Système informatique permettant d'émettre des factures entre assujettis à la TVA, contenant les mentions obligatoires prévues à l'article 242 nonies A de l'annexe II au CGI et respectant les conditions de l'article 289 du CGI
Logiciel libre	Logiciel dont les utilisateurs ont un libre usage, une libre étude, une libre modification et une libre distribution. Ces libertés permettent aux utilisateurs d'adapter le logiciel à leurs besoins spécifiques. [Source : BOI-TVA-DECLA-30-10-30]
Mandataire	Personne morale ou physique implantée dans l'Espace Economique Européen (E.E.E) qui a une fonction de représentation du titulaire hors E.E.E et dispose d'un mandat écrit de celui-ci lui signifiant qu'il peut agir en son nom dans le processus de certification suivant les dispositions des présentes règles. Le mandataire peut également être distributeur ou importateur des

	produits certifiés, ses différentes fonctions sont alors clairement identifiées.
Mode/environnement école	Mode ou environnement optionnel d'un système d'encaissement permettant de générer ou de simuler des données afin d'enregistrer des transactions fictives à des fins de tests ou de formation.
Périmètre fiscal	Ensemble exhaustif du code source, des bibliothèques, pilotes et modules impactant les fonctionnalités et exigences énoncées dans le présent référentiel.
Preuve d'authenticité	Donnée qui permet de prouver l'authenticité d'un document. Voir empreinte à clé, signature.
Preuve d'intégrité	Donnée qui permet de prouver l'intégrité d'un document. Voir empreinte, signature.
Purge	Suppression irréversible des données enregistrées sur un système.
Redondance	Méthode consistant à dupliquer tout ou partie de données pour pouvoir les restaurer à leur état d'origine en cas d'altération. Elle peut assurer la disponibilité de l'information qui est la capacité d'un système à rester fonctionnel ou à garder les données accessibles dans le temps.
Secret cryptographique	Un secret cryptographique est une donnée confidentielle utilisée pour chiffrer ou authentifier un document. La confidentialité de ce secret permet de garantir les propriétés (confidentialité ou authenticité) du mécanisme qui l'emploie. Pour être qualifié de cryptographiquement sûr, ce secret doit être généré aléatoirement, ne pas être utilisé pour différents usages, et avoir une taille définie par le mécanisme qui l'emploie.
Signature	Une signature numérique est un mécanisme qui permet de garantir l'intégrité d'un document et d'en assurer l'authenticité. À la différence d'une empreinte à clé, le vérifieur n'a pas besoin de connaître un secret pour vérifier l'authenticité et il ne peut pas usurper l'identité du signataire.
Système d'encaissement	Un système d'encaissement est un système informatique doté d'une fonctionnalité de caisse.
Titulaire	Personne morale qui assure la maîtrise et/ou la responsabilité du respect de l'ensemble des exigences définies dans les présentes règles de certification. Ces exigences couvrent au moins les étapes suivantes : conception, fabrication, assemblage, contrôle qualité, marquage, conditionnement ainsi que la mise sur le marché et précisent les points critiques des différentes étapes. Certaines de ces activités peuvent être réalisées sur le site du titulaire ou sur un

	<p>autre site par le titulaire lui-même ou par une autre structure avec laquelle il y a une délégation de responsabilités. Cela inclut par exemple des filiales ou des sous-traitants. Quel que soit le site ou le niveau d'externalisation, il importe que le titulaire soit en mesure de présenter l'intégralité des preuves de conformité au référentiel. Le paragraphe 310 du BOI-TVA-DECLA-30-10-30-20160803 indique que le titulaire est l'éditeur du système de caisse. Lorsque le titulaire n'est pas établi dans la communauté européenne, il doit obligatoirement désigner un mandataire.</p>
Total cumulatif / cumul de période	<p>Cumul du chiffre d'affaires décompté depuis l'ouverture de la période concernée. Il s'agit d'un compteur initialisé à 0 à l'ouverture de la période (ou clôture de la période précédente) et dont la valeur est stockée au moment de la fin de la période.</p>
Total perpétuel / cumul perpétuel	<p>Cumul du chiffre d'affaires décompté depuis l'initialisation du système d'encaissement. Il s'agit d'un compteur ne se remettant jamais à, qui n'est pas directement lié à une période mais dont la valeur est enregistrée à un instant t : au moment de chaque clôture (journalière, mensuelle ou annuelle).</p>
TPV	<p>Terminal Point de Vente identifié par un numéro unique (n° de terminal, de caisse, de balance etc.). Un terminal assure l'enregistrement des données d'encaissement localement, temporairement (en attendant le transfert des données vers un système centralisateur) ou dans le respect avec l'exigence n° 16 concernant la conservation des données pendant la durée de 6 ans à partir de la date de la dernière transaction enregistrée sur l'exercice fiscal courant.</p>
Traçabilité	<p>Aptitude à retrouver l'historique, la mise en œuvre ou l'emplacement de ce qui est examiné. Elle est liée à la journalisation et à l'imputabilité.</p>
X	<p>Terme provenant des anciennes caisses enregistreuses actionnées par clé. Lecture simple du chiffre d'affaires de la journée, pouvant être réalisé à tout moment et sans impact sur les données de transactions enregistrées.</p>
Z	<p>Terme provenant des anciennes caisses enregistreuses actionnées par clé. Clôture de caisse de la journée : plus aucune modification des données de transactions enregistrées depuis le dernier Z n'est possible, seuls sont conservés les soldes de caisse (par exemple les espèces encore présentes dans le tiroir-caisse).</p>