LNE
Le progrès, une passion à partager

Référentiel de certification des systèmes de caisse

Réf. rédacteur : LNE/PCI/QSE/AS

Révision n° 1.2 – décembre 2016

Approbation LNE : 20/12/2016

1ère mise en application : 03/01/2017

Laboratoire national de métrologie et d'essais
Établissement public à caractère industriel et commercial • Siège social : 1, rue Gaston Boissier - 75724 Paris Cedex 15 • Tél. : 01 40 43 37 00
Fax : 01 40 43 37 37 • E-mail : info@lne.fr • Internet : www.lne.fr • Siret : 313 320 244 00012 • NAF : 7120B • TVA : FR 92 313 320 244
CRCA PARIS C.AFF.RENNES - IBAN : FR76 1820 6002 8058 3819 5600 104 - BIC : AGRIFRPP882

Table des matières

Révisions du document

Version	Date	Motif de la mise à jour
1	29/11/2016	Version initiale
1.1	07/12/2016	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 1er comité de marque du 06/12/2016.
1.2	12/12/2016	Ajustement de la composition du comité de marque (V.4). Ajustement de la procédure de recours et de plainte (VI).

Chapitre I : Objet et domaine d'application

I.1/ Objet

Afin de lutter contre la fraude à la TVA liée à l'utilisation de logiciels permettant la dissimulation de recettes, la loi de finances pour 2016 a instauré l'obligation à partir du 1er janvier 2018 pour les commerçants et autres professionnels assujettis à la TVA d'enregistrer les paiements de leurs clients au moyen d'un logiciel de comptabilité ou d'un système de caisse sécurisé. Le but est de rendre impossible la fraude qui consiste à reconstituer par un logiciel frauduleux des tickets de caisse pour soustraire des paiements en espèces des recettes de la comptabilité.

A cette fin, des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage sont fixées. Le respect de ces conditions se voit formalisé soit par une attestation individuelle délivrée par l'éditeur, soit par un certificat délivré par un organisme accrédité.

Le présent référentiel décrit les modalités de certification des systèmes de caisse ; 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 publiques BOI-TVA-DECLA-30-10-30-20160803.

Ce référentiel présente :

- le champ et les conditions d'application de la certification de produit ;
- les caractéristiques certifiées ;
- les modalités d'évaluation par l'organisme certificateur de la conformité du produit certifié ;
- la nature et le mode de communication relatifs aux caractéristiques certifiées.

I.2/ Modalités d'élaboration et de validation du référentiel

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.

La certification est un acte volontaire qui peut procurer aux entreprises un avantage concurrentiel. C'est un outil de compétitivité qui renforce la confiance dans leurs relations avec leurs clients en leur garantissant, via le certificat, l'atteinte d'engagements de service et de conformité du produit. Elle doit donc être délivrée par des organismes certificateurs indépendants des entreprises certifiées ainsi que des pouvoirs publics. Elle est accessible à tout professionnel du secteur d'activité répondant aux critères des référentiels de certification.

Le présent référentiel a été élaboré par le LNE, à partir des documents de travail issus des réunions du groupe d'experts et du comité, comprenant les fabricants des systèmes de caisse, les éditeurs de logiciel d'encaissement, les donneurs d'ordres, les utilisateurs.

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, le LNE 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.

I.3/ Domaine d'application

La certification concerne les systèmes d'information dotés d'un ou plusieurs logiciels permettant l'enregistrement des opérations d'encaissement. Il s'agit de tous les systèmes informatisés comptables, de tous les systèmes de gestion commerciale et d'encaissement qui enregistrent des données ou informations concourant à la détermination du résultat comptable, et plus généralement, de tous les systèmes de caisse, c'est-à-dire de tous les matériels permettant l'enregistrement des opérations d'encaissement, notamment de ventes et de prestations de services. Dans la suite du document, le terme générique « système de caisse » est utilisé.

Est concerné l'encaissement en commerce de bouche, en restauration, en hôtellerie, dans la grande distribution, en commerce de détail (coiffure, pressing, soins esthétiques), en négoce inter-entreprises, etc.

En revanche, on exclut du domaine d'application de la certification les logiciels servant au support des services après-vente (rapports de maintenance, rapports de services, génération de bons d'intervention, etc.) ainsi que les logiciels de comptabilité pure ou les applications monétiques (terminaux de paiement électroniques par exemple).

Les bénéficiaires de la certification sont les éditeurs et développeurs de logiciels d'encaissement, les fabricants de caisse, les fabricants d'imprimantes dites fiscales ou encore les fabricants d'instruments de pesage utilisés pour réaliser des encaissements ou plus largement les fabricants de dispositifs d'encaissement intégrés dans des instruments de mesure réglementés.

Les entreprises, pour les produits certifiés, s'engagent à réaliser exclusivement des systèmes de caisse conformes au présent référentiel de certification. Il est également précisé que tous les systèmes de caisse certifiés doivent satisfaire aux dispositions réglementaires qui leur sont applicables, indépendamment de toute demande de certification (par exemple en ce qui concerne la contrefaçon, les obligations de conformité et de sécurité, le marquage CE, etc.).

Les entreprises certifiées sont seules responsables de la conformité de leurs produits, les contrôles du LNE ne pouvant se substituer à leurs responsabilités.

I.4/ Normes et documents de référence

- Norme NF X50-067 (avril 2008) : Elaboration d'un référentiel de certification de produit ou de service ou d'une combinaison de produit et de service.
- Norme NF EN ISO 9001 (novembre 2008 et octobre 2015) : Systèmes de management de la qualité – Exigences.

- Loi n° 2015-1785 du 29 décembre 2015 de finances pour 2016 – Article 88

- Code de la consommation – version à venir au 1er janvier 2018 – articles L433-3 à L433-11, articles R433-1 et R433-2

- Code général des impôts – version à venir au 1er janvier 2018 – articles 286, 1770 duodecies

- Livre des procédures fiscales – version à venir au 1er janvier 2018 – 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-30-10-30-20160803 : Obligation d'utiliser un logiciel de comptabilité ou de gestion ou un système de caisse satisfaisant à des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données en vue du contrôle de l'administration fiscale
- 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 – notamment Annexe B1 – Mécanismes cryptographiques – version 2.03 du 21 février 2014

Chapitre II : Exigences applicables aux systèmes d'encaissement

II.1/ Caractéristiques certifiées

L'article 88 de la loi n° 2015-1785 et le BOI-TVA-DECLA-30-10-30-20160803 fixe quatre conditions auxquelles doivent répondre les systèmes de caisse :

- condition d'inaltérabilité ;
- condition de sécurisation ;
- condition de conservation ;
- condition d'archivage.

A ces quatre conditions techniques s'ajoutent la caractérisation des versions et la documentation à gérer, ainsi que la gestion du système de management de la qualité pour assurer la production de systèmes de caisse conformes à la version certifiée.

II.2/ Exigences techniques

Ce chapitre présente les caractéristiques certifiées, les méthodes de contrôle ainsi que les moyens qui doivent être mis en œuvre par le prestataire certifié pour y répondre (en y incluant des exemples de solutions acceptables).

Les méthodes de contrôle sont basées sur :

- l'évaluation de l'organisation prise par le fabricant ou le distributeur du système (vérifications documentaires, entretiens avec le personnel, etc.) pour garantir la disponibilité des informations et produits demandés par la réglementation ainsi que la conformité des produits à ceux certifier,

– des vérifications fonctionnelles et de robustesse sur des échantillons (systèmes candidats à la certification ou certifiés).

Les données concernées sont toutes les données :

– qui concourent directement ou indirectement à la réalisation d'une transaction ;
– liées à la réception du paiement immédiat ou différé ;
– permettant de tracer la transaction et la réception du paiement.

Pour chaque condition sont donnés, lorsque c'est applicable : la documentation requise, les vérifications à partir de la documentation, les vérifications fonctionnelles, des exemples de solutions acceptables, les modalités de réalisation des vérifications de robustesse (incluant également les outils de tests nécessaires, les produits et documents que le fabricant devra fournir, etc.), ainsi que les vérifications de la robustesse des mesures prises par l'éditeur pour répondre à l'exigence.

Dans la ligne « condition », les numéros qui précèdent les exigences sont les numéros de paragraphe du BOI-TVA-DECLA-30-10-30-20160803.

II.2.1 / Conditions préliminaires

Condition 1

La documentation réglementaire est l'ensemble des documents qui retrace les différentes phases du processus de conception, d'exploitation et de maintenance du système informatique. Elle comprend notamment :

- le dossier de conception générale ;
- le dossier des spécifications fonctionnelles ;
- les dossiers technique, organisationnel et d'architecture ;
- le dossier de maintenance ;
- le dossier d'exploitation ;
- le dossier utilisateur ;
- le code source.

Ces documents peuvent être conservés sur tout support, rédigés en français, au choix de la personne tenue de les présenter (support papier ou support informatique).

En application de l'article L. 102 D du LPF, ces renseignements doivent être conservés jusqu'à l'expiration de la troisième année suivant celle au cours de laquelle le logiciel ou le système de caisse a cessé d'être diffusé (BOI-CF-COM-10-10-30-10 au I § 55).
[Source : BOI - CF-COM-10-80-20160803 paragraphe 200]

Notes spécifiques

Le droit de communication exercé auprès d'une personne ne s'applique que pour la documentation se rattachant au produit qu'elle a conçu ou édité.

Lorsqu'une personne n'est intervenue techniquement que sur une partie des fonctionnalités du produit, le droit de communication exercé auprès de cette personne ne s'applique que pour la documentation se rattachant aux fonctionnalités qu'elle a développées sur ce produit et aux autres fonctionnalités directement ou indirectement impactées par ces développements.

Les commentaires du code source sont considérés au même titre que le code source lui-même et

peuvent donc être rédigés dans une autre langue que le français.

Il n'est pas requis de transmettre au LNE l'intégralité du code source avant l'évaluation ; néanmoins, au minimum une signature du code source est nécessaire.

Documentation requise

Documentation réglementaire (citée par le BOI-CF-COM-10-80) :

- le dossier de conception générale ;
- le dossier des spécifications fonctionnelles ;
- les dossiers : technique, organisationnel et d'architecture ;
- le dossier de maintenance ;
- le dossier d'exploitation ;
- le dossier utilisateur ;
- le code source.

Documentation complémentaire :

- une description du produit dans son ensemble ;
- une description de la portion du logiciel concernée par la présente certification ;
- une identification non ambigüe du logiciel ;
- une description des algorithmes utilisés pour la réalisation des fonctions d'intégrité, de sécurisation et d'inaltérabilité ;
- une description de l'interface utilisateur, des menus et des boîtes de dialogues ;
- une vue d'ensemble du matériel associé au logiciel ou au système, comme des schémas de principe, type d'ordinateur, réseau, etc. ;
- une vue d'ensemble des parties du système d'exploitation utilisé, des aspects liés à la sécurité du système d'exploitation utilisé, comme la protection, les comptes utilisateurs, les privilèges, ainsi que les outils, logiciels, méthodes ou algorithmes utilisés pour renforcer la sécurité ;
- le manuel d'utilisation ;
- les spécifications de conception (incluant l'ensemble des exigences fonctionnelles, de performance, de sécurité, techniques, architecturales,...) ;
- les plans et rapports de test (revue de code, test unitaire, test d'intégration, vérification fonctionnelles, vérification/validation du logiciel, vérification/validation du produit dans son ensemble).

La documentation complémentaire peut être présentée en français ou en anglais.

L'ensemble des documents sont sur support papier ou informatique ; ils peuvent être séparés selon les catégories ci-dessus ou regroupés en un ou plusieurs documents.

Les descriptions portent sur les parties logicielles concernées par la certification et ont pour but de décrire comment le demandeur de la certification répond à chaque exigence.

Le dossier de maintenance est destiné à identifier le suivi des évolutions du produit, les licences, la méthode de mise à jour d'une version, ou encore la procédure de mise à jour de version chez le client. Le dossier d'exploitation peut concerner le paramétrage du système et intégrer le manuel de programmation. Enfin, le plan de test doit permettre de déterminer comment l'éditeur du logiciel a vérifié une exigence du présent référentiel.

Vérification à partir de la documentation

Vérifier que la documentation réglementaire existe et couvre tous les points requis, y compris la présence de la signature du code source.

Vérifier que les documents réglementaires sont bien rédigés en français.

Vérifier que des dispositions existent dans l'entreprise pour que les documents réglementaires requis (par le BOFIP BOI-CF-COM-10-80-20160803 § 200) soient bien conservés jusqu'à l'expiration de la 3ème année suivant celle au cours laquelle le logiciel ou le système de caisse a cessé d'être diffusé.

Vérification fonctionnelle

Vérifier qu'un échantillon des documents relatifs à un logiciel ou un système toujours en cours de diffusion est effectivement disponible.

Si l'entreprise a un logiciel ou un système qui a cessé d'être diffusé depuis 3 ans ou moins, vérifier qu'un échantillon des documents est effectivement disponible.

Dans l'hypothèse où le code ou une sous-partie du code n'est pas disponible chez l'éditeur (emploi de bibliothèques tierces déjà compilées par exemple), il peut être possible de faire une évaluation sur la base du binaire et de la documentation, dès lors que le binaire n'est pas obfusqué et que la documentation associée précise clairement les API utilisées et les différents paramètres employés.

Exemples de solutions acceptables

/

Modalités de réalisation des vérifications de robustesse

Non applicable

Vérification de la robustesse

Non applicable

Condition 2

Identification du logiciel :
Le logiciel du système de caisse doit être clairement identifié par une version fixe ou une version majeure selon les principes ci-dessous.
340
On entend par version majeure d'un logiciel ou système toute nouvelle version de ce système ou logiciel obtenue en ayant modifié, dans la précédente version de ce logiciel ou système, un ou plusieurs paramètres impactant le respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données.
A l'inverse, on entend par version mineure toute version de ce logiciel ou système obtenue sans que les paramètres impactant le respect des conditions précitées aient été modifiés par rapport à la précédente version de ce logiciel ou système.
380 (pris pour référence pour les certifications)
Il sera admis que le certificat demeure valable pour attester du respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données par les versions mineures ultérieures du logiciel ou système :

- si ce certificat identifie clairement la racine de la dernière version majeure à sa date d'émission et les subdivisions de cette racine qui sont ou seront utilisées pour l'identification des versions mineures ultérieures ;
- et si l'éditeur s'engage à n'utiliser ces subdivisions que pour l'identification des versions mineures ultérieures, à l'exclusion de toute version majeure.

Notes spécifiques

1. L'identification doit inclure les pilotes spécialement programmés pour une tâche spécifique impactant le respect des conditions d'inaltérabilité, de sécurisation, de conservation, et d'archivage des données ainsi les pilotes de bas niveau (comme les pilotes vidéo, les pilotes des disques, etc.) impactant le respect des conditions d'inaltérabilité, de sécurisation, de conservation, et d'archivage des données.
2. Si les fonctions impactant le respect des conditions d'inaltérabilité, de sécurisation, de conservation, et d'archivage des données et les comptes associés sont protégées par une configuration spécifique du système d'exploitation, les fichiers de la configuration considérée doivent avoir une identification additionnelle.
3. L'identification du logiciel doit être aisément affichable lors d'une vérification ou d'une inspection (facilement signifie grâce à une interface utilisateur standard, sans outil additionnel).

4. Les identifications peuvent s'appliquer à différents niveaux, comme des programmes complets, des modules, des fonctions, etc.
5. Si les fonctions du logiciel peuvent être désactivées par des paramètres spécifiques, chaque fonction ou variante doit être identifiée séparément. Autrement, le progiciel entier devrait être identifié dans son ensemble.

Documentation requise

La documentation doit établir la liste des identifications du logiciel. Elle doit également expliquer comment l'identification du logiciel est créée et comment elle est inextricablement liée au logiciel lui-même. La documentation doit aussi préciser la manière dont on peut accéder à l'identification sur l'écran et comment elle est structurée pour différencier les changements de versions nécessitant ou non un examen.

Les documents doivent indiquer les mesures prises pour protéger l'identification du logiciel d'une quelconque falsification.

Vérification à partir de la documentation

Examiner la documentation décrivant comment l'identification du logiciel est générée et affichée.

Vérifier que tous les programmes possédant des fonctions ou des paramètres impactant le respect des conditions d'inaltérabilité, de sécurisation, de conservation, et d'archivage des données sont clairement identifiés et décrits afin que l'organisme de certification et l'éditeur n'aient aucun doute sur les fonctions dont la modification entraine un passage en version majeure.

Vérifier que le fabricant a fourni une valeur nominale de l'identification (numéro de version et somme de contrôle fonctionnelle à indiquer dans le rapport d'évaluation).

Vérification fonctionnelle

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

Vérifier que l'algorithme permettant de générer l'identification a intégré toutes les parties logicielles concernées. Vérifier que l'algorithme est utilisé correctement.

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

Exemples de solutions acceptables

Exemples d'algorithmes 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.

Exemples d'algorithmes non considérés comme intrinsèquement robustes par le RGS de l'ANSSI mais suffisants pour réaliser les empreintes des logiciels ou sous-parties des logiciels dans un but d'identification précise : SHA-1, MD5.

Exemples d'algorithmes non acceptables : CRC16, CRC32 et toutes autres formes de sommes de contrôles non cryptographiques.

Les empreintes utilisées pour l'identification des versions doivent idéalement être faites à partir du binaire mais une empreinte faite à partir du code source est également acceptable. L'empreinte peut être stockée à côté du code source.

Modalités de réalisation des vérifications de robustesse

Accès au code source de plusieurs versions mineures successives.
Accès au journal des versions ("changelog").

Vérification de la robustesse

Vérifier que les algorithmes employés pour l'identification précise des logiciels ou sous-parties des logiciels sont suffisamment robustes, c'est-à-dire qu'ils suivent les critères de l'annexe B1 du RGS ou, a minima, qu'ils sont résistants à une attaque par seconde pré-image (i.e. étant donné une empreinte cible, il ne doit pas être possible de forger des données qui produisent une telle empreinte).

Vérifier au travers d'une analyse de plusieurs codes sources de versions mineures successives que les modifications réalisées n'impactent pas le respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données.

Vérifier que les subdivisions employées pour l'identification des versions mineures sont bien respectées sur un échantillon de versions successives.

Condition 3

60

Les conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données du logiciel de comptabilité ou de gestion ou du système de caisse doivent permettre à l'administration fiscale de contrôler les données enregistrées. Le logiciel ou le système doit donc prévoir un accès de l'administration fiscale à l'ensemble des données enregistrées.

Note spécifique

/

Documentation requise

Description de l'interface utilisateur, des menus et des boîtes de dialogues.
Manuel d'utilisation

Vérification à partir de la documentation

Vérification en suivant la documentation constructeur de l'existence d'un moyen permettant à l'administration d'accéder à l'ensemble des données enregistrées.

Vérification fonctionnelle

Vérification du fonctionnement effectif du moyen permettant à l'administration d'accéder à l'ensemble des données enregistrées.

Exemples de solutions acceptables

Il doit par exemple 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.

Pour accéder aux données durant l'évaluation, il peut être envisagé d'utiliser un outil d'accès spécifique ; ceci reste une possibilité, pas une exigence.

Modalités de réalisation des vérifications de robustesse

Accès au dispositif
Audit de code.

Vérification de la robustesse

Vérifier que les modalités d'accès par l'administration ne remettent pas en cause les 4 conditions (d'inaltérabilité, de sécurisation, de conservation et d'archivage des données du logiciel de comptabilité ou de gestion ou du système de caisse). En effet ces modalités d'accès ne doivent pas créer de brèche par ce biais.

Vérification par un audit de code que les fonctionnalités associées au rôle de l'administration fiscale, sont bien restreintes à ses prérogatives légitimes.

Condition 4

70

Lorsque le logiciel ou système sert à la tenue de la comptabilité de l'entreprise, celle-ci est soumise, en application du I de l'article L. 47 A du LPF, aux normes fixées par arrêté du ministre chargé du budget pour la remise des fichiers des écritures comptables. Pour plus de précisions, se reporter au BOI-CF-IOR-60-40.

Note spécifique

/

Documentation requise Description de la génération des données servant au fichier des écritures comptables et du fichier généré à partir de ces données.
Vérification à partir de la documentation /
Vérification fonctionnelle Uniquement pour les systèmes ou les logiciels généraux servant à la tenue de la comptabilité de l'entreprise, sur la base des exigences des articles L47 A et A47 A-1 du LPF, vérifier qu'un échantillonnage de fichiers test, générés par le système ou le logiciel, contient bien l'ensemble des données réglementaires.
Exemples de solutions acceptables /
Modalités de réalisation des vérifications de robustesse Non applicable
Vérification de la robustesse Non applicable

II.2.2 / Condition d'inaltérabilité

Condition 5 **80** Le logiciel de comptabilité ou de gestion ou le système de caisse doit enregistrer toutes les données d'origine relatives aux règlements.
Note spécifique Par exemple, toute réimpression de facture faite à partir du logiciel doit être enregistrée dans les données relatives aux opérations d'encaissement.
Documentation requise Description de la méthode utilisée pour enregistrer toutes les données d'origine de manière exhaustive.
Vérification à partir de la documentation Vérifier que la méthode décrite dans la documentation permet que toutes les données relatives aux règlements soient enregistrées.
Vérification fonctionnelle Réaliser un ensemble échantillonné d'opérations d'encaissement. Vérifier que l'ensemble des opérations d'encaissement réalisées préalablement apparait dans les données enregistrées ; vérifier que l'ensemble des éléments relatifs à une opération d'encaissement apparait pour chaque opération d'encaissement enregistrée. 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.
Exemples de solutions acceptables /
Modalités de réalisation des vérifications de robustesse Non applicable
Vérification de la robustesse Non applicable

Condition 6

Le logiciel de comptabilité ou de gestion ou le système de caisse doit conserver ces données d'origine enregistrées et les rendre inaltérables.

Note spécifique

La notion d'inaltérabilité est ici comprise comme l'assurance de l'absence de perte d'intégrité des données enregistrées.

Documentation requise

Document de conception du mécanisme assurant l'inaltérabilité des données dans le temps avec la spécification des mécanismes cryptographiques employés par le dispositif pour assurer l'inaltérabilité des données dans le temps.

Vérification à partir de la documentation

/

Vérification fonctionnelle

Non applicable

Exemples de solutions acceptables

L'annexe B1 du RGS, prise pour référence de l'état de l'art, précise que pour être acceptable, une fonction de hachage cryptographique doit notamment produire des empreintes de taille supérieure à 200 bits (256 bits pour un usage après 2020).
Exemples d'algorithmes à l'état de l'art pour réaliser les empreintes des données d'opérations enregistrées : SHA-2, SHA-3, Whirlpool, Blake.
Exemples d'algorithmes non suffisamment robustes pour réaliser les empreintes des données d'opérations enregistrées : SHA-1, MD5.
Exemples d'algorithmes non acceptables : CRC16, CRC32 et toutes autres formes de sommes de contrôles non cryptographiques y compris un CRC32[SHA256].
Exemples d'algorithmes de signatures de données à l'état de l'art : RSA-SSA-PSS, ECDSA.

Dans le cas d'un logiciel déployé sur le poste de travail d'un gérant, il est envisageable que le logiciel s'appuie sur une base de donnée chiffrée et signée (par exemple, 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).

Dans le cas d'un logiciel déployé sur un poste pour lequel l'utilisateur dispose des droits administrateurs, il est impossible d'empêcher tout accès aux données. Néanmoins dans ce cas, l'altération des données doit être détectée.

Modalités de réalisation des vérifications de robustesse

Accès logique au dispositif et capacité à accéder en lecture aux enregistrements, ainsi qu'aux signatures (ou chaînage des enregistrements).
Audit de code

Vérification de la robustesse

Vérifier que l'inaltérabilité des données dans le temps repose sur un mécanisme robuste, tel que le chainage des enregistrements ou le scellement des enregistrements par signature horodatée.

Dans le cas de l'utilisation d'un mécanisme de chaînage des enregistrements, 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 l'empreinte cryptographique de l'enregistrement précédent ainsi que la date et l'heure.
Vérifier par analyse documentaire que l'algorithme de hachage utilisé pour produire les empreintes cryptographiques est conforme à l'état de l'art (cf. annexe B1 du RGS sur les "Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques").
Vérifier sur le dispositif le paramétrage du mécanisme de chaînage des enregistrements afin de

s'assurer que les algorithmes décrits dans la documentation du dispositif sont bien mis en œuvre et seulement ceux-ci.
Vérifier sur le dispositif, et par échantillonnage, la cohérence d'une chaîne pour un ensemble d'enregistrements contenant des corrections (modifications et des annulations).
Vérification par un audit de code que les fonctionnalités associées au rôle de l'opérateur, sont bien restreintes à ses prérogatives légitimes.
Dans le cas de l'utilisation d'un scellement des enregistrements par signature horodatée, vérifier par analyse documentaire que les données suivantes sont utilisées pour produire la contremarque temporelle :

- la valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
- la date et le temps en valeur UTC ;
- l'identifiant du certificat du dispositif produisant la contremarque de temps.
- dans le cas d'une correction sur un enregistrement précédent, un identifiant permettant de localiser de manière fiable l'enregistrement concerné, et les valeurs de modifications ou d'annulation.

Vérifier par analyse documentaire que les algorithmes de signature et de hachage utilisés pour produire les contremarques temporelles sont conformes à l'état de l'art (cf. annexe B1 du RGS sur les "Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques").
Vérifier sur le dispositif que la clé privée est bien uniquement accessible en lecture/écriture par le seul processus et utilisateur chargé de réaliser les opérations de signature et de renouvellement de la clé.
Vérifier sur le dispositif le paramétrage du mécanisme de scellement en s'assurant que les algorithmes décrits dans la documentation du dispositif sont bien mis en œuvre et seulement ceux-ci.
Vérifier sur le dispositif, et par échantillonnage, la cohérence de plusieurs signatures d'enregistrements.
Vérification par un audit de code que les fonctionnalités associées au rôle de l'opérateur, sont bien restreintes à ses prérogatives légitimes.

Condition 7

90

Si des corrections sont apportées à des opérations de règlement, que ce soit au moyen du logiciel ou système lui-même ou d'un dispositif externe au logiciel ou système, ces corrections (modifications ou annulations) s'effectuent par des opérations de « plus » et de « moins » et non par modification directe des données d'origine enregistrées. Ces opérations de correction donnent également lieu à un enregistrement.

Note spécifique

Par exemple, le logiciel embarqué dans une télécommande doit enregistrer en plus ou en moins avant le chargement sur la caisse.

Documentation requise

Description complète des méthodes de correction des opérations de règlement.

Vérification à partir de la documentation

Vérifier à partir de la documentation la traçabilité des modifications :

- en cas de correction par le logiciel, ces corrections s'effectuent par des opérations de "plus" et de "moins" et non par des modifications directes des données d'origines enregistrées ;
- en cas de correction par un dispositif externe au logiciel ou au système, ces corrections s'effectuent par des opérations de "plus" et de "moins" et non par des modifications directes des données d'origines enregistrées ;
- en cas de correction par le logiciel, les données sont effectivement enregistrées ;
- en cas de correction par un dispositif externe au logiciel ou au système, les données sont

effectivement enregistrées.

Vérification fonctionnelle

Tester le fonctionnement du logiciel 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.

Tester le fonctionnement du logiciel pour vérifier que suite à des corrections par les dispositifs externes au logiciel ou au système prévus par le fabricant, ces corrections s'effectuent par des opérations de "plus" et de "moins" et non par des modifications directes des données d'origines enregistrées.

Vérifier visuellement par examen de la base de données que les données sont effectivement enregistrées, en cas de correction par le logiciel ou le système lui-même.

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.

Exemples de solutions acceptables

/

Modalités de réalisation des vérifications de robustesse

Accès au dispositif par les moyens préconisés par le constructeur, puis avec un matériel d'accès aux interfaces propriétaires ou interfaces non classiques (hors USB, série, etc.).

Vérification de la robustesse

Etapes d'évaluation d'essai :

- réaliser un ensemble d'opérations d'encaissement ;
- utiliser les capacités prévues par le logiciel pour tenter de modifier des opérations d'encaissement déjà réalisées ;
- exploiter les interfaces physiques du dispositif (par exemple, le port USB, le port Firefiwre ou encore le port RJ-45) pour brancher un équipement non légitime (tel qu'un dispositif de type PC, clavier, ou encore disque externe) et tenter de modifier des opérations d'encaissement déjà réalisées ;
- vérifier que l'ensemble des opérations d'encaissement réalisées préalablement apparait dans les données enregistrées, avec leurs valeurs initiales.

Condition 8

100

Autrement dit, le logiciel de comptabilité ou de gestion ou le système de caisse doit prévoir que l'administration fiscale puisse accéder aux données d'origine enregistrées initialement ainsi qu'au détail daté (année, mois, jour, heure, minute) des opérations et des corrections apportées lorsque ces données ont fait l'objet de corrections.

Note spécifique

/

Documentation requise

Description du moyen permettant à l'administration fiscale d'accéder aux données initiales et modifiées, description de l'horodatage.
Manuel d'utilisation du dispositif.
Par exemple, les autres documents suivants pourront être revus :

- le dossier de conception générale ;
- le dossier des spécifications fonctionnelles ;
- les dossiers technique, organisationnel et d'architecture.

Vérification à partir de la documentation

Vérifier au moyen de la documentation constructeur de l'existence d'un moyen permettant à l'administration d'accéder à l'ensemble des données enregistrées.

Vérifier au moyen de la documentation constructeur que ces données comprennent les données d'origines initialement enregistrées, le détail daté des opérations et des corrections apportées lorsque les données ont fait l'objet de correction.

Vérifier au moyen de la documentation constructeur que le format des dates est (année, mois, jour, heure, minute).

Vérification fonctionnelle

Vérification du fonctionnement du moyen permettant à l'administration d'accéder à l'ensemble des données enregistrées.

Vérification visuelle que les données accédées à l'aide du moyen contiennent effectivement les données d'origines initialement enregistrées, le détail daté des opérations et des corrections apportées lorsque les données ont fait l'objet de correction.

Vérification visuelle du format des dates accédées.

Exemples de solutions acceptables

/

Modalités de réalisation des vérifications de robustesse

Accès au dispositif.

Vérification de la robustesse

Etapes d'évaluation d'essai :

- se connecter sur le dispositif avec un compte légitimement utilisable par l'administration (par exemple compte dédié à l'administration, compte utilisateur, etc.) ;
- vérifier qu'avec cette modalité de connexion, il est possible d'accéder aux données d'origine enregistrées ainsi qu'au détail daté des opérations et des corrections apportées lorsque ces données ont fait l'objet de corrections.

Condition 9

110

S'agissant des éventuelles corrections et annulations apportées par le logiciel ou le système ou par un dispositif externe, il est rappelé que les entreprises sont soumises aux obligations comptables suivantes :

- principe du caractère intangible ou de l'irréversibilité des écritures comptables ;
- principe d'une procédure de clôture périodique des enregistrements chronologiques ;
- principe de la permanence du chemin de révision.

Pour plus de précisions, se reporter aux BOI-BIC-DECLA-30-10-20-40 et BOI-CF-IOR-60-40.

Note spécifique

Ce paragraphe est un rappel de la réglementation relative à une comptabilité informatisée et son contrôle. Il est de la responsabilité des éditeurs de systèmes ou de logiciel pour lesquelles ces exigences sont applicables de s'y conformer. Ce paragraphe n'amène pas d'exigence supplémentaire dans le présent référentiel ; les vérifications sont faites conformément aux dispositions prévues à la condition 8 ci-avant.

Documentation requise

Non applicable

Vérification à partir de la documentation

Non applicable

Vérification fonctionnelle

Non applicable

Exemples de solutions acceptables

Non applicable

Modalités de réalisation des vérifications de robustesse

Non applicable

Vérification de la robustesse
Non applicable

Condition 10
120
Pour respecter la condition d'inaltérabilité, l'intégrité des données enregistrées doit être garantie dans le temps par tout procédé technique fiable.

Note spécifique
/

Documentation requise
La documentation doit comprendre les éléments démontrant :
- que des spécifications de conception couvrant cette exigence ont été définies ;
- que des vérifications (plan de test, rapport de test, etc.) existent et démontrent que l'éditeur a vérifié que les spécifications de conception définies étaient atteintes de manière satisfaisante.

Vérification à partir de la documentation
Selon les critères relatifs à la fonctionnalité : Intégrité dans le temps § **80** – conditions 5 et 6 ci-avant.

Vérification fonctionnelle
Selon les critères relatifs à la fonctionnalité : Intégrité dans le temps § **80** – conditions 5 et 6 ci-avant.

Exemples de solutions acceptables
/

Modalités de réalisation des vérifications de robustesse
Accès au dispositif par les moyens préconisés par le constructeur, puis avec un matériel d'accès aux interfaces propriétaires ou interfaces non classiques (hors USB, série, etc.).

Vérification de la robustesse
Etapes d'évaluation d'essai :
- réaliser un ensemble d'opérations d'encaissement ;
- se connecter sur le dispositif avec l'ensemble des moyens d'accès autorisés, et essayer de modifier l'intégrité des données d'opérations déjà enregistrées.

II.2.3/ Condition de sécurisation

Condition 11
130
Le logiciel de comptabilité ou de gestion ou le système de caisse doit sécuriser les données d'origine, les données de modifications enregistrées et les données permettant la production des pièces justificatives émises.

Note spécifique
/

Documentation requise
Description de la méthode de sécurisation des données, des données modifiées et des données permettant la production de pièces justificatives.
Par exemple, les documents suivants pourront être revus :
- manuel d'utilisation du dispositif ;
- le dossier de conception générale ;
- le dossier des spécifications fonctionnelles ;
- les dossiers technique, organisationnel et d'architecture.

Vérification à partir de la documentation

Vérifier à partir de la documentation de conception et d'implémentation de l'existence d'un mécanisme de sécurisation.

Vérifier que les données sécurisées comprennent :

- les données d'origines,
- les données de modification enregistrées,
- les données permettant la production de pièces justificatives émises.

Vérification fonctionnelle

Sur une base de données test, effectuer des essais pour vérifier que l'ajout de données avec le logiciel ou le système est bien répercuté dans la base de données :

- sans modification des données d'origines
- avec la présence des données de modification.

Sur une base de données test, demander la production d'un échantillon de différentes pièces justificatives et vérifier que la base de données est bien mise à jour avec les données de production de pièces justificatives.

Exemples de solutions acceptables

/

Modalités de réalisation des vérifications de robustesse

/

Vérification de la robustesse

S'assurer au travers d'une analyse documentaire de l'existence de documents de conception et d'implémentations d'un mécanisme de sécurisation des données d'origine, des données de modifications enregistrées et des données permettant la production des pièces justificatives émises.

Condition 12

140

Cette sécurisation peut être assurée par tout procédé technique fiable, c'est-à-dire de nature à garantir la restitution des données de règlement dans l'état de leur enregistrement d'origine. Il peut notamment s'agir d'une technique de chaînage des enregistrements ou de signature électronique des données.

Note spécifique

/

Documentation requise

Pas de documentation spécifique à cette condition, celle-ci étant déjà présente pour avoir répondu aux conditions ci-avant.

Vérification à partir de la documentation

Selon les critères relatifs à la fonctionnalité : Intégrité dans le temps § **80** – conditions 5 et 6 ci-avant.

Vérification fonctionnelle

Selon les critères relatifs à la fonctionnalité : Intégrité dans le temps § **80** – conditions 5 et 6 ci-avant.

Exemples de solutions acceptables

/

Modalités de réalisation des vérifications de robustesse

Avis d'expert concluant sur la capacité du système de caisse à garantir la sécurisation des enregistrements.

Vérification de la robustesse

Etapes d'évaluation d'essai :

- 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, robustesse des mécanismes cryptographiques employés et conformité vis-à-vis de l'état de l'art, etc.) ;
- conclure sur la capacité du mécanisme à assurer la sécurisation des enregistrements de manière fiable ou non.

Condition 13

150

L'emploi d'une fonction « école » ou « test » destinée à l'enregistrement d'opérations de règlement fictives aux fins de formation du personnel doit être sécurisé, par une identification très claire des données de règlement, des pièces justificatives (par exemple en apposant la mention « factice » ou « simulation » en trame de fond de ces documents) et de toutes les opérations enregistrées lors de l'utilisation de cette fonction, ainsi que par l'identification de l'opérateur sous la responsabilité duquel le personnel en formation enregistre les données.

Note spécifique

1. Le mode école doit être visible par exemple sur les affichages (à destination du vendeur et du client le cas échéant) et/ou sur tous les documents imprimés.
2. Dans la base de données, les données écoles doivent être distinguées des autres données.
3. Le clonage du système d'origine par l'utilisateur reste de sa responsabilité.

Documentation requise

Si applicable, description complète du mode école ou test.

Vérification à partir de la documentation

Si une telle fonction est présente :

- vérifier que les données de règlement fictives font l'objet d'une identification très claire ;
- vérifier que les pièces justificatives font l'objet d'une identification très claire ;
- vérifier que toutes les opérations enregistrées font l'objet d'une identification très claire ;
- vérifier que l'opérateur sous la responsabilité duquel le personnel en formation enregistre les données, fait bien l'objet d'une identification très claire dans les données de règlement, dans les pièces justificatives, et dans toutes les opérations enregistrées lors de l'utilisation de cette fonction.

Vérification fonctionnelle

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

Vérifier dans la base de données et dans les pièces justificatives émises que le fonctionnement est celui qui décrit dans la documentation, et notamment :

- que les données de règlement fictives font l'objet d'une identification très claire ;
- que les pièces justificatives font l'objet d'une identification très claire ;
- que toutes les opérations enregistrées font l'objet d'une identification très claire ;
- que l'opérateur sous la responsabilité duquel le personnel en formation enregistre les données, fait bien l'objet d'une identification très claire dans les données de règlement, dans les pièces justificatives, et dans toutes les opérations enregistrées lors de l'utilisation de cette fonction.

Vérifier que le même niveau de sécurité est également assuré dans le mode école, en ce qui concerne l'inaltérabilité des données enregistrées dans le temps. Les critères relatifs à la vérification de cette fonctionnalité sont précisés aux conditions 5 et 6 : intégrité dans le temps § **80**.

Exemples de solutions acceptables

Les données de règlements et les pièces justificatives peuvent par exemple se voir apposées la mention "factice" ou simulation" en trame de fond.

Les bases de données peuvent indiquer le même type de mention pour chaque donnée de règlement.

Modalités de réalisation des vérifications de robustesse

Non applicable

Vérification de la robustesse
Non applicable

II.2.4 / Condition de conservation

Condition 14
160
Le logiciel de comptabilité ou de gestion ou le système de caisse qui enregistre les données de règlement doit prévoir une clôture. Cette clôture doit intervenir à l'issue d'une période au minimum annuelle (ou par exercice lorsque l'exercice n'est pas calé sur l'année civile).

Notes spécifiques
L'exigence de prévoir une clôture est comprise comme obligation de donner la possibilité à l'utilisateur de réaliser cette clôture.
L'action de clôture peut prendre la forme d'une opération manuelle ayant pour but de figer les données concernées par la clôture.
Il reste de la responsabilité de l'utilisateur du logiciel ou du système de réaliser ces clôtures régulièrement.

Documentation requise
Description de la méthode à suivre pour réaliser des clôtures et des modalités d'avertissement pour l'utilisateur.

Vérification à partir de la documentation
Vérification à partir de la documentation :
- de la présence d'une fonctionnalité de clôture ;
- que la clôture intervient à l'issue d'une période au minimum annuelle ou par exercice lorsque celui-ci n'est pas calé sur l'année civile ;
- que l'utilisateur est prévenu de la possibilité de réaliser une clôture au minimum annuelle ou par exercice.

Vérification fonctionnelle
S'authentifier sur le dispositif avec le rôle destiné à la configuration du dispositif.
S'assurer de l'existence d'une configuration destinée à déterminer la périodicité des enregistrements et la date de clôture périodique des enregistrements.
Paramétrer cette configuration avec des valeurs réduites à quelques jours, voire quelques heures si cela est permis par le dispositif afin de réaliser une vérification sur une période de temps compatible avec l'évaluation.
S'authentifier sur le dispositif avec le rôle destiné à l'utilisateur du dispositif.
Réaliser des opérations d'enregistrements sur cette période.
Accéder aux données d'enregistrement.
Vérifier la bonne génération d'une clôture par exercice.
Vérifier la bonne génération d'une clôture annuelle.

Exemples de solutions acceptables
Il est considéré comme acceptable d'informer l'utilisateur de la possibilité de procéder à une clôture par tout moyen adéquat (Affiche sur le système ou le logiciel, notice d'utilisation, contrat, etc.).

Modalités de réalisation des vérifications de robustesse
Non applicable

Vérification de la robustesse
Non applicable

Condition 15

170

Les systèmes de caisse doivent, de plus, prévoir obligatoirement une clôture journalière et une clôture mensuelle.

Note spécifique

L'exigence de prévoir une clôture journalière ou mensuelle est comprise comme obligation de donner la possibilité à l'utilisateur de réaliser cette clôture journalière et mensuelle.
Il reste de la responsabilité de l'assujetti à la TVA de faire sa clôture à la périodicité appropriée.

Documentation requise

Description de la méthode à suivre pour réaliser des clôtures et des modalités d'avertissement pour l'utilisateur.

Vérification à partir de la documentation

Uniquement applicable aux systèmes de caisse.
Vérification à partir de la documentation :

- de la présence d'une fonctionnalité de clôture ;
- que la clôture intervient à l'issue d'une période journalière ou mensuelle ;
- que l'utilisateur est prévenu de la possibilité de réaliser une clôture journalière et mensuelle.

Vérification fonctionnelle

Clôture mensuelle :

- s'authentifier sur le dispositif avec le rôle destiné à la configuration du dispositif ;
- s'assurer de l'existence d'une configuration destinée à déterminer la périodicité des enregistrements et la date de clôture périodique des enregistrements ;
- paramétrer cette configuration avec des valeurs réduites à quelques jours, voire quelques heures si cela est permis par le dispositif afin de réaliser une vérification sur une période de temps compatible avec l'évaluation ;
- s'authentifier sur le dispositif avec le rôle destiné à l'utilisateur du dispositif ;
- réaliser des opérations d'enregistrements sur cette période mensuelle ;
- accéder aux données d'enregistrement ;
- vérifier la bonne génération d'une clôture mensuelle.

Clôture journalière :

- s'authentifier sur le dispositif avec le rôle destiné à l'utilisateur du dispositif ;
- réaliser des opérations d'enregistrements sur cette période journalière ;
- accéder aux données d'enregistrement ;
- vérifier la bonne génération d'une clôture journalière.

Exemples de solutions acceptables

Il est considéré comme acceptable d'informer l'utilisateur de la possibilité de procéder à une clôture journalière et mensuelle.

Modalités de réalisation des vérifications de robustesse

Non applicable

Vérification de la robustesse

Non applicable

Condition 16

Pour chaque clôture - journalière, mensuelle et annuelle (ou par exercice) - des données cumulatives et récapitulatives, intègres et inaltérables, doivent être calculées par le système de caisse, comme le cumul du grand total de la période et le total perpétuel pour la période comptable.

Note spécifique

/

Documentation requise

Description des données cumulatives et récapitulatives calculées.

Vérification à partir de la documentation

Vérifier à partir de la documentation que des données cumulatives et récapitulatives sont calculées pour chacune des clôtures suivantes :

- journalière (si applicable – cf. condition 15 ci-avant),
- mensuelle (si applicable – cf. condition 15 ci-avant),
- annuelle ou par exercice.

Vérification fonctionnelle

Sur un échantillonnage de données de test représentatives, vérifier que le logiciel ou le système génère des données cumulatives et récapitulatives (comme le grand total de la période et le total perpétuel pour la période comptable) pour chacune des clôtures suivantes :

- journalière (si applicable – cf. condition 15 ci-avant),
- mensuelle (si applicable – cf. condition 15 ci-avant),
- annuelle ou par exercice.

Exemples de solutions acceptables

La solution retenue peut être équivalente à la solution employée pour assurer l'intégrité des données d'opérations enregistrées (chaînage, signature cryptographique, etc.).
Il est considéré comme acceptable d'avoir un même chiffrement pour les données de règlement et les données cumulatives et récapitulatives.

Modalités de réalisation des vérifications de robustesse

Accès au dispositif.

Vérification de la robustesse

Vérifier que l'intégrité des données cumulatives et récapitulatives repose sur un mécanisme robuste, tel que le chaînage des données ou le scellement des données par signature horodatée, ou a minima par une gestion stricte des droits d'accès au système de fichiers avec réalisation d'une empreinte cryptographique des données.

Condition 17

180

Toutes les données mentionnées au I-A-3 § **50** doivent être conservées. Cette obligation de conservation porte sur toutes les données enregistrées ligne par ligne, ainsi que pour les systèmes de caisse, sur les données cumulatives et récapitulatives calculées par le système (cf. I-B-3 § **170**).

Note spécifique

/

Documentation requise

Description de la méthode de conservation des données ligne à ligne et des données de cumul et de récapitulation.
La documentation réglementaire et complémentaire doit comprendre en particulier les éléments démontrant :

- que des spécifications de conception couvrant cette exigence ont été définies.
- que des vérifications (plan de test, rapport de test, etc.) existent et démontrent que l'éditeur a vérifié que les spécifications de conception définies étaient atteintes de manière satisfaisante.

Vérification à partir de la documentation

Vérification à partir de la documentation :

- pour tous les logiciels et systèmes, que toutes les données (telles que mentionnées au I-A-3 § **50**) enregistrées ligne par ligne sont bien conservées.
- uniquement pour les systèmes de caisses, que toutes les données cumulatives et

récapitulatives sont bien conservées.
Vérification fonctionnelle Sur une base test, ajouter un ensemble échantillonné de données telles que mentionnées au I-A-3 § **50** afin de vérifier leur bonne conservation. Uniquement pour les systèmes de caisse, sur une base test, ajouter un ensemble échantillonné de données afin de vérifier la bonne conservation des données cumulatives et récapitulatives.
Exemples de solutions acceptables /
Modalités de réalisation des vérifications de robustesse Non applicable
Vérification de la robustesse Non applicable

Condition 18 **190** Cette conservation est opérée, soit en ligne, c'est-à-dire dans le logiciel ou système, soit dans une archive dans le respect des conditions d'archivage détaillées au I-B-4 § **220** à **260**.
Note spécifique /
Documentation requise /
Vérification à partir de la documentation /
Vérification fonctionnelle Vérifier que la conservation des données est réalisée soit en ligne, c'est-à-dire dans le logiciel ou le système, soit dans une archive. Lorsque la conservation des données est réalisée dans une archive, vérifier que les dispositions sont conformes aux conditions d'archivage détaillées au I-B-4 §**220** à **260** (conditions **22** à **30**).
Exemples de solutions acceptables /
Modalités de réalisation des vérifications de robustesse Non applicable
Vérification de la robustesse Non applicable

Condition 19 **200** Les données de règlement étant des données servant à l'établissement de la comptabilité de l'entreprise, elles doivent être conservées pendant le délai de six ans prévu au premier alinéa de l'article L.102 B du LPF. Se reporter au BOI-BIC-DECLA-30-10-20-40 pour plus de précisions.
Note spécifique Cette exigence s'applique même si le logiciel ou le système ne réalise pas lui-même la comptabilité de l'entreprise. Le stockage avec conservation pendant 6 ans peut être réalisé par le dispositif lui-même ou bien par l'environnement de déploiement. Dans ce dernier cas, le dispositif doit alors présenter des fonctionnalités d'export et de sauvegarde sur support externe. Il n'est pas de la responsabilité de l'éditeur ou du fabricant de réaliser l'archivage, par contre, le logiciel ou le système doit proposer une possibilité d'archivage.
Documentation requise

Description des méthodes utilisées pour garantir la conservation des données pendant le délai requis, y compris les méthodes pour prévenir une saturation de la mémoire lorsque la conservation est faite dans le logiciel ou le système lui-même.

Vérification à partir de la documentation

Vérification à partir de la documentation :

- que le logiciel ou le système permet une conservation des données pendant une durée d'au moins 6 ans.
- ou bien, si les données sont établies ou reçues sous forme informatique, que le logiciel ou le système permet une conservation des données pendant une durée d'au moins 3 ans et que le système permet au contribuable de conserver les données sur un autre support prévu jusqu'à l'expiration du délai général de 6 ans.
- que le fabricant a mis en place des dispositions pour prévenir le risque de saturation de la mémoire du dispositif.

Vérification fonctionnelle

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

Exemples de solutions acceptables

Des modalités d'information à l'utilisateur ou des modalités visant à prévenir l'effacement des données lors d'une saturation mémoire sont considérées comme acceptables.

Modalités de réalisation des vérifications de robustesse

Accès au dispositif.

Vérification de la robustesse

Vérification documentaire :

- vérifier par une analyse documentaire l'aptitude du logiciel ou du système à conserver les données (servant à l'établissement de la comptabilité de l'entreprise) pendant une durée de 6 ans ;
- vérifier dans les documents de conception que cette aptitude repose, par exemple, sur l'utilisation d'un mécanisme assurant un certain niveau de disponibilité au niveau du système de stockage (RAID 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 sur le dispositif que la mise en œuvre du mécanisme assurant la disponibilité des données (paramétrage du RAID matériel dans le firmware, du RAID logiciel sur le système support, ou encore choix et configuration du type de système de fichiers) correspond à ce qui est décrit dans la documentation de conception.

Etapes d'évaluation d'essai :
- s'authentifier sur le dispositif avec le rôle destiné à la configuration du dispositif ;
- vérifier dans la configuration qu'une durée d'enregistrement des opérations pendant une durée de 6 ans est mise en œuvre par défaut.
Si une purge est possible, vérifier qu'il est possible de faire la purge avant les 6 ans.

Condition 20

210

Lorsque l'assujetti utilise un système de caisse centralisé avec remontée des données de règlement depuis des points de vente vers un système centralisateur, la conservation des données enregistrées ligne par ligne et la conservation des données cumulées peut être réalisée au niveau du système centralisateur, à condition qu'une traçabilité de la remontée des données de règlement des points de vente vers le système centralisateur soit prévue.

Note spécifique

L'examen de cette exigence est réalisé seulement si le système centralisateur revendique une fonction de conservation des données enregistrées.

Documentation requise

Description complète du fonctionnement avec un système centralisateur.

Vérification à partir de la documentation

Uniquement dans le cas de système centralisé avec remontée des données de règlement depuis des points de vente vers un système centralisateur :
Vérifier l'existence d'un système de remontée des données de règlement des points de vente vers le système centralisateur.

Vérification fonctionnelle

Uniquement dans le cas de système centralisé avec remontée des données de règlement depuis des points de vente vers un système centralisateur.
En échantillonnant un système de caisse parmi la liste exhaustive des systèmes de caisse :

- vérifier la bonne traçabilité du système de remontée des données de règlement des points de vente vers le système centralisateur ;
- vérifier la bonne remontée dans le système centralisateur d'un ensemble échantillonné de données ligne à ligne ainsi que de données cumulées.

En échantillonnant un logiciel parmi la liste exhaustive des logiciels :

- vérifier la bonne traçabilité du système de remontée des données de règlement des points de vente vers le système centralisateur.
- vérifier la bonne remontée dans le système centralisateur d'un ensemble échantillonné de données ligne à ligne ainsi que de données cumulées.

Exemples de solutions acceptables

/

Modalités de réalisation des vérifications de robustesse

Accès à un ensemble de dispositif annexes.
Accès au dispositif centralisateur.

Vérification de la robustesse

Réaliser un ensemble d'opérations d'encaissement depuis des dispositifs annexes reliés au système centralisateur, et vérifier sur ce dernier, qu'à chaque enregistrement réalisé sur un dispositif annexe est associé :

- l'identifiant du dispositif annexe concerné,
- un horodatage ou une numérotation incrémentale traçant le moment de l'envoi des données par le dispositif annexe,
- un horodatage ou une numérotation incrémentale traçant le moment de la réception des données par le système centralisateur,
- une valeur incrémentale traçant l'ensemble des envois de données d'opérations depuis chaque dispositif, afin de s'assurer qu'un envoi n'a pas été omis.

Vérifier que les données enregistrées ligne par ligne et que les données cumulatives sont stockées et conservées sur le système centralisateur.

Condition 21

Cette traçabilité doit permettre à l'administration de vérifier l'exhaustivité du flux des données transférées.

Note spécifique

/

Documentation requise

Uniquement dans le cas de système de caisse centralisé avec remontée des données de règlement depuis des points de vente vers un système centralisateur.

Description de la méthode employée pour garantir l'exhaustivité de la remontée des données de règlement des points de vente vers le système centralisateur.
Vérification à partir de la documentation Vérifier que le fabricant a fourni une déclaration explicite d'exhaustivité de la remontée des données de règlement des points de vente vers le système centralisateur afin de démontrer la traçabilité des données.
Vérification fonctionnelle Non applicable
Exemples de solutions acceptables Un chiffrement ou une signature sur les ensembles de données transférées du système local au système centralisateur pour garantir l'exhaustivité des données lors de la remontée d'informations.
Modalités de réalisation des vérifications de robustesse Accès au dispositif.
Vérification de la robustesse Vérifier par sondage qu'aucune donnée n'est perdue lors de la remontée des informations vers 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.

II.2.5 / Condition d'archivage

Condition 22 **220** Le logiciel de comptabilité ou de gestion ou le système de caisse doit permettre d'archiver les données enregistrées selon une périodicité choisie, au maximum annuelle ou par exercice.
Note spécifique L'exigence de prévoir un archivage est comprise comme obligation de donner la possibilité à l'utilisateur de réaliser cet archivage.
Documentation requise Description de la manière de prévenir l'utilisateur et de la méthode d'archivage.
Vérification à partir de la documentation Vérifier que la périodicité prévue pour la procédure d'archivage est au maximum annuelle ou par exercice.
Vérification fonctionnelle Non applicable
Exemples de solutions acceptables /
Modalités de réalisation des vérifications de robustesse Accès au dispositif.
Vérification de la robustesse Essayer de créer une procédure d'archivage d'une périodicité supérieure à une périodicité annuelle ou d'un exercice et vérifier l'impossibilité de réaliser un tel archivage.

Condition 23 La procédure d'archivage a pour objet de figer les données et de donner date certaine aux documents archivés.
Note spécifique /

Documentation requise
Description de la méthode utilisée pour figer les données et les dater.

Vérification à partir de la documentation
Vérifier que la documentation constructeur précise que la procédure d'archivage a pour objet de figer les données et de donner date certaine aux documents archivés.

Vérification fonctionnelle
Non applicable

Exemples de solutions acceptables
/

Modalités de réalisation des vérifications de robustesse
Attendus concernant le dispositif : accès logique au dispositif et capacité à accéder en lecture aux archives, ainsi qu'aux signatures.

Vérification de la robustesse
Vérifier que la production de la date certaine des archives repose sur un mécanisme robuste, telle que la signature horodatée. La vérification repose sur le respect de la condition 24 ci-après (exigence **220** liée à l'intégrité dans le temps des archives).

Condition 24
La procédure d'archivage doit prévoir un dispositif technique garantissant l'intégrité dans le temps des archives produites et leur conformité aux données initiales de règlement à partir desquelles elles sont créées.

Note spécifique
/

Documentation requise
Non applicable

Vérification à partir de la documentation
Non applicable

Vérification fonctionnelle
Non applicable

Exemples de solutions acceptables
L'annexe B1 du RGS, prise comme référence de l'état de l'art, précise que pour être acceptable, une fonction de hachage cryptographique doit notamment produire des empreintes de taille supérieure à 200 bits (256 bits pour un usage après 2020).

Exemples d'algorithmes à l'état de l'art pour réaliser les empreintes des archives : SHA-2, SHA-3, Whirlpool, Blake.

Exemples d'algorithmes non suffisamment robustes pour réaliser les empreintes des archives : SHA-1, MD5.

Exemples d'algorithmes non acceptables : CRC16, CRC32 et toutes autres formes de sommes de contrôles non cryptographiques.

Exemples d'algorithmes de signatures de données à l'état de l'art : RSA-SSA-PSS, ECDSA.

Dans le cas d'un logiciel déployé sur le poste de travail d'un gérant, il est envisageable que le logiciel s'appuie sur une base de donnée chiffrée et signée (par exemple, 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).

Un enregistrement et un chiffrement avec signature des données en temps réel sont considérés comme un archivage.

Modalités de réalisation des vérifications de robustesse

Accès logique au dispositif et capacité à accéder en lecture aux archives, ainsi qu'aux signatures (ou chainage des enregistrements).
Audit de code

Vérification de la robustesse

Vérifier que l'inaltérabilité des archives dans le temps repose sur un mécanisme robuste, tel que le chainage des archives ou le scellement des archives par signature horodatée.

Dans le cas de l'utilisation d'un mécanisme de chaînage des archives, vérifier par analyse documentaire que chaque archive est cryptographiquement liée à l'archive qui la précède chronologiquement, en incluant dans le calcul de l'empreinte cryptographique de l'archive courante l'empreinte cryptographique de l'archive précédente ainsi que la date et l'heure.
Vérifier par analyse documentaire que l'algorithme de hachage utilisé pour produire les empreintes cryptographiques est conforme aux à l'état de l'art (cf. annexe B1 du RGS sur les "Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques").
Vérifier sur le dispositif le paramétrage du mécanisme de chaînage des archives afin de s'assurer que les algorithmes décrits dans la documentation du dispositif sont bien mis en œuvre et seulement ceux-ci.
Vérifier sur le dispositif, et par échantillonnage, la cohérence d'une chaine pour un ensemble d'archives.
Vérification par un audit de code que les fonctionnalités associées au rôle de l'opérateur, sont bien restreinte à ces prérogatives légitimes.

Dans le cas de l'utilisation d'un scellement des archives par signature horodatée, vérifier par analyse documentaire que les données suivantes sont utilisées pour produire la contremarque temporelle :

- la valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
- la date et le temps en valeur UTC ;
- l'identifiant du certificat du dispositif produisant la contremarque de temps.

Vérifier par analyse documentaire que les algorithmes de signature et de hachage utilisés pour produire les contremarques temporelles sont conformes à l'état de l'art (cf. annexe B1 du RGS sur les "Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques").
Vérifier sur le dispositif que la clé privée est bien uniquement accessible en lecture/écriture par le seul processus et utilisateur chargé de réaliser les opérations de signature et de renouvellement de la clé.
Vérifier sur le dispositif le paramétrage du mécanisme de scellement en s'assurant que les algorithmes décrit dans la documentation du dispositif sont bien mis en œuvre et seulement ceux-ci.
Vérifier sur le dispositif, et par échantillonnage, la cohérence de plusieurs signatures d'archives.
Vérification par un audit de code que les fonctionnalités associées au rôle de l'opérateur, sont bien restreinte à ses prérogatives légitimes.

Condition 25

Les archives peuvent être conservées dans le système lui-même ou en dehors du système lorsqu'il existe une procédure de purge.

Note spécifique

/

Documentation requise

Description de la méthode de conservation des archives dans le système ou de la méthode de purge.

Vérification à partir de la documentation

Vérifier que la documentation du fabricant précise que les archives sont conservées dans le système lui-même.

S'il existe une procédure de purge, vérifier que la documentation constructeur précise que les archives purgées ne sont pas conservés dans le système lui-même mais en dehors du système.

Vérification fonctionnelle

Non applicable

Exemples de solutions acceptables

/

Modalités de réalisation des vérifications de robustesse

Accès au dispositif

Audit de code

Vérification de la robustesse

Créer une archive non purgée et vérifier son stockage dans la mémoire du système lui-même.

S'il existe une procédure de purge, créer une archive et la purger, vérifier l'absence de l'archive dans la mémoire du système lui-même et vérifier la création du fichier de purge en dehors du système.

Condition 26

230

Les archives doivent pouvoir être lues aisément par l'administration en cas de contrôle, y compris lorsque l'entreprise a changé de logiciel ou de système.

Note spécifique

L'entreprise correspond ici à l'éditeur du logiciel ou le fabricant du système.

Documentation requise

Description des moyens de lecture des archives.

Vérification à partir de la documentation

Vérification au moyen de la documentation constructeur de l'existence d'un moyen permettant à l'administration de lire des archives en cas de contrôle.

Vérification de la présence d'un engagement de l'entreprise à donner à l'administration en cas de contrôle, les moyens aisés d'accès aux archives, y compris lorsque l'entreprise a changé de logiciel ou de système.

Vérification fonctionnelle

Vérification du fonctionnement aisé du moyen permettant à l'administration de lire des archives en cas de contrôles.

Exemples de solutions acceptables

A titre d'exemples, un format d'archive lisible par un humain peut être employé, tel que : JSON, XML, CSV, texte à plat.

En ce qui concerne le format XML, il est possible d'intégrer directement le support des signatures dans le fichier XML produit, notamment au travers des standards XMLDsig et XAdES.

Si le fichier archive est chiffré, il faut un outil de déchiffrement qui doit avoir une durée de vie et une disponibilité supérieure à celle du système.

De plus l'éditeur doit documenter l'outil de déchiffrement si l'utilisation est prévue sans intervention de l'éditeur du logiciel.

Modalités de réalisation des vérifications de robustesse

Non applicable

Vérification de la robustesse

Non applicable

Condition 27

240

Le logiciel ou système doit prévoir une traçabilité des opérations d'archivage, selon un procédé

fiable.

Note spécifique

/

Documentation requise

/

Vérification à partir de la documentation

Non applicable

Vérification fonctionnelle

Non applicable

Exemples de solutions acceptables

A titre d'exemple, il est envisageable que la traçabilité des opérations d'archivage soit assurée par un journal de bord, dans la mesure du possible signé.

Dans le cas d'un dispositif de faible puissance de calcul (de type caisse enregistreuse ou balance par exemple), un horodatage des archives produites associé à une protection en écriture peut être mis en place.

Modalités de réalisation des vérifications de robustesse

Accès au dispositif.

Vérification de la robustesse

Vérifier sur le dispositif, après avoir réalisé un ensemble d'opérations d'archivage :

- qu'il est possible de recenser l'ensemble des opérations d'archivage réalisées ;
- qu'un horodatage des archives est mis en place ;
- qu'une association existe entre l'archive et le dispositif qui a produit l'archive.
- qu'un moyen fiable est employé pour tracer les archives réalisées.

Condition 28

250

Au-delà de la périodicité choisie et au maximum annuelle ou par exercice, le logiciel ou le système peut prévoir une procédure de purge des données de règlement. Avant la mise en œuvre de cette procédure de purge, le logiciel ou le système doit garantir la production d'une archive complète des données de règlement (données d'origine et éventuelles modifications), avec la date de l'opération de règlement (année – mois – jour).

Note spécifique

/

Documentation requise

Description de la méthode de purge si applicable et du moyen garantissant la production de l'archive.

Vérification à partir de la documentation

Vérification à partir de la documentation :

- de la complétude de l'archive des données de règlement.
- que les dates d'opération de règlement sont au format (année - mois - jour).

Vérification fonctionnelle

Création d'une archive fictive initiale contenant un échantillon de données d'origines et de modification, mise en place de la procédure de purge, vérification de la complétude de l'archive purgée par rapport à l'archive initiale.

Visualisation à l'aide d'un outil des données de l'archive afin de vérifier que le format des dates des opérations de règlement est bien (année - mois - jour).

Exemples de solutions acceptables

/

Modalités de réalisation des vérifications de robustesse

Non applicable

Vérification de la robustesse
Non applicable

Condition 29
La production de l'archive complète doit se faire sur un support physique externe sécurisé.

Note spécifique
/

Documentation requise
Idem ci-avant

Vérification à partir de la documentation
Non applicable

Vérification fonctionnelle
Non applicable

Exemples de solutions acceptables
A titre d'exemple, un support externe sécurisé de type disque dur externe chiffré est envisageable.
Une alternative peut être la production d'une archive sécurisée (signée) qui est stockée sur un dispositif externe classique (disque externe, clé USB, etc.).
Dans le cas d'un support externe non sécurisé, c'est l'archive qui doit être sécurisée.

Modalités de réalisation des vérifications de robustesse
Accès par l'évaluateur au dispositif auquel est branché un support externe sécurisé.

Vérification de la robustesse
Vérifier, après avoir réalisé une opération d'archivage avec comme destination un support externe sécurisé, que l'archive est bien entreposée sur ce support à la fin de l'opération.

Dans le cas de l'utilisation d'un support externe intégrant un mécanisme de sécurisation :
- vérifier par analyse documentaire que le support externe propose des mesures de sécurité à l'état de l'art (c'est à dire dont les algorithmes employés respectent les exigences de l'état de l'art, cf. annexe B du RGS de l'ANSSI) ;
- vérifier qu'il n'est pas possible d'altérer l'intégrité des données archivées sur le support externe depuis une station extérieure, ou qu'en cas d'altération, celle-ci soit bien détectée ;
- vérifier qu'il n'est pas possible d'employer un composant externe non légitime pour stocker les archives.

Dans le cas de la production d'archives nativement sécurisées, vérifier que les mêmes mécanismes qui assurent l'intégrité des archives sont bien employés (voir exigence **220**), afin de détecter d'éventuelles pertes d'intégrité.

Condition 30
260
Pour les systèmes de caisse, la purge n'est que partielle : le système doit conserver dans un état sécurisé « en ligne », c'est-à-dire dans le système lui-même, les données cumulatives et récapitulatives contenues dans le grand total de la période et le total perpétuel pour la période dont les données ont été purgées.

Note spécifique
/

Documentation requise
Pour les systèmes de caisse uniquement, description complémentaire de la purge.

Vérification à partir de la documentation
Vérification que les données cumulatives et récapitulatives (grand total et total perpétuel pour la période dont les données ont été purgées) sont correctement conservés dans le système de caisse.

Vérification fonctionnelle Sur un système de caisse représentatif, introduire des données connues, réaliser une purge et vérifier l'exactitude des données cumulatives et récapitulatives contenues dans le grand total de la période et le total perpétuel pour la période dont les données ont été purgées contenues dans le système de caisse avec les données initialement introduites.
Exemples de solutions acceptables /
Modalités de réalisation des vérifications de robustesse Accès par l'évaluateur au dispositif auquel est branché un support externe sécurisé.
Vérification de la robustesse Vérifier sur le dispositif que le mécanisme de purge ne remet pas en cause l'intégrité des données cumulatives et récapitulatives contenues dans le grand total de la période et le total perpétuel pour la période dont les données ont été purgées (cf. condition 16 ci-avant - exigence **170**).

II.3 / Exigences applicables au système de management de la qualité

Le titulaire de la certification met en place un système de management de la qualité destiné à s'assurer que chaque système de caisse mis sur le marché répond aux exigences du présent référentiel.

II.3.1 / Exigences générales

Ce système qualité doit être conforme aux chapitres cités ci-dessous de la norme ISO 9001 version 2008 ou version 2015 (systèmes de management de la qualité – exigences).

ISO 9001 version 2008	ISO 9001 version 2015
4.2. Exigences relatives à la documentation	7.5. Informations documentées
7.3. Conception et développement	8.3. Conception et développement de produits et services
7.4. Achats	8.4. Maîtrise des processus, produits et services fournis par des prestataires externes
7.5. Production et préparation du service	8.5. Production et prestation de service
7.5.1. Maîtrise de la production et de la préparation du service	8.5.1. Maîtrise de la production et de la prestation de service
7.5.2. Validation des processus de production et de préparation du service	8.5.1. Maîtrise de la production et de la prestation de service
7.5.3. Identification et traçabilité	8.5.2. Identification et traçabilité
7.5.5. Préservation du produit	8.5.4. Préservation
8.3. Maîtrise du produit non conforme	8.7. Maîtrise des éléments de sortie non conformes

II.3.2/ Exigences spécifiques

Pour chacun de ces chapitres le système qualité doit en outre être conforme aux exigences spécifiques définies ci-dessous.

4.2. Exigences relatives à la documentation (7.5. pour la version 2015 de l'ISO 9001)

Le titulaire doit mettre en place des dispositions destinées à s'assurer du respect des exigences relatives à la documentation définies dans la réglementation. En particulier, en lien avec la condition 1 du § III.2.1 et en application de l'article L. 102 D du LPF, les documents réglementaires doivent être conservés jusqu'à l'expiration de la troisième année suivant celle au cours de laquelle le logiciel ou le système de caisse a cessé d'être diffusé.

7.5.1. Maîtrise de la production et de la préparation du service (8.5.1. pour la version 2015 de l'ISO 9001)

La fourniture des documents nécessaires au bon fonctionnement des systèmes de caisse doit faire partie du service (mode d'emploi, prérequis matériel, etc.).

En cas de sous-traitance des activités de production des systèmes de caisse, cette dernière doit faire l'objet d'un contrat entre le fabricant et le sous-traitant. Dans ce contrat, le sous-traitant s'engage à produire des systèmes conformes au présent référentiel.

7.5.3. Identification et traçabilité (8.5.2. pour la version 2015 de l'ISO 9001)

Lorsque le titulaire prévoit l'apposition du marquage prévu au § IV.2, il doit prévoir des dispositions destinées à s'assurer du bon usage de la marque.

La traçabilité des produits doit permettre une traçabilité descendante (enregistrements des clients/distributeurs associés à chaque produit commercialisé).

8.3. Maîtrise du produit non conforme (8.7. pour la version 2015 de l'ISO 9001)

Il ne peut exister aucune dérogation aux exigences du présent référentiel.

Le fabricant doit traiter un produit non conforme suivant l'une des manières suivantes :

- en menant les actions permettant d'éliminer la non-conformité,
- en menant les actions permettant d'empêcher son utilisation,
- le cas échéant, en mettant en place toutes les dispositions nécessaires pour prévenir ses clients, et procéder au rappel des produits ou à leur mise à jour.

Chapitre III : Information des clients

La communication concernant la certification de produit ou de service ne doit pas être ambiguë pour le client quant au nom et au service / produit bénéficiaire de la certification.

La liste des produits certifiés est disponible sur le site www.lne.fr, dans "Certification", puis "Certification de produit et de service", via une recherche dans le moteur dédié. Le LNE fournit sur demande les informations relatives à la validité d'un certificat donné.

III.1/ Supports de communication

L'entreprise qui a un ou plusieurs de ses systèmes de caisse peut utiliser le logo sur ses supports de communication, comme par exemple :

- sur l'emballage du produit,
- sur l'étiquette du fabricant apposée sur le produit,
- sur les interfaces logicielles (fenêtre à propos par exemple),
- sur le papier à en-tête,
- sur le site internet,
- sur une plaquette de promotion publicitaire,
- etc.

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

Toute référence à la certification avant la notification de celle-ci est interdite. De même, en cas de retrait de certification ou d'échéance de validité, la référence à cette certification retirée ou échue est interdite.

Dans tous les cas de figure, l'utilisation de la marque ou la référence à la certification ne doivent porter à confusion, ni sur le système de caisse certifié, ni sur le fait que la certification porte sur un produit et non une entreprise ou un système de management de la qualité ou une prestation de service.

III.2/ Caractéristiques essentielles communiquées

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 :

- la marque LNE systèmes de caisse :

- le type de système de caisse et la version ou la version majeure couverte par le certificat correspondant,
- l'adresse du site internet du LNE.

L'entreprise s'engage à :
- faire des déclarations sur la certification en cohérence avec la portée du certificat,
- ne pas utiliser la certification délivrée par le LNE d'une manière qui puisse nuire au LNE, ni faire de déclaration sur la certification de ses produits que le LNE puisse considérer comme trompeuse ou non autorisée,
- faire référence à la certification de ses produits dans des supports de communication, tels que documents, brochures ou publicité, en indiquant :
    - systématiquement la révision du certificat si le numéro du certificat est mentionné,
    - que le certificat est délivré par le LNE,
- reproduire les certificats dans leur intégralité, avec les annexes le cas échéant, en cas de fourniture à un tiers.

Tout usage abusif de la marque ou référence abusive à la certification LNE peut faire l'objet de poursuites en application de la réglementation en vigueur.

Le certificat délivré par le LNE précise au minimum les éléments suivants :
- le nom du titulaire du certificat,
- le type du système de caisse, le cas échéant la portion du logiciel concernée par la certification,
- la version fixe ou la version majeure du système,
- la date de début de validité,
- dans le cas d'une version majeure, la racine de la dernière version majeure et les subdivisions de cette racine qui sont ou seront utilisées pour l'identification des versions mineures ultérieures,
- la mention que le système de caisse respecte les conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données prévues par la législation française au 3° bis du I de l'article 286 du CGI,
- une phrase invitant le lecteur du certificat à vérifier sur le site internet du LNE que le certificat est toujours en cours de validité au moment de sa consultation.

Note : dans le cas d'un système d'encaissement certifié pour un titulaire A et qui peut être commercialisé sous la marque d'une autre société B moyennant des dispositions contractuelles entre les sociétés A et B, il est possible d'identifier B comme distributeur du système d'encaissement sur le certificat de A, ou de procéder au transfert du certificat de A à B, sous réserve que B produise au LNE l'autorisation de A pour ce faire et fournisse les garanties de mettre sur le marché un système d'encaissement identique à celui certifié pour le titulaire A.

Chapitre IV : Conditions d'attribution et de surveillance du certificat

On distingue les rôles et responsabilités suivants pour l'attribution et la surveillance du certificat.

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 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.

Note : le paragraphe 310 du BOI-TVA-DECLA-30-10-30-20160803 indique que le titulaire est l'éditeur du logiciel ou du système de caisse.

Dans le cas d'un installateur réalisant un paramétrage du logiciel ou du système ayant pour objet ou pour effet de modifier un des paramètres permettant le respect des conditions de certification, la démarche de certification est réalisée intégralement et porte sur la vérification de la conformité de chaque exigence du référentiel. Le produit doit avoir son propre nom et sa propre identification au nom de l'installateur. L'installateur ne peut se prévaloir dans ce cas de la certification d'un produit existant.

Lorsque le titulaire n'est pas établi dans la communauté européenne, il doit obligatoirement désigner un mandataire.

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.

Note : un titulaire établi dans la communauté européenne peut mandater une entité pour le représenter, moyennant la présentation d'un mandat écrit.

IV.1 / Conditions d'attribution du certificat

Le processus d'attribution du certificat se découpe en 3 étapes successives. Ces étapes comprennent :

1. l'instruction du dossier de demande,

2. l'évaluation de la conformité d'un système aux exigences du § II.2
3. la réalisation d'un audit destiné à s'assurer de la conformité du système qualité mis en place aux exigences du § II.3.

La décision de certification s'appuie sur l'examen des éléments du dossier, du rapport de l'évaluation et de l'audit. Chaque décision de certification est matérialisée par 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 n'est apportée. Il appartient à l'entreprise de signaler au LNE les modifications afin de faire réaliser les évaluations nécessaires à la révision du certificat.

Schéma n° 1 – processus d'attribution du certificat

LNE	Responsable d'évaluation	Entreprise
		1. Demande d'information
2. Envoi du questionnaire		3. Retour du questionnaire complété
4. Etablissement de l'offre		5. Acceptation de l'offre
		6. Envoi du dossier technique
7. Examen de la recevabilité OUI : planification évaluation NON : demandes complémentaires à l'entreprise		
8. Planification de l'évaluation : période, équipe d'évaluation, lieu	9. Programmation de l'évaluation avec l'entreprise	
	10. Réalisation de l'évaluation : préparation (examen du dossier technique), évaluation sur site, rapport d'évaluation	
	11. Envoi du rapport d'évaluation au LNE	
12. Examen du rapport d'évaluation CONFORME : présentation en comité de lecture NON CONFORME : demandes complémentaires à l'entreprise puis programmation d'une évaluation complémentaire (cf. n° 10)		12. Si Evaluation non conforme, envoi des demandes complémentaires et corrections sur le système de caisse
13. Consultation du comité de lecture		
14. Décision sur l'attribution de la certification et information de l'entreprise		
15. Enregistrement du certificat		

Point n° 7 - Examen de la recevabilité

Envoi des extraits de la documentation technique et réglementaire prévue dans les conditions 1 à 30 permettant d'appréhender le fonctionnement du système de caisse et les méthodes employées pour répondre aux exigences.

Tous les documents doivent être rédigés en français ou en anglais, exception faite des documents exigés par l'administration fiscale qui sont obligatoirement en français.

Point n° 10 - Organisation de l'évaluation

Lorsque les titulaires possèdent un système de management de la qualité certifié par un organisme de certification accrédité selon l'ISO 9001 version 2008 ou version 2015 et dont le champ inclut la conception et la vente de système de caisse, les exigences définies au § II.3.1 sont réputées satisfaites.

L'examen du système de management de la qualité a lieu chez le titulaire ou sur le site du management du système qualité. Lorsqu'un titulaire souhaite certifier ou dispose de plusieurs systèmes de caisse, l'examen du système de management de la qualité est mutualisé pour l'ensemble des systèmes.

La durée d'audit est fixée au cas par cas, mais ne peut être inférieure à une journée.

La durée des vérifications fonctionnelles d'un système de caisse est liée à sa complexité et est fixée individuellement mais ne peut être inférieure à une journée. Ces vérifications portent systématiquement sur l'ensemble des conditions techniques du référentiel.

De même, la durée des vérifications de la robustesse d'un système de caisse est liée à sa complexité et est fixée individuellement mais ne peut être inférieure à une journée. Ces vérifications portent systématiquement sur l'ensemble des conditions techniques du référentiel.

IV.2 / Surveillance du certificat

Il est procédé à une évaluation de surveillance annuelle selon le schéma ci-dessous.

Schéma n° 2 – processus de surveillance du certificat

LNE	Responsable d'évaluation	Entreprise
1. Envoi du questionnaire pour connaître les évolutions depuis la précédente évaluation		2. Retour du questionnaire complété
3. Etablissement de l'offre		4. Acceptation de l'offre
5. Planification de l'évaluation : équipe d'évaluation, lieu	6. Programmation de l'évaluation avec l'entreprise	
	7. Réalisation de l'évaluation	
	8. Envoi du rapport d'évaluation au LNE	
9. Examen du rapport d'évaluation CONFORME : présentation en comité de lecture		10. Si Evaluation non conforme, envoi des demandes complémentaires et corrections sur le système de caisse

LNE	Responsable d'évaluation	Entreprise
NON CONFORME : demandes complémentaires à l'entreprise puis programmation d'une évaluation complémentaire le cas échéant (cf. n° 6)		
11. Consultation du comité de lecture		
14. Décision sur le maintien de la certification et information de l'entreprise		
Retour à la phase n° 1 de ce schéma pour la surveillance suivante		

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

Système de caisse certifié en version fixe : l'évaluation annuelle porte sur l'examen du système de management de la qualité du titulaire. Le but de l'évaluation est de s'assurer que le système est maintenu afin de produire des systèmes identiques au type certifié.

Système de caisse certifié en version majeure et sans évolution de la version mineure : l'évaluation porte sur l'examen du système de management de la qualité du titulaire.

Système de caisse certifié en version majeure et avec évolution de la version mineure : l'évaluation annuelle porte sur l'examen du système de management de la qualité du titulaire et sur l'examen des vérifications fonctionnelles d'un système de caisse.

Système de caisse certifié en version majeure avec évolution de la version majeure : l'évaluation est par défaut une évaluation initiale avec l'examen de l'ensemble des dispositions du référentiel, sauf cas très particulier qui ne le justifierait pas (par exemple, changement de l'outil de compilation du logiciel sans modification de la version majeure). Dans ce cas très particulier, l'éditeur transmet toutes les documentations nécessaires pour justifier de l'absence d'impact sur la version majeure et le LNE fixe les modalités d'évaluation.

IV.3/ Cas particuliers

Comme indiqué ci-avant, les systèmes de caisse font l'objet d'une évaluation initiale. Si cette évaluation permet de certifier le système, le certificat demeure valable tant qu'aucune modification n'est apportée au système. Il appartient à l'entreprise de signaler au LNE les modifications envisagées afin d'évaluer l'impact sur le produit certifié et les modalités de réévaluation qui par défaut sont celles d'une évaluation initiale.

Dans le cas particulier d'un système de caisse certifié en version majeure et dont le titulaire de la certification souhaiterait réviser le certificat pour citer une version fixe (par exemple,

fin d'exploitation d'un système), il doit en faire la demande au LNE qui examinera au cas par cas l'impact sur la certification et les modalités d'évaluation correspondantes.

IV.4/ Comité de marque

IV.4.1 / Modalités de fonctionnement

Il est constitué un comité de marque dont les attributions 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.

Le comité de marque se réunit au minimum une fois par an en réunion ordinaire. Des comités extraordinaires peuvent être organisés chaque fois que nécessaire (par exemple en vue de modifier les règles de certification).

Préalablement à la réunion du comité, le LNE transmet aux membres du comité, un ordre du jour de la séance accompagné, le cas échéant, des documents associés. Le LNE rédige le compte-rendu des observations et propositions formulées en réunion de comité. Ce compte-rendu est adressé à tous les membres du comité. Le cas échéant, un bureau du comité ou des groupes de travail pourront compléter le dispositif pour gagner en efficacité.

La composition nominative du comité de marque est approuvée par le directeur général du LNE ou son délégué, chaque membre en étant ensuite informé. Le mandat des membres est de 3 ans, il est renouvelable par tacite reconduction.

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 le titulaire.

IV.4.2 / Rôle, engagements et composition du comité

Les membres du comité s'engagent :

- à contribuer de par leur expertise au bon fonctionnement de la marque de certification des systèmes de caisse,
- à conserver la confidentialité des échanges et informations communiqués au cours des réunions du comité de marque et ceci jusqu'à leur publication par le LNE,
- à participer régulièrement aux réunions,
- à contribuer au développement de la marque de certification et promouvoir les prestations certifiées.

Le comité est composé comme suit :

- 3 représentants des clients certifiés :
    - 1 représentant parmi les éditeurs de logiciel,
    - 1 représentant parmi les fabricants de caisses,

    - 1 représentant parmi les fabricants de dispositifs d'encaissement associés à un instrument de mesure réglementé,
- 2 représentants des associations ou organismes représentatifs des consommateurs et / ou des utilisateurs ou à défaut les utilisateurs eux-mêmes.

Chaque collège dispose d'une voix. Aucune des parties intéressées ne peut faire valoir un droit de veto.

Le LNE assure le secrétariat du comité.

IV.4.3 / 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 extérieurs 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.

IV.5 / 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 du LNE (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 du LNE.

Ce comité de lecture a pour mission :

- d'examiner les rapports d'évaluation et de formuler un avis et une recommandation sur les décisions à prendre,
- le cas échéant, d'examiner dans un premier temps les appels contre les décisions du LNE et de formuler un avis sur les suites à donner,
- d'évaluer la qualité des rapports d'évaluation.

Chapitre V : Recours et traitement des plaintes

V.1 / Recours contre décision

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

Dans un premier temps, le LNE 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 au LNE par lettre recommandée avec accusé réception dans un délai de 15 jours ouvrés. Ce recours, non suspensif de la décision du LNE, doit être motivé. Il est instruit par le LNE 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. Le LNE 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 du LNE, qui après examen, propose ses conclusions. La décision finale est notifiée par le LNE 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.

V.2/ Traitement des plaintes

Toute plainte concernant des produits fait l'objet d'un examen par le LNE 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, le LNE les examine et le cas échéant contacte l'entreprise concernée.

L'Entreprise concernée doit alors informer le LNE des suites apportées et tenir à disposition du LNE, 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, le LNE examine les enregistrements relatifs aux plaintes et réclamations et vérifie que les corrections et actions correctives appropriées ont été entreprises.

Chapitre VI : Glossaire et lexique

VI.1/ Glossaire

BOFIP	Bulletin Officiel des Finances Publiques Ancienne appellation : BOI (Bulletin Officiel des Impôts)
CA	Chiffre d'Affaires
CC	Code de Commerce
CGI	Code Général des Impôts
CPC	Chef de Projet Certification
DGFIP	Direction Générale des Finances Publiques
DCR	Direction de la Certification et des Référentiels
LPF	Livre des Procédures Fiscales
LNE	Laboratoire National de Métrologie et d'Essais
TVA	Taxe sur la Valeur Ajoutée

VI.2/ Lexique

Archivage	Enregistrement des données de manière à garantir sur le long terme leur conformité à un état donné.
Clôture comptable	Opération périodique figeant les écritures comptables.
Concepteur de logiciel	Auteur du logiciel au sens du code de la propriété intellectuelle (C. prop.intell., art. L. 113-1). Lorsque le logiciel a été créé par un employé dans l'exercice de ses fonctions ou d'après les instructions de son employeur, le concepteur s'entend à la fois du salarié et de l'employeur, ce dernier étant en principe seul habilité à exercer les droits patrimoniaux sur le logiciel ainsi créé, conformément à l'article L. 113-9 du code de la propriété intellectuelle. [Source : BOI-CF-COM-10-80-20160803]
Correction d'une donnée	Modification ou annulation d'une donnée.
Cumul du grand total	Cumul du chiffre d'affaires pour une période donnée, de son ouverture à sa clôture. Applicable aux systèmes d'encaissement faisant des purges.
Donnée élémentaire	Données immatérielles traitées par des procédés informatiques qui concourent 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 visés par le droit de contrôle.
Donnée d'encaissement	Donnée de règlement
Ecriture comptable	Opération consistant à enregistrer un flux commercial, économique ou financier à l'intérieur de comptes. Les écritures sont portées dans un document appelé journal.
Editeur de logiciel	Personne qui détient le code source du logiciel ou système et qui

	a la maîtrise de la modification des paramètres de ce produit.
Encaissement	Action de mettre en caisse.
Enregistrement	Ecriture des données dans une base de données ou sur un périphérique (par exemple, disque dur, clé USB, etc.) où les informations resteront présentes même après l'arrêt de la machine. Cet enregistrement peut être matériel ou immatériel.
Exercice	Période de calcul du résultat.
Facture	Document commercial établi par le vendeur, qui le remet à l'acheteur et sur lequel ont été portés les détails des marchandises vendues et les conditions de la vente, incluant les conditions de prix. La facture sert de pièce justificative pour les enregistrements des achats et des ventes.
Grand total	Chiffre d'affaires total de la période Applicable aux systèmes d'encaissement faisant des purges.
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.
Identification logicielle	Séquence de caractères lisibles (par exemple un numéro de version ou une somme de contrôle) qui est inextricablement liée au logiciel. Elle peut être vérifiée sur l'instrument en cours d'utilisation.
Inaltérable	Caractéristique d'un système dont rien ne peut changer les données enregistrées sans traçabilité (i.e. sans que le système ne le détecte).
Intégrité	Etat de quelque chose qui a conservé son état d'origine
Interface logicielle	Code programme et domaine de données dédiés qui reçoivent, filtrent ou transmettent les données entre les modules logiciels. [Source : OIML D31 :2008]
Journal comptable	Document comptable qui enregistre de façon chronologique toutes les opérations quotidiennes effectuées par l'entreprise.
Logiciel de comptabilité	Programme permettant à un appareil d'assurer tout ou partie des tâches de la comptabilité d'une entreprise en enregistrant et traitant toutes les transactions réalisées par l'entreprise dans différents modules fonctionnels (comptabilité fournisseurs, comptabilité clients, paie, grand livre, etc.).
Logiciel de gestion	Programme permettant à un appareil d'assurer des tâches de gestion commerciale : gestion automatisée des devis, des factures, des commandes, des bons de livraison, suivi des achats et des stocks, suivi du chiffre d'affaires, etc. Les données peuvent provenir de systèmes tiers (front et back office).
Logiciel d'encaissement	Programme permettant le pilotage et la gestion des activités de vente et d'encaissement par l'utilisation de terminaux de vente dédiés ou non dédiés, quelles que soient les modalités de leur

	mise sur le marché (vente, location, mise à disposition de toute autre manière, etc.).
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.
Mode école	Mode de fonctionnement optionnel d'un système de caisse dédié à la formation, permettant de réaliser des transactions et des encaissements qui sont enregistrés mais pas comptabilisés dans les écritures.
Note	Document indiquant au moins un total à payer et remis au client pour réaliser un encaissement. Document à caractère provisoire, ne faisant pas office de pièce justificative d'encaissement (ticket ou facture).
Période	Intervalle de temps.
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.
Purge	Suppression irréversible d'enregistrements dans un système de données informatiques.
Sauvegarde	Opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique
Séparation logicielle	Division d'un logicielle en une partie réglementairement pertinente et une partie non réglementairement pertinente. Ces parties communiquent via une interface logicielle.
Système de caisse	Système d'information doté d'un ou plusieurs logiciels permettant l'enregistrement des opérations d'encaissement. On distingue notamment : - les systèmes de caisse autonomes (caisses enregistreuses et balances par exemple) : ils ont la capacité d'enregistrer des données de règlement mais n'ont pas la capacité d'être paramétrés pour avoir un fonctionnement en communication avec d'autres systèmes de caisse ou avec un système centralisateur d'encaissement. Toutefois, ils sont paramétrables pour fonctionner en réseau avec des systèmes de même type. - les systèmes de caisse reliés à un système informatisé capables d'enregistrer, de sécuriser et d'archiver les données d'encaissement en temps réel directement dans le système ; selon le cas, ils génèrent ou non directement les écritures comptables ; - les logiciels d'encaissement installés sur un ordinateur ou des ordinateurs (en réseau ou non) : outre les fonctionnalités d'enregistrement, de sécurisation et d'archivage des données d'encaissement en temps réel directement dans le système, ils disposent de fonctionnalités comptables (tenue des écritures comptables) et plus largement incorporent une gestion comptable et financière. Dans tous les cas pour le premier type de caisses et suivant le cas, pour certaines caisses du deuxième type, les écritures comptables ne sont pas directement générées par le système de caisse à partir des données

	d'encaissement enregistrées. Les données d'encaissement sont alors exportées (par exemple à l'aide d'une clé usb, ou par leur remontée vers un ordinateur ou un serveur via un logiciel de « back office ») pour permettre la tenue de la comptabilité et des écritures du livre-journal. Sont ainsi concernés tous les systèmes informatisés comptables, tous les systèmes de gestion commerciale et d'encaissement qui enregistrent des données ou informations concourant à la détermination du résultat comptable, et plus généralement, tous les systèmes de caisse, c'est-à-dire tous les matériels permettant l'enregistrement des opérations d'encaissement, notamment de ventes et de prestations de services. Le droit de communication s'exerce donc aussi sur les caisses enregistreuses non informatisées. [Source : BOI-CF-COM-10-80 § 180 MAJ 03/08/2016]
Ticket	Document indiquant un total à payer et remis au client pour finaliser un encaissement.
Total perpétuel	Chiffre d'affaires total depuis le début d'utilisation du système et ne se remettant jamais à zéro. Applicable aux systèmes d'encaissement faisant des purges.
Traçabilité	aptitude à retrouver l'historique, la mise en œuvre ou l'emplacement de ce qui est examiné.
Verrouillage de période	Clôture de période du système d'encaissement figeant les données qui pourront être exploitées en vue d'une clôture comptable.
Version majeure	Toute nouvelle version d'un système ou logiciel obtenue en ayant modifié, dans la précédente version de ce logiciel ou système, un ou plusieurs paramètres impactant le respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données.
Version mineure	Toute version d'un logiciel ou système obtenue sans que les paramètres impactant le respect des conditions précitées aient été modifiés par rapport à la précédente version de ce logiciel ou système.