Standard for the certification of cash register systems

Author’s ref: LNE/CITI/CH

Revision No. 1.4 – January 2019

LNE approval: 24/01/2019

This document is an unofficial translation of the certification standard. Original wording is in French language. In case of litigation refer back to the text in French language. No legal claims or duties can be derived from the translation.
VII.2) Requirements correspondence table V1.2/V1.4

V.3) Standards and reference documents

V.2) Procedures for drafting and validating the standard

V.1) Mark committee

V.1.3) Working Group

V.1.2) Role, commitments and composition of the committee

V.1.1) Operational procedures

V.2) Procedures for drafting and validating the standard

V.3) Standards and reference documents

Chapter VI: Appeals and treatment of complaints

VI.1) Appeal against a decision

VI.2) Treatment of complaints

Section VII: Annexes

VII.1) Glossary

VII.2) Requirements correspondence table V1.2/V1.4
## Document revisions

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Reason for the update</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>29/11/2016</td>
<td>Initial version</td>
</tr>
<tr>
<td>1.1</td>
<td>07/12/2016</td>
<td>Further details provided for Chapters I.3/ scope (exclusion of electronic cash) and V.4 / mark committee (deletion of the president and addition of the impossibility of the right of veto in compliance with standard NF X50-067) following the first mark committee of 06/12/2016.</td>
</tr>
<tr>
<td>1.2</td>
<td>12/12/2016</td>
<td>Change to the composition of the mark committee (V.4). Amendment of the appeals and complaints procedure (VI).</td>
</tr>
</tbody>
</table>
| 1.3     | DRAFT     | Entire document: integration of the FAQ of the DGFIP for secure cash register software dated 28/07/2017  
§ I.3: further details provided regarding the scope of the standard  
§ II.2: integration of feedback in order to draft conditions  
§ III: further details provided on the LNE cash register system mark and the commitments of certification holders  
§ IV: further details provided on the initial assessment and monitoring procedures.  
Glossary: addition of definitions |
| 1.4     | 24/01/219  | • Integration of changes to the version of BOI-TVA-DECLA-30-10-30 updated on 04/07/2018  
  o Inclusion of further details derived from the FAQ of 28 July 2017  
  o Use of an open archive format  
  o Obligation to offer three levels of closure  
  o Redefinition of the cash register system  
  o Further details on the data concerned  
  o Obligation to track purging/archiving operations  
• Reorganisation of the different sections of the standard  
• Clarification on the difference between certification/attestation  
• Further details on the certification process  
• Recast of the quality requirements  
• Reorganisation of the technical requirements  
• Addition of the establishment identifier to the data concerned  
• Addition of receipt securisation  
• Update of the examples of acceptable solutions in the mechanisms guaranteeing the inalterability of data |
Chapter I: General information

I.1) Purpose & VAT liable taxpayers concerned

In order to fight VAT fraud associated with the use of systems that enable cash receipts to be concealed, the finance law for 2016 established the obligation, for all VAT liable professional taxpayers who deliver goods and services to individual customers and record the corresponding payments received by means of a cash register system, to use a secure cash register system. This system must thus be certified by an independent body accredited by COFRAC or attested by the editor as being compliant with the fiscal regulations using an individual attestation¹.

This obligation concerns all sectors of activity, it being recalled that the finance law for 2018 excluded from the measure those VAT liable taxpayers benefitting from a basic exemption regime, those subject to an agricultural VAT reimbursement regime, those who exclusively perform operations that are VAT exempt² and those who perform the entirety of their operations exclusively among professionals (B to B).

This standard describes the procedures for the certification of cash register systems. They are essentially based on article 88 of finance law No. 2015-1785 of 29 December 2015 for 2016 and the official bulletin for public finance BOI-TVA-DECLA-30-10-30-20180704, which defines the conditions of inalterability, security, conservation and archiving of transaction data that the system must satisfy. This standard aims to certify these 4 characteristics, the characterisation of the fiscal scope of the system and the versions of the system, the documentation relating to the system, and the organisation (CMS³) implemented to ensure the production and delivery of cash register systems that comply with the certified version.

I.2) Scope: definition of a cash register system

A cash register system is an IT system (regardless of its qualification: management, CRM, accounting, etc.) with a cash register function.

A cash register function consists in memorising and recording, off the balance sheet, payments received in respect of the sale of goods or services, regardless of the means of payment. Recording off the balance sheet means that a payment registered by the system does not simultaneously, automatically, obligatorily and without human intervention generate an entry in the accounting system⁴.

Certain specific exclusions exist and are laid down in BOI-TVA-DECLA-30-10-30. It is not the role of the LNE to decide on the applicability of this BOI (official tax bulletin) regarding the system concerned.

¹ BOI-TVA-DECLA-30-10-30-20180704: point 1.
² BOI-TVA-DECLA-30-10-30-20180704: point 25.
³ CMS: Compliance Management System
⁴ BOI-TVA-DECLA-30-10-30-20180704: point 30.
I.3) Attestation or certification?

Certification is a procedure whereby a third party, the certifying body, gives written assurance that a system of organisation, process, person, product or service complies with the requirements specified in a standard or a norm. It falls within the framework of the Consumer Code. It must not be confused with an individual attestation supplied by the editor, which is a declaration by which the editor declares that the cash register system they supply respects the conditions of inalterability, security, conservation and archiving of transaction data.

In the context of the finance law for 2016, product certification by an accredited body is obligatory for VAT-liable taxpayers who edit their own cash register system\textsuperscript{5}.

\textsuperscript{5} BOI-TVA-DECLA-30-10-30-20180704: point 375.
Chapter II: Certificate attribution process

II.1) Ordering process
After initial contact and exchange of information, the commercial department of the LNE sends an initial questionnaire to the certification applicant, which must be completed and returned in order to establish a quote. The commercial department then sends the applicant a certification proposal. Once the application has been registered, the certification process can begin.

II.2) Certification process
The certification process is divided into several successive stages. The main ones are:
1. examination of the application file: documentary admissibility review;
2. performance of the certification audit:
   it is divided into four assessments of a minimum duration of one day each:
   o the organisational audit designed to ensure that the CMS implemented complies with the requirements of Chapter III;
   o assessment of the documentary compliance of the system with the requirements of Chapter IV;
   o assessment of the functional compliance of the system with the requirements of Chapter IV;
   o assessment of the robustness compliance of the system with the requirements of Chapter IV;
3. feedback via the non-compliance forms if necessary;
4. the certification decision taken in a reading committee;
5. issue of the certificate once the decision has been endorsed.

II.2.1) documentary admissibility review
Once the application has been registered, the LNE sends the applicant the documentary admissibility form.

This form must be returned to the LNE, completed and accompanied by the technical file comprising the documentation relating to the system. This documentation must be complete and must precisely describe all of the functions and mechanisms implemented to ensure compliance and make it possible to meet the technical requirements of the LNE standard.

The documentary admissibility review is not equivalent to the documentary assessment performed during the certification audit.

The documentary admissibility review consists in determining whether it is possible to assess the compliance of the cash register system given the degree of completion of the technical file provided by the applicant. To do this, it is ascertained whether:
- any documents needed for Requirement 1 of Chapter IV are missing;
- all or part of the regulatory documentation is not written in French (see requirement no 1 of Chapter IV);
- the fiscal scope and management of the version numbers are well defined;
- the principle of the methods proposed to meet the requirements of Chapter IV is relevant.

---

6 CF: Chapter IV: technical requirements applicable to the certified cash register system
Following the documentary admissibility review, the LNE informs the applicant of the result.

Should the file be deemed inadmissible at this stage, it is the applicant’s responsibility to respond to the LNE by providing the missing documents. An additional quote will be sent by the commercial department of the LNE if a second documentary admissibility review is necessary.

**II.2.2) Scheduling the certification audit**

If the documentary admissibility review is satisfactory, the certification application file is admissible and the LNE contacts the applicant in order to define the locations and dates of the various stages of the audit.

The duration of the organisational audit may be increased if it is necessary to travel to several sites, if subcontractors participate in the design, development, tests, configuration/installation of the system to be certified and are not supervised by the certification holder, or if it is necessary to employ the services of an interpreter. The default duration is one day. This may be reduced provided that the applicant can demonstrate that they possess an ISO 9001 QMS for the activities covered by the standard.

The duration of the documentary, functional and robustness assessments of a cash register system is related to its complexity; it is set by default at one day per assessment. It may be increased, notably after the documentary admissibility review, depending on the complexity of the cash register system (several human-machine interfaces, configurations and/or data flows to be tested, system architecture, etc.).

**II.2.3) Performance of the certification audit**

Several assessments may take place at the same time, depending on the composition of the audit team.

It is recalled that auditing is based on sampling of the available information. The absence of non-compliance constitutes a presumption and not a proof of compliance with the audited requirements.

**II.2.3.1): Organisational audit**

The certification applicant must implement a Compliance Management System (CMS) designed to ensure that each cash register system produced or update deployed meets the requirements of Chapter IV.

The requirements applicable to this CMS are defined in Chapter III and checked during the organisational audit to ensure that they are being correctly applied.

The organisational audit of the CMS takes place on the applicant’s premises, preferably on the site where the design, development and testing activities concerning the system to be certified are performed. When an applicant wishes to certify several cash register systems, the organisational audit can be mutualised for all the systems.
The certification applicant must ensure the availability of a contact person with a grasp of the CMS implemented and the organisation of the company and its processes, as well as any other person considered relevant.

II.2.3.2) Robustness assessment

The objective of the robustness assessment of a cash register system is to check compliance with the robustness requirements defined in Chapter IV. The certification applicant must ensure the availability of:

- an expert technician with a grasp of the design, development/manufacture (knowing the source code), configuration and use of the cash register system to be certified;
- a connected and functional cash register system in a test environment (notably with the possibility to easily modify the date of the system) with all the related peripherals (printers, displays, remote controls, etc.) and any possible connections or configurations (to a PC, server or any other centralised system);
- a cash register system in a development environment (with full access to the source code, direct access to databases, servers, etc.);
- access to user and technical documentation.

II.2.3.3) Documentary assessment

The objective of the documentary assessment of the cash register system is to check compliance with the documentary requirements defined in Chapter IV. The certification applicant must ensure the availability of:

- a contact person with a grasp of the documentation and the design of the cash register system to be certified;
- the regulatory documentation\(^7\) in French;
- complementary documentation\(^8\) in French or English;
- all the documentation for the assessor, as well as a relevant means of transfer. The documents will be kept by the LNE as proof of the audit.

II.2.3.4) Functional assessment

The objective of the functional assessment of the cash register system is to check compliance with the functional requirements defined in Chapter IV. The certification applicant must ensure the availability of:

- a contact person with a grasp of the design, development/manufacture, configuration and use of the cash register system to be certified;
- a connected and functional cash register system in a test environment (notably with the possibility to easily modify the date and the transaction data of the system) with all the related peripherals (printers, displays, remote controls, etc.) and any possible connections or configurations (to a PC, server or any other centralised system);
- a sufficiently large payment data set to be able to perform the standard test routines: periodic closure (daily, weekly, monthly), data synchronisation, archiving, etc.

---

\(^7\) CF: Chapter IV Requirement 1
\(^8\) CF: Chapter IV Requirement 2
II.2.4) Response to non-compliance reports

If non-compliance is observed during one of the stages of the certification audit, a form describing the NC\(^9\) is drafted by the assessor\(^{10}\)/auditor\(^{11}\). This is transmitted by the LA\(^{12}\) to the certification applicant during the closing meeting of the certification audit.

Two categories of NCs are distinguished:

1) CMS ‘system’ NCs (Chapter III)
   These may be minor or major.
   - A major NC blocks certification: it must be corrected before certification.
   - A minor NC does not block certification but must be corrected before the next monitoring audit, under penalty of suspension of the certificate.

2) Cash register system ‘product’ NCs (Chapter IV)
   Any product NC blocks certification: it must be corrected before certification.
   - If the NC is purely documentary, the LA or the LNE can dismiss it once the appropriate documents have been provided.

The certification applicant then has a deadline fixed by the LA (at least three weeks) to return each completed NC form with the analysis of the NC and the action undertaken.

After analysis of the actions proposed by the certification applicant, the LA decides on their relevance and recommends the type of follow-up necessary for the NC.

II.2.5) Opinion of the Evaluation Manager and report review

Once it has received any NC reports completed by the certification applicant and the AM, the LNE analyses the assessment report and the opinion of the assessment manager. After reading the report, they may request that the applicant provide complementary information before it is presented to the reading committee.

II.2.6) Decision of the reading committee

The reading committee is charged of giving an opinion on the certification decision in the process of awarding, monitoring, withdrawing or suspending certificates. It is composed of at least:

- one representative of the LNE management (who may not be involved as the certification project manager and who has not participated in the assessment);
- a certification project manager not in charge of the file;
- a certification project manager in charge of presenting the file.

The committee is chaired by a representative of the LNE management and its role is to:

- examine the assessment reports and express an opinion and a recommendation on the decisions to be made, notably on the type and duration of NC monitoring;
- if necessary, make an initial examination of appeals against LNE decisions and to express an opinion on the appropriate follow-up;
- assess the quality of the assessment reports.

---

\(^{9}\) NC: Non-compliance
\(^{10}\) Assessor for stages 2/3/4: assessments of the cash register system (Chapter IV)
\(^{11}\) Auditor for stage 1: organisational audit on the compliance management system (Chapter III)
\(^{12}\) LA: Lead Auditor
The certification decision will be based on examination of the documents in the file and the certification audit report. Each certification decision is finalised by the registration and, where appropriate, the issuance of a certificate.

Certificates are issued without an expiry date and remain valid as long as there are no changes to the certified characteristics (fiscal scope). It is the company’s responsibility to inform the LNE of any changes in order to perform the assessments necessary for revision of the certificate.

II.3) Certificate monitoring

A monitoring assessment is performed yearly. The content of the yearly assessment varies on a case-by-case basis; its duration may not be less than one day.

In order to schedule this monitoring assessment, the LNE sends a questionnaire to the company whose system has been certified in order to identify any changes that have occurred since the previous assessment. Once the questionnaire has been returned, the LNE establishes a proposal for monitoring according to the changes made.

Depending on the changes, the monitoring assessment procedures are as follows:

- **If the certified system has not undergone any changes:**
  The yearly monitoring audit covers the certificate holder’s CMS audit and the checks intended to confirm that there have been no changes to the system (comparison of the fingerprint). It lasts 1 day. The objective of the assessment is to ensure that the CMS is maintained in order to produce cash register systems that are identical to the one being certified and that the traceability of the distributed systems is ensured.

- **If the certified system has undergone a change in its fiscal scope** (and thus a change in its major version):
  The yearly monitoring audit is by default considered to be an initial assessment with examination of all the documentary, functional and robustness requirements listed in Chapter IV as well as the organisational requirements relating to the CMS listed in Chapter III. Its duration depends on the changes made to the system.

  **NB:** in the event of any change in the fiscal scope, the company must inform LNE of the changes made before it can distribute this version. The certificate effectively only covers the system for a given major version.

- **If the certified system has undergone a minor change** (i.e. with no change in the fiscal scope):
  The yearly monitoring audit covers the certificate holder’s CMS and functional checks to ensure that the later minor versions of the cash register system continue to respond to the 4 conditions for transaction data defined by the BOI\textsuperscript{13}, as well as the absence of changes in the fiscal scope of the system (comparison of the fingerprint). It lasts 2 days.

---

\textsuperscript{13} BOI-TVA-DECLA-30-10-30-20180704: point 330.
Once the order has been placed, the steps below are identical to those of the initial certification audit:

1. scheduling of the monitoring audit;
2. performance of the monitoring audit (according to the previous assessment procedures);
3. responses to any NC reports;
4. report review;
5. decision of the reading committee.
Chapter III: Requirements applicable to the compliance management system (CMS)

The certification applicant/holder must implement, evaluate and update a Compliance Management System (CMS) designed to ensure that each cash register system or update distributed continues to meet the requirements of this standard.

This CMS must respect the requirements defined below.

NB: any future mention of the action of recording data or producing a recording refers to the requirements of III.14) of this chapter.

III.1) Context

The entity must determine and register the internal and external issues as well as the risks (legal, reputation, financial, etc.) associated with the compliance of the cash register system distributed.

To do so, the entity must notably take into account the external regulatory and economic contexts, but also the entity’s internal context (resources, processes, suppliers, subcontractors, etc.). This may, for example, be done by implementing a risk management process, risk mapping or through a SWOT analysis.

III.2) Commitments and responsibilities of the company

Certified companies are solely responsible for the compliance of their products; LNE inspections cannot substitute their responsibilities.

For the certified products, the companies undertake to:

- exclusively produce cash register systems that are compliant with this certification standard;
- ensure that all certified cash register systems distributed continue to meet the requirements concerning them;
- implement the appropriate changes in the event of new requirements;
- take all measures necessary for performance of the initial and monitoring assessments:
  - provide the technical file and, when appropriate, the necessary samples, access to sites, zones, personnel and subcontractors concerned by the assessment if necessary;
  - examine the non-compliance issues expressed in the assessment reports;
  - participation of observers when appropriate;
- only provide true and accurate information;
- promptly inform the LNE of any changes that might have consequences on the compliance of the system or the validity of the certification issued (change of legal status, changes to/update of the certified system, etc.).
III.3) Roles and responsibilities

The management must entrust and transfer responsibility and authority to the person in charge of compliance to:

a) ensure that the compliance management system complies with Chapter III;
b) analyse the technical requirements defined in Chapter IV;
c) break them down into functional specifications that can be implemented;
d) provide or organise training/information sessions for the employees concerned in order to ensure that they are aware of the compliance requirements that concern them;
e) define compliance performance indicators;
f) check and measure these indicators;
g) analyse the results to identify whether corrective actions are necessary;
h) identify and manage the risks associated with compliance in relation to third parties such as suppliers, agents, distributors, consultants and subcontractors;
i) supervise outsourcing conditions in order to ensure that they take into account the compliance requirements defined in this standard.

The management must ensure that the responsibilities and authorities for each activity relating to cash register systems are defined in such a way as to ensure that the requirements defined in this standard are systematically and continuously implemented.

III.4) Objectives and implementation of the CMS

The entity must take into account the issues, risks and requirements of this standard to define the objectives of the CMS and to break them down at each level and function into compliance objectives for the activities of designing, developing, testing, distributing, configuring installing the cash register standard, assessing the CMS and processing NCs.

These compliance objectives must be:

- relevant;
- consistent with the objectives of the CMS;
- measurable;
- communicated to the persons concerned;
- understood and applied;
- regularly monitored by a person in charge of compliance;
- updated if necessary;
- recorded.

The entity must ensure that the CMS can obtain the expected results and prevent or reduce the risks. For this, they must notably plan:

- the relevant actions to implement related to:
  - the issues;
  - the risks;
  - the requirements;
- the integration of these actions into the activities concerned;
- the assessment (and record) of the efficiency of these actions.
III.5) Updating the CMS

As the context evolves, the entity must be in a position to identify new aspects and changes to the legislation, directives, regulations and compliance requirements in order to ensure sustainability in the compliance of cash register systems.

For example, the entity may:

- be the recipient of the information bulletins of regulatory (DGFIP, ministries, etc.) and certification bodies (LNE).
- follow or participate in professional work groups;
- subscribe to appropriate newsletters;
- participate in professional events within the sector;
- regularly consult the websites of regulatory and certification bodies;
- call on the services of legal advisors;
- etc.

The impact of these changes must be assessed and the resulting actions (and changes to the CMS) must be performed, monitored and recorded. Should the requirements change, the functional specifications must clearly identify these changes.

III.6) Establishment of compliance checks

The entity must:

- implement and record effective checks for each activity relating to the cash register system (design, development, integration, configuration/installation) in order to ensure that the requirements are met and that non-compliance is avoided or detected and corrected;
- designate competent persons with a grasp of the requirements of the standard to perform these checks;
- record the results of these checks;
- in the event of non-compliance, record the analysis of the cause and the actions taken in order to correct the NC;
- ensure that the defined checks have been properly performed at the correct stages and that the results demonstrate the compliance of the cash register system with this standard.

These checks may be based on:

- documented, clear, practical and easy-to-follow policies, procedures, processes and operational work instructions;
- systems and anomaly reports;
- code reviews or approvals;
- test plans and reports;
- a separation of incompatible roles and responsibilities;
- automated processes;
- yearly compliance schedules;
- compliance audits

III.7) Design and development of the cash register system

The entity must implement, in a controlled manner, and record, a design process and a development process for the cash register system or appropriate updating thereof, to
ensure the supply of cash register systems that comply with the requirements of this standard.

The elements resulting from the design process that must be recorded include at least all of the functional specifications related to compliance with this standard and the associated test plans.

The outcome of the development process is a prototype or an update of a cash register system compliant with this standard, as well as, at least, the recording of compliance test reports.

The following elements of the development process must be defined and recorded:
- the development method followed (V model, W model, agile method, method specific to the entity, etc.);
- the management of the source code: explanation of the organisation of directories, source code files, classes, packages, libraries, dll, etc.;
- the fiscal scope of the cash register system\footnote{14 CF: Technical Requirement 20};
- the management of the nomenclature of the versions (and notably management of the numbers of major and minor versions)\footnote{15 CF: Technical Requirement 21}.

These processes must take into account:
- the compliance requirements of this standard;
- the review of the functional specifications and test reports by the person in charge of compliance.

Management of these processes must notably be based on achieving and recording the previously defined objectives and compliance checks and implementing, monitoring and recording any action deemed necessary to remedy problems identified during the checks.

In the event of any changes in the design and/or development processes, the entity must ensure, and record the proof, that the change has no negative impact on the compliance of the cash register system with this standard.

\textbf{III.8) Management of subcontractors}

Certain activities (design, development, manufacture, tests, configuration, installation) related to the cash register system may be subcontracted, provided that they are managed, as well as any risks concerning the compliance of the cash register system.

For this, the subcontracting conditions must be formalised and recorded (definition of the subcontractor, requirements, objectives and compliance checks, communication of results, procedure to follow in cases of non-compliance).

The subcontractor must undertake to comply with the requirements of this standard.

The entity must monitor the subcontracting conditions as well as the results of the outsourced activity (and record them) by implementing checks in order to ensure continuous...
compliance of the cash register system. They must disclose these checking and assessment procedures to the subcontractor concerned.

It is, for example, possible to monitor these conditions via a subcontractor quality management system audit performed by the LNE or to consider an ISO 9001 certification, through a body accredited for the above-mentioned activities related to the cash register systems and the sites in question.

The entity must identify its critical suppliers/subcontractors, assess the compliance risks of the cash register system associated with subcontracting, and implement all actions deemed necessary to reduce these risks. This information must be recorded.

III.9) Identification and traceability of distribution

Each cash register system distributed must be uniquely identified (along with the version distributed). This identification must permit:

- traceability of the systems distributed on the market;
- updates or, where applicable, a new installation (major vulnerability detected, changes to the compliance requirements to be applied, etc.).

The entity must record and continuously update a registry of the systems and versions distributed to its customers.

III. 10) Communication with customers

The entity must transmit to their cash register system customers the following:

- all documents necessary to the proper operation of the cash register system (instructions, equipment prerequisites, etc.), whether provided by the editor/manufacturer or a distributor;
- support and training procedures, where applicable;
- customer liability commitments vis-à-vis the Finance Law for 2016 (obligation to keep accounts, data conservation, etc.)
- a description of the way in which tax authorities can access the cash register’s data, as well as a user manual dedicated to the tax authorities, describing the ways of accessing the cash register’s data, and the procedure for checking all data¹⁶;
- the corresponding certificate approved by the LNE.

In addition, the entity must make sure the above-mentioned documents are available to internal teams and users for three years after the final distribution date of the certified cash register system.

The communication concerning certification of the cash register system must not:

- be ambiguous for the customer as to the name and version of the cash register system receiving certification;
- cause confusion over the fact that the certification concerns a cash register system and not a company, management system or service.

¹⁶ CF: Technical Requirement 19
The list of certified cash register systems is available on the LNE website by using the dedicated search engine (https://www.lne.fr/recherche-certificats): select “LNE Products.” Upon request, LNE provides information on the validity of a given certificate.

III.11) Usage of the LNE mark – Cash register system

Companies with one or more LNE-certified cash register systems may use the logo “LNE cash register system” on their communication media.

When the applicant/holder plans to use the LNE mark (LNE logo – cash register system, they must comply with the conditions for use of the mark, i.e.:

- not use the certification obtained in a way that could harm the LNE, nor make any declaration or issue any statement over the certification of its products that could be considered as misleading or unauthorised;
- any reference to the certification prior to notification of its issue is prohibited;
- if the certification is withdrawn or its validity expires, reference to this withdrawn or expired certification is prohibited: any means of communication that makes reference to it must cease to be used;
- only make declarations regarding the certification that are consistent with the certificate issued by LNE;
- reproduce the certificates in their entirety, with the annexes, where applicable, if providing them to a third party;
- any reference to the LNE cash register systems certification in advertising, the presentation of any service, as well as commercial documents of any kind that refer to it must feature the following information, as a minimum:
  - the certificate number;
  - the LNE website address.

Any use or abusive reference to the LNE cash register systems mark/certification, whether by the bearer of a certificate or a third party, shall be subject to legal action in application of the regulations in force concerning misleading advertising and intellectual property.

III.12) Assessment and improvement of CMS performance

The entity must implement monitoring of the CMS, collecting and analysing information in order to evaluate and improve the effectiveness of the CMS.

This monitoring includes assessment of the effectiveness:

- of the checks defined in III.6, for example through analysis of test results from sampling;
- of the handling of previously identified non-compliance issues;
of the actions implemented to reduce the risks associated with the compliance of the
distributed cash register systems;

of external service providers.

The entity must take advantage of the CMS monitoring system in order to determine,
implement and record any action deemed relevant to improve the CMS and reduce the risks
of non-compliance.

III.13) Handling of non-compliance issues

There must be no deviation from the requirements of this standard.

The entity must ensure that non-compliant cash register systems are identified and
controlled in order to prevent their distribution and use.

The entity must react (even after possible distribution) to a non-compliance issue in
the following way:

- analyse the non-conformity: identify its causes in order to determine whether it is
  necessary to do anything to eliminate them so that the non-conformity does not
  occur again;
- implement actions that:
  - correct the non-conformity;
  - or prevent use of the cash register system(s) in question, warn their
    customers and conduct a recall of the products or update them;
- evaluate the effectiveness of the actions taken;
- update the identified risks in III.1 if necessary;
- update the CMS as described in III.5 if necessary.

The entity must record information on the nature of the non-conformity, its analysis,
the actions taken and their results.

III.14) Records management

The entity must manage the records cited in this standard, as well as all records
deemed relevant so that they are available, accessible and suitable for use whenever and
wherever necessary. The entity must ensure the correct storage, protection, duration of
conservation and deletion of these records.

The records in question shall be at least the following:

- risks (legal, reputational, financial, etc.) related to the compliance of cash register
  systems (III.2);
- compliance objectives for each level and function for the activities in question (III.4);
- relevant action to achieve the expected results or prevent risks, as well as assessment
  of its effectiveness (III.4);
- relevant action following a change of context and/or of the CMS, as well as
  assessment of its effectiveness (III.5);
- compliance checks implemented and their results (III.6 & III.7);
- analysis of the cause of a non-compliance issue and the actions taken following it
  (III.6 & III.7);
- design process (III.7);
- functional specifications relating to compliance (III.3 & III.7);
- test plans (III.7);
- development process and method (III.7);
- test reports (III.7);
- source code management (III.7);
- definition of the fiscal scope (III.7);
- management of version nomenclature (III.7);
- evidence that a design and development process change has no impact on compliance (III.7);
- subcontracting conditions (III.8);
- results of outsourced processes (III.8);
- identification of critical suppliers/subcontractors (III.8);
- risk analysis on the compliance of subcontractors (III.8);
- relevant action to reduce the risk associated with subcontracting (III.8);
- registry of the systems and versions distributed (III.9);
- information on the NCs, their analysis and actions taken (III.13).

When the entity records and updates the information recorded, it must ensure that the following elements are defined and correct:
- identification and description: document title, date, version number;
- record format (paper, electronic);
  - in the case of electronic records: file name and extension (word, pdf, jpg, etc.);
- and also that the information’s suitability and relevance is reviewed/approved by the appropriate people prior to its dissemination.

The entity must ensure that documents of external origin are identified and prevent any use of out-of-date documents.
Chapter IV: Technical requirements applicable to the certified cash register system

This Chapter presents the technical requirements that certified cash register systems must meet. The certification applicant is free to demonstrate how they meet these requirements. Examples of acceptable solutions are presented for certain requirements.

Checking methods are based on assessment of the documentation associated with the cash register system, functional and robustness checks on the cash register system to be certified.

Where applicable, the following is set out for each requirement: the title of the requirement, indications or examples of (an) acceptable solution(s) and the documentary, functional and robustness checking procedures.

IV.1) Documentation

The cash register system’s documentation must describe all of the functions and mechanisms implemented under the certification that mean it meets all the technical requirements set out in this chapter. Organisation of this documentation must be described in a framework document 17.

All of this documentation must be:

- conserved in paper or electronic form;
- conserved until the end of the third year following the year in which distribution of the system ceased 18;
- identified clearly and uniquely:
  - with the relevant title, in English or French;
  - with the document version number and/or document approval date.

Note: For each technical requirement, refer to the documentation set out in the “documentary check” box.

The certification applicant is free to respond to each of these requirements in the regulatory documentation or the additional documentation, while respecting the constraints of these (language of publication in particular).

18 CF: III. 10) Communication with customers
**Requirement 1: regulatory documentation**

The cash register system must be accompanied by documentation describing its design, operation, maintenance and use. The documents listed below are covered by the tax authorities access rights and must be written in French, separately and entitled as follows:

- General design file;
- Functional specifications file;
- Technical architecture file;
- Organisational file;
- Maintenance file;
- Operational file;
- User file.

**Indications concerning the expected elements:**

These indications are not exhaustive; they are intended only to provide a better understanding of the expectations of each document.

**General design file:** describes the system and its main operating principles in their entirety and the equipment associated with the system to enable payments. Mapping of the different modules and their interactions. What are the operating systems and languages used, the network characteristics, brief description of any databases and the way in which they are interfaced? (Conceptual and logical data models: CDM/LDM). Must also enable the system to be identified unambiguously: fiscal scope, minor/major versions.

**Functional specifications file:** description of the usages identified, points of attention and specific demands inherent to the system, defined during the design phase in order to validate whether the solution will properly meet the explicitly identified requirements. In particular, the specifications related to the LNE standard requirements must be included.

**Technical architecture file:** describes the technical implementation of the solution in depth: technologies, algorithms (particularly the signatures and hashes used to secure data), frameworks, protocols used; detailed architecture of the system (diagram with flows and the system’s different components); backup procedures, etc. This file must cover all processing performed on data to be secured, particularly its transmission, back-up, export, printing and display.

**Organisational file:** describes what processes and organisation have been implemented for the design, development and configuration/deployment of the system: RACI, organisational charts, etc.

**Maintenance file:** intended to identify the monitoring of the product’s developments/corrections, processes and organisation put in place to manage vulnerabilities, licence management, methods of updating a version (corrective or progressive) and its delivery to the customer, code versioning policy mentioning the management of major/minor versions according to regulations. Description of the source code architecture (organisation of various code files, branches on the code administrator) and identification of the relevant portions in terms of certification for the fiscal scope.

Code version management policy (where applicable, the tool used: git, SVN, etc.) identifying the portions of code that impact the fiscal scope, relating to security, conservation, inalterability or archiving functions in the sense of BOI TVA 30-10-30 [French Tax Bulletin on VAT]. This code, known as a “major version” or major/fiscal scope may not be amended without informing the LNE and, in this case, it will be subject to an additional assessment in order to check the impact on compliance.

**Operational file:** Description of the system’s possible configurations and calibrations, its installation, the equipment prerequisites, the data backup procedures, the management of user rights, the use and monitoring of the system by system administrators as well as the replacement of the system.

**User file:**
- User manual for the end user describing the system’s functions and its operating instructions.
- User manual dedicated to the tax authorities describing precisely and simply how transaction data can be accessed by the tax authorities (with descriptions of any table fields, XML files, CSV files, etc.) This may be included in the user manual or be in a separate manual.

**Documentary check:**
Check whether the regulatory documentation exists, is correctly identified (titles, version number and/or approval date) and is written in French.

**Functional check:**
Check whether a sample of documents relating to a system that is being distributed is available.

**Robustness check:**
Check whether the technical documentation on security methods is consistent with what has been implemented.

---

### Requirement 2: additional documentation

Additional documentation comprises all documentation meeting the technical requirements of this standard that is not part of the regulatory documentation. It must be written in French or English.

The entity must provide main document (or table) describing the organisation of the documentation and listing the relevant documents, paragraphs and page numbers for each technical requirement.

**Documentary check:**
Check whether the additional documentation exists, is correctly identified (titles, version number and approval date) and is indeed written in French or English

**Functional check:**
Check whether a sample of documents relating to a system that is being distributed is available.

**Robustness check:**
Check whether the technical documentation on security methods is consistent with what has been implemented.

### IV.2) Recording data

#### Requirement 3: Data to be recorded

The cash register system must record all payment data related to the execution of a transaction and its payment. The data must be recorded, at the latest, at the point of calculating the total amount for the transaction prior to payment. This data includes, as a minimum:

- the receipt number (or transaction number);
- the POS identifier;\(^{21}\)
- a unique identifier for the establishment using the cash register system;
- the date and time of the transaction (year, month, day, hour, minute);
- the total amount, including tax;
- any data that may be used to produce receipts (definitive or provisional);
- the payment method (and the details of the amounts paid per payment method if the payment was made via several payment methods);
- the payment date (if different to the transaction date);
- details of the items or services: name, quantity, unit price, total excluding tax for the line and associated rate of VAT. These details must include any other basic data\(^ {22} \) needed to calculate the total excluding tax for the line.
- any data that may be used to ensure the traceability of the transaction and to guarantee the integrity of the payment data.

---

\(^{20}\) BOI-TVA-DECLA-30-10-30-20180704: point 50-75-130.

\(^{21}\) POS: Point of Sale identified by a unique number (terminal number, till number, balance number, etc.). A terminal records the cash data locally and temporarily (pending transfer of the data to a centralised system) or in keeping with Requirement 16 concerning the storage of data for six years from the date of the final transaction recorded in the current tax year.

\(^{22}\) Basic data: data that is not obtained by calculation from other data.
**Requirement 3: Data to be recorded**

**Specific note:**
Any future reference to “payment data” corresponds to the data listed under this requirement rather than the data generated through corrections (Requirement 4), the data required under Requirement 5 concerning the training/test mode or the cumulative and summary data required under Requirement 7.

**Examples of acceptable solutions:**
The unique identifier of the establishment of use may be the SIRET number of the establishment or the address of the establishment (full address).

**Documentary check:**
Description of the method used to record all the data exhaustively.

**Functional check:**
Perform a sample collection of operations. Check that all the transactions completed beforehand appear in the data recorded.
The following test routines are to be carried out if possible: application of discounts, application of promotions, application of loyalty rewards or equivalent, reprinting of receipt, etc.

---

**Requirement 4: corrections**

If corrections (changes or cancellations) are made to transactions in any way, these corrections are effected by recording new corrective payment data through “more” or “less” operations, rather than through direct changes to the payment data recorded.

**Documentary check:**
Check, using the full description of the transaction correction methods, how the changed data is related to the original data and that changes can be tracked.

**Functional check:**
Test the operation of the system to check that the corrections are made through “more” or “less” operations and not through direct changes to the original data recorded.
Check, by examining the database or the file, that the data is actually recorded, in cases of corrections.
Test routines must include the following cases: change of quantity, deletion of an item, deletion of a receipt, addition of an item to an already finalised receipt prior to payment, application of discounts, application of promotions, application of loyalty rewards or equivalent, etc.

---

23 BOI-TVA-DECLA-30-10-30-20180704: points 90 and 100.
### Requirement 5: Training/test mode

1) Data generated or simulated through a “training”, “test”, “acceptance”, “pre-production” or other mode or environment that permits the recording of fictitious transactions must be recorded and secured as payment data but explicitly identified as being issues from this mode.

2) The identifier of the manager of the operator recording transactions, as well as the transactions recorded during use of this mode/environment are part of the payment data. In this regard, this data must meet all of the requirements pertaining to it (recording, securing, archiving).

3) Any supporting document issued during the use of this mode must be identified as such with the word “factice”, “test” or any other relevant French word in the background.

4) The use of the training mode must be visibly marked on the cash register system’s display/graphical user interface.

5) If any mode of this type is present in the system, this must be indicated in the documentation.

### Examples of acceptable solutions:
In order to identify payment data generated through simulated transactions, it is, for example, possible to use a specific field in the database or a different database from the production data, as long as the same security mechanisms are in place and this data is properly integrated into the archives.

### Documentary check:
Using the full description of the relevant mode, check that:
- the data generated is properly recorded and secured like all payment data;
- the identifier of the manager and any transactions made are properly recorded and secured;
- the fictitious payment data is clearly identified;
- the supporting documents are clearly identified;
- the display of the system identifies the mode appropriately.

Check that if any mode or environment means that data relating to a fictitious transaction cannot be simulated or generated, this is explicit and reasoned, where applicable, in the documentation.

### Functional check:
Enter the “training” or “test” or similar mode.
Check in the database and the supporting documents issued that the operation is compliant with the requirement and consistent with the documentation.
Check that the data generated during the use of this training mode is properly identified and secured by attempting to modify it.
IV.3) Closures

<table>
<thead>
<tr>
<th>Requirement 6: annual, monthly and daily closures</th>
</tr>
</thead>
<tbody>
<tr>
<td>The cash register system must include daily, monthly and annual closing functions. The cash register system mustn’t be able to record new transactions, modify or cancel a transaction across a closed period. These closures can be done automatically by the cash register system or by the user. If the closures have to be done by the user, they must be informed of this.</td>
</tr>
</tbody>
</table>

**Specific note:**
When the closure is done by the user, it is the responsibility of the user of the cash register system to perform the periodic closures.

The annual closure can be based on the tax year if this does not coincide with the calendar year.

**Examples of acceptable solutions:**
It is possible to notify the user of the need to perform the closures by any suitable means (display on the system’s interface, notice of use, contract, etc.).

**Documentary check:**
Check, based on the description of the closing function:
- whether the three closure functions (daily, monthly and annually) are indeed available;
- that the function is compliant with the requirements;
- that, if the functionality is not automatic, the user is notified of the obligation incumbent on them to perform the closures.

**Functional check:**
Record the transactions and do the closures (at least 1 closure of each frequency) and check the closures are generated properly. Also check that it is impossible to record a new transaction or to modify/cancel a transaction for the closed period.
Requirement 7: Cumulative and summary data

For each closing, the cash register system must record the cumulative total for the period and the perpetual total like any other payment data.

Specific note:
The cumulative total for the period is the total turnover accounted since the opening of the period in question. It consists of the frozen value at the closure of the period (daily, monthly, annual) of a counter initialised to 0 at the start of the period (daily, monthly or yearly) and running during the period.
The perpetual total is the total turnover accounted since the cash register system was first launched. This is a counter that never resets to 0, the value of which is periodically saved at each period closure.
If the cash register system is changed, all the counters restart from zero. The counters of the previous system must therefore be archived (CF Requirement 10).
If the system is updated, all of the counters must continue to rise incrementally without being reset to 0.

Documentary check:
Using the description of cumulative and summary data, check that the method used to calculate these totals is based on the turnover and that this data is properly recorded for each accounting period.

Functional check:
Based on a representative test data sample, check that the cash register system correctly calculates and records the periodic cumulative totals and perpetual total for each of the accounting periods.

Robustness check:
Check that the integrity and authenticity of cumulative and summary data are based on a robust mechanism.

IV.4) Data security & inalterability

Requirement 8: Data inalterability

All payment data defined in the previous requirements must be conserved and secured in such a way that it cannot be altered.

Specific note:
The purpose of making data inalterable is to guarantee, and to be able to demonstrate by any reliable technical process, that none of the payment data has been lost since it was originally recorded. This technical process should be capable of detecting and providing evidence of any change or deletion of the payment data.

---

26 BOI-TVA-DECLA-30-10-30-20180704: points 80 & 100.
27 Defined in Requirement 3, the corrective payment data defined in Requirement 4, the training/test mode data defined in Requirement 5, the cumulative and summary data defined in Requirement 7, the receipt printing/reprinting traceability data (Requirement 9), as well as data purging, archiving and restoration operations (Requirement 15)
### Requirement 8: Data inalterability

**Examples of acceptable solutions:**

The inalterability of the data may be guaranteed through:

1) evidence of the authenticity and integrity of the data that may take the form of key fingerprint chaining or signature chaining for each record.

   Authentication and integrity can be guaranteed through a signature mechanism (such as RSA-SSA-PSS, ECDSA) or a fingerprint mechanism with key (HMAC). The key must be generated at random by a reliable process and the end user (the professional taxpayer) must not be able to find it out or easily guess it. The signature (or fingerprint with key) of a transaction must include authentication elements for the previous transaction as well as the last transaction recorded (via a counter or other unique element) in order to guarantee that no transaction has been deleted.

   The following examples of key fingerprint mechanisms are acceptable: HMAC-SHA-256, HMAC-SHA3.

   The following examples of hashing are not acceptable: SHA-1, MD5, CRC16, CRC32 and any other form of non-cryptographic checks, including the CRC32 of a SHA256 fingerprint.

   The following examples of data signature algorithms are acceptable: RSA-SSA-PSS, ECDSA.

   For the RSA algorithm, a key of 1024 bits minimum must be used. Use of a key of 2048 bits or more is recommended. Elliptic curves should be of at least 256 bits. The following examples of elliptic curves would be deemed acceptable: ed25519, Brainpool, P-256, ed448.

2) The signature or key fingerprint for all of the data logged. In this case the new signature or key fingerprint for each transaction should be calculated for all of the data, after having first been checked for older data values.

3) A perfect grasp of data write permissions may be deemed acceptable. The professional taxpayer may under no circumstances be able to gain access to data write permissions. It should be possible for the system to be based on signed and encrypted data (such as the “encryption at rest” mechanism in MongoDB) for which the cryptographic key can not be easily accessed by the user (the use of key dumping principles, as one example, or the use of an external USB dongle with a licence protection mechanism).

Regardless of the type of solution selected, in the event that a cash register system is deployed on a workstation whose user holds administrator’s rights, a protective mechanism against data being restored to a previous state will be required. This sort of operation must be detected or made impossible to perform. It must be possible to log - without the user having to access the payment system - proof of authenticity (signature, key fingerprint) for the last log made (for cases of data chaining) or for the whole of the database, where allowed by the system.

These solutions are not exhaustive and may be used alongside any other solutions as duly accepted.

**Documentary check:**

Check that the mechanisms governing the inalterability of data have been accurately described, including the cryptography algorithms used. Check that the data covered by these mechanisms includes all of the payment data to be secured:

1) all payment data as defined in Requirement 3;
2) all corrective data as defined in Requirement 4;
3) all training/test mode data as defined in Requirement 5;
4) the cumulative and summary data as defined in Requirement 7;
5) the printing/reprinting traceability data as defined in Requirement 9;
6) Traceability data for data purge, archiving and recovery operations as defined in Requirement 15.

**Functional check:**

Check that a mechanism is in place for checking data integrity as well as its effectiveness for...
Requirement 8: Data inalterability

modifying data directly on the hard drive or in the payment database.

**Robustness check:**

- Perform a selection of payment operations.
- Connect to the device via all of the approved means of access and then try to change the data of transactions already logged.
- Check - in particular via a code audit - that all of the payment data logged is protected against alteration (change, insertion, deletion or replacement) based on the following cases:
  - Case 1: Check that the secret (key) is randomly generated and cannot be accessed by an attacker.
  - Case 2: Check that the secret code (key) is randomly generated and cannot be accessed by an attacker. Check that the previous signature for all of the data has been checked prior to overwriting each log.
  - Case 3: Check that the protection measures provide the same level of security as the previous examples and are properly implemented. In the event of an inspection conducted by a trusted third party, check that provisions and SLAs are in place for these protective measures based on the agreements, terms and conditions, description of rights management procedures and access control protocols, RACI documents for teams working on the data, traceability information for maintenance operations and any other documents deemed relevant.
- Conduct a robustness analysis on the mechanism, ensuring all records are secure (an example of tests to be carried out: validation of the electronic certification chain, proper use and implementation of cryptographic mechanism used and compliance vis-à-vis the state of the art, etc.).
- Check that data flow security is based on secured channels (e.g. HTTPS/TLS).
- Check that recovery of a database or file containing protected data is prevented or detected.
- Check that all payment data referred to in Requirements 3, 4, 5, 7 and 15 is covered by the security mechanisms.
- Draw a conclusion regarding the system’s capacity to ensure the integrity and authenticity of data.
Requirement 9: securing receipts

The cash register system must allow to unequivocally identify and distinguish receipts issued prior to payment between those issued after the payment has been made. Any receipt that is reprinted should bear the word “duplicata” [duplicate]. The system must provide secure traceability of receipts (both definitive and provisional) printed and reprinted. The information included in the receipts must be consistent with the payment data recorded securely by the cash register system.

Specific note:
Invoices, bills, short form receipts and tickets are deemed to be receipts.

Examples of acceptable solutions:
It is possible to include the words “valable pour encaissement” [valid for payment], “provisoire” [provisional], “pro-forma” and/or “non payé” [unpaid] on receipts prior to payment as well as the words “paiement réalisé” [payment made] or “paiement reçu” [payment received] on post-payment receipts.

In the event that a single bill is shared between multiple clients then it should be possible to issue an initial receipt identified as provisional, followed by the issuance of multiple receipts following payment, the sum of which should correspond to the amount shown on the provisional receipt.

It must be possible to ensure the traceability of printed/reprinted receipts by logging and securing the number of times each receipt is printed or tracking each print/reprint by logging the time, date and receipt number (or transaction number, where applicable) in a secure log/event journal with the same security level as set out in Requirement 8.

Documentary check
Check from the description of the receipt printing methods that all of the requirements are listed and documented.

Functional check
Check, for the various instances of use of the system, that the receipts issued are consistent with the transactions recorded. Similarly, ensure that the printout counters are updating on the database or the printings logged into a journal.

Check, where bills are being split, that the sum of the various receipts issued is equal to the amount of the initial transaction inclusive of all taxes.

IV.5) Archiving payment data

Requirement 10: Data archiving

The cash register system must provide an archiving function intended for users enabling the export of uneditable, time-stamped payment data\(^\text{28}\) in an open format.\(^\text{29}\)

In the event of a change of cash register system, the cumulative and summary data\(^\text{30}\) must be archived.

---

\(^{28}\) Defined in Requirement 3, the corrective payment data defined in Requirement 4, the training/test mode data defined in Requirement 5, the cumulative and summary data defined in Requirement 7, the receipt printing/reprinting traceability data defined in Requirement 9, the purge and archiving operations traceability data, the traceability data for POS terminal data transmissions to the centralised system, where applicable.

\(^{29}\) Open format: an interoperable data format, i.e. a format that is not dependent on the specific software that was used to create, modify or read it and whose technical specifications are in the public domain, with no restrictions in place concerning access or implementation. Article 4 of Law no. 2004-575 of 21 June 2004 on confidence in the digital economy

\(^{30}\) CF Requirement 7.
## Requirement 10: Data archiving

### Specific note
The archiving function mentioned here should not be confused with a simple long-term data backup solution. It refers to properly exporting secure, uneditable, time-stamped payment data from the system in an open format for the purposes of preventing data loss following a hardware failure, discovery of a security vulnerability, changes in the cash register system or any other reason. It is a means for the taxpayer to be able to conserve their payment data independently of the cash register system used and send it to the tax authority in the event of an audit.

The cash register system editor is not responsible for performing the archiving. Rather, the system must enable the user to archive data. Therefore system users shall be responsible for executing the archiving task.

### An example of an acceptable solution:
The following open formats are acceptable for archiving data: .ods, .xls, .odb, .csv, .json, .xml and .txt. If archived data is compressed then the following open compression formats are acceptable: .zip, .7z, .gz, .bz2, .tar, .rar.

On the other hand, the following are closed or proprietary formats that are not acceptable: .xls or .mdb.

### Documentary check
Based on the description of the data archiving function, check that users of the cash register system are able to use it and are notified of it, that the format is open and that the data presented in the archive is uneditable, time-stamped and complete.

Check, if necessary, that there is a commitment in place from the editor of the cash register system to provide users, as well as the tax authority, archived data, particularly in the event that the user stops using the cash register system.

### Functional check
Check that the archiving function is available, capable of properly producing open format archives and that the data presented has been properly time stamped and is complete.

Check that it is possible to archive the cumulative totals for a given period as well as uneditable perpetual totals for each period.

### Robustness check
Check that the integrity and authenticity of the data on the date the archive was created are protected by a robust mechanism, as described in Requirement 8 above.
### Requirement 11: Archiving frequency

The archiving function must enable users - at any point in time - to access or generate archives for any past period of time. The period of time covered by one archive should not be greater than one calendar year or one tax year.

**Examples of acceptable solutions**

It is acceptable to give the user the ability to define start and end dates for the period they wish to archive data for (whilst not exceeding the maximum limit of one calendar/tax year) or to generate multiple periodic archive files (i.e. daily, monthly and/or annually).

**Documentary check**

Check that, based on the description of the archiving function, users are able to archive data for any desired period of time up to the limit of one calendar or tax year per archive.

**Functional check**

Check that users can at any time archive all of the payment data for any desired period of time (as one or more files), up to the limit of one calendar/tax year per archive.

For example, make one or more archives for a period of several days, one month, several months and/or one year. Check that it is impossible to produce an archive file exceeding a period of one calendar or one tax year.

### Requirement 12: Archive integrity

The data contained in the archive must be identical to the original uneditable data from which it was created and the archive must include a reliable mechanism that is independent of the archive conservation medium, guarantees this integrity and permits checking.

**Specific note**

These mechanisms must make it possible to detect and reveal any change in or deletion of payment data conserved in the archive. They must also make it possible to detect and reveal any differences relative to the original payment data or the payment data contained in the archive. The security level for these mechanisms must be at least equivalent to that used to meet Requirement 8.

**Examples of acceptable solutions**

For example, an encrypted external hard disk-type secure external medium would be acceptable. An alternative to this might be the production of a secure archive (protected either by signature or key fingerprint) that is stored on an external device (external hard drive, USB key drive, etc.).

In the event that a secure external medium is not used then the archive itself must be secure. Conserving archives in the cloud is possible, as long as best practice rules are observed.

**Documentary check**

Check that the mechanisms ensuring archive integrity have been accurately described, including the cryptography algorithms used.

**Functional check**

Check that an archive integrity check mechanism is in place and ensure its efficacy by attempting to modify the archive directly.

**Robustness check**

Check that the inalterability of archives over time is based on a robust mechanism capable of guaranteeing a level of protection that is at least equivalent to the level specified under Requirement 8.

Check that a reliable archive integrity checking mechanism is in place that is independent of the storage medium.
### IV.6) Purges

#### Requirement 13: Purge

If the cash register system has a payment data purge function associated with the need to free up memory, this must compulsorily generate an archive containing all of the payment data to be purged and conserve it pursuant to Requirement 17 below, prior to performance of the purge.

**Documentary check**

Based on the description of the purge method, check that this method systematically involves the prior generation of an archive containing all of the payment data to be purged. If there is no purge procedure, check that this fact is properly described in the documentation.

**Functional check**

Create an initial dummy archive containing samples of both original and modified data (+ & - operations), copy this archive to another medium and then run the purge procedure. Check that the archive generated by the purge is complete when compared with the original archive.

**Robustness check**

Check that the archive thus generated is secured to the same level specified under Requirement 12. Create an archive for a given period. Run a data purge for this same period. Check that the archive is consistent.

#### Requirement 14: Partial purge

The purge function must not delete cumulative and summary data or operation traceability data from the cash register system. This data must remain conserved for an indefinite period of time, and must be secure in the cash register system.

**Documentary check**

Based on the description of the purge method, check that the cumulative, summary and traceability data is properly conserved at all times and secure, in the cash register system itself.

**Functional check**

Using a representative payment system, firstly enter known data, perform a purge then check the accuracy and proper conservation of the cumulative and summary data for the period of time the data was known to have been purged from the cash register system. Then compare this result against the original data.

**Robustness check**

Check that the purge mechanism does not negatively affect the integrity of the cumulative and summary data stored in the cash register system for the period of time the data has been purged for.

---

31 BOI-TVA-DECLA-30-10-30-20180704: point 250.
33 CF Requirement 7.
34 CF Requirement 15.
35 CF Requirement 17.
36 CF Requirement 8.
### IV.7) Operation traceability

<table>
<thead>
<tr>
<th>Requirement 15: Operation traceability</th>
</tr>
</thead>
<tbody>
<tr>
<td>The cash register system must provide secure traceability of archiving, purging and data recovery operations by logging the time, date and identifier of the POS used for the operation, on the system, for each of these operations.</td>
</tr>
</tbody>
</table>

**Examples of acceptable solutions**

It should be possible to ensure the traceability of these operations through the use of a secure event log with the same level of security as defined for Requirement 8.

**Documentary check**

Based on the description of the means used to ensure the traceability of these operations, check that the mechanism covers all closures, purges and archive generations.

**Functional check**

After having performed a collection of archiving operations, check on the system:
- that it is possible to identify all of the archiving operations performed;
- that time stamping is set up for the archives;
- that there is a link between the archive and the device that produced the archive;
- that any change in the traceability data is detected by the system.

**Robustness check**

Check that the traceability data security mechanisms implemented have security levels that are at least equivalent to that achieved under Requirement 8. Check that the time stamping of operations is based on a reliable mechanism that cannot be modified.

### IV.8) Data conservation

<table>
<thead>
<tr>
<th>Requirement 16: Data conservation</th>
</tr>
</thead>
<tbody>
<tr>
<td>All payment and traceability data as well as evidence of its inalterability must be stored for six years (from the date of the final transaction of the tax year). Cumulative and summary data as well as traceability data must be stored in the system. Payment data (excluding cumulative, summary data and traceability data) may be conserved in either the system itself or in the archives.</td>
</tr>
</tbody>
</table>

**Specific note**

The payment data in question is that defined in Requirement 3, the corrective payment data defined in Requirement 4, the training/test mode data defined in Requirement 5, the cumulative and summary data defined in Requirement 7 and the operation traceability data defined in Requirement 15. Taxpayers only conserving the Z from tills (total cumulative amount for the day) will not be deemed to have fulfilled conservation obligations.

Checks concerning the duration of data conservation shall be based on a term of seven years in order to simplify the possible interpretations of the Tax Procedure Code and shall take into account exceptional instances of offsetting for the tax year.

The system should be capable of anticipating hardware issues for storage media or more explicitly be capable of notifying users (taxpayers) of their responsibilities and their obligation to store data under this requirement.

**Examples of acceptable solutions:**

It is for example possible to implement memory capacity monitoring procedures and/or tools, to

---

37 CF article L.102 B of the Tax Procedure Code.
38 CF Requirement 15.
39 CF Requirement 14.
## Requirement 16: Data conservation

estimate the required memory capacity, to notify the user that a purge needs to be run, to increase the memory capacity if necessary, or to mirror backups on physical media, ideally remote media.

**Documentary check**

Based on the description of the payment data conservation method, check that all payment data has been properly conserved for a term of seven years.

Check that payment data (excluding cumulative and summary data and traceability data) is properly conserved in either the system itself or in the archives.

Check that the manufacturer has implemented measures to prevent the risk of memory saturation and that the system is capable of conserving data for at least seven years.

**Functional check**

Check that the measures implemented by the manufacturer to reduce the risk of memory saturation are functioning properly.

Check that payment data (excluding cumulative and summary data and traceability data) is properly conserved in either the system itself or in the archives.

Check that cumulative, summary and traceability data is properly stored in the system itself.

**Robustness check**

In the case that data conservation is provided by the system and not by the archives, check that the payment system is properly capable of conserving payment data for a period of seven years.

Check that this capacity is based, for example, on the use of a mechanism capable of ensuring a suitable level of availability of the storage system (RAID 1 hardware or software) or the file system (mirroring files on multiple storage units, logging, self-repair capacity, etc.). Check that the settings for the mechanisms implemented are capable of guaranteeing the proper conservation and availability of payment data for seven years.

## Requirement 17: Archive conservation

Archives must be conserved in such a way as to guarantee the integrity and availability of the archived data for inspection, for six years (starting from the date of the final transaction for the tax year).

**Examples of acceptable solutions:**

Archives may be conserved within or outside the cash register system itself, or by a third party archiving service that is responsible for conserving the archives. All necessary measures must be taken to guarantee the integrity and availability of the archives in accordance with Requirements 12 and 16.

**Documentary check**

Based on the archive conservation method used, check that the archives are stored so as to guarantee their integrity and availability with the same level of confidence as for Requirements 12 and 16.

**Functional check**

Check how the archives are conserved in such a way that their integrity and availability is guaranteed with the same level of confidence as for Requirements 12 and 16.

**Robustness check**

Check that the cash register system is capable of conserving complete, readily available archives with the same level of confidence as for Requirements 12 and 16.
**Requirement 18: Centralised system**

When data conservation\(^{40}\) is ensured via a centralised system, the cash register system must include reliable mechanisms demonstrating the completeness and traceability of payment data transmissions. The system must be capable of managing a dropped connection between the centralised system and the terminals and ensuring that the POS terminals cannot carry on functioning indefinitely without a connection to the centralised system.

**Specific note**

Systems are deemed to be centralised if one or more POS terminals storing information locally prior to transmission (such as autonomous payment points periodically transmitting data, or which send data in real time while employing a buffering system in case of disconnection) send payment data to a central system that conserves it in compliance with Requirement 16. In contrast, a system with client-server architecture in which the client interface is solely a graphic interface with no temporary data storage capacity and which enables communications over a server (such as an open website in a browser, for example) is not deemed to be a centralised system as long as autonomous use of the interface with no connection to the server is not possible.

If the terminals provide data conservation in compliance with Requirements 8 and 16, then this requirement does not apply. The purpose of payment data transmission traceability is to ensure that all transaction data is properly transmitted, including in the event of connection issues or transmission errors.

**Examples of acceptable solutions:**

For the purposes of ensuring the completeness of the data transfer it is possible to implement a time-stamped incremental number system for sending and receiving data or a reference to the last log sent (such as a log hash, for example) along with identification of the source POS terminal for the purposes of ensuring that no data is missing.

For the purposes of ensuring the integrity of the transferred data it is possible to use a signature, key fingerprint or secure network protocol (such as TLS or IPsec).

If the system is capable of allowing POS terminals to carry out transactions autonomously in the event of loss of the connection with the centralised system, then the locally stored data must have a security level at least equivalent to the security network provided in response to Requirement 8. Furthermore, once the connection is re-established, the centralised system must ensure that it has recovered all of the data stored locally and temporarily by the POS terminals.

**Documentary check**

If data conservation is insured by the terminals, check the elements proving that this requirement does not apply.

If data conservation is provided by the centralised system, check - based on the full description of this system - that the completeness of the data transmission can be demonstrated and that these transmissions are tracked. Check that the editor has provided an explicit declaration concerning the completeness of transmitted payment data.

**Functional check**

If data conservation is insured by the terminals, check the elements proving that this requirement does not apply.

Check that there is effective traceability between the POS terminal payment data transmission system and the centralised system.

Check that a sample collection of payment data is transmitted correctly to the centralised system.

\(^{40}\) BOI-TVA-DECLA-30-10-30-20180704: point 210.

\(^{41}\) CF Requirement 13.
### Requirement 18: Centralised system

**Robustness check**

In the event that counters are used to track the number of transactions issued and received, perform a collection of operations from the POS terminals connected to the centralised system and ensure (via the centralised system) that each record made on a POS terminal is associated with:

- the identifier of the POS terminal in question,
- an incremental numbering system tracking the moment the data is sent by the POS terminal,
- an incremental numbering system tracking all of the transaction data received from each POS terminal by the centralised system in order to ensure that no transmission has been omitted.

In the event that encryption or signatures are used for data being sent, check that the security level is at least equivalent to that provided in response to Requirement 8.

Check that all of the payment data is properly stored and conserved in the centralised system. Check that any fault arising during data transmissions or when data is received does not produce missing data or errors within the centralised system.

Check that the mechanism protecting against alteration of the transmission has a security level at least equivalent to that for Requirement 8.

Check that, in the event that the connection to the centralised system is lost, it is not possible to indefinitely perform transactions using the POS terminals and that this mechanism is robust enough to check that all elements are properly transmitted when the connection is re-established.
IV.9) Tax authority access to payment data

**Requirement 19: Tax authority access to payment data**

The cash register system must provide a mechanism allowing the tax authority access to all of the payment data recorded. The editor must provide the tax authority with an automated means of checking the integrity of the payment data. The manufacturer must provide the relevant tax authority with a user manual in French that gives details of the procedure for accessing the data as well as a clear description of the operation of the tools used to access this data and check its integrity. This access shall not compromise the security of the payment data.

**Specific note:**
The user manual to be sent to the tax authority must be clear and readily understood by non-computer specialists. The manual should additionally detail the procedure enabling the tax authority to check that the data has not been altered.

**Examples of acceptable solutions:**
It may be possible to operate the managing account, or a dedicated account intended for the tax authority to access all of the company’s data, which may be in a native form (flat files, XML files, etc.) or an interpreted form for display purposes.
It is possible to detail the support contact and escalation processes, if necessary, in the manual intended for the tax authority. This may be included in the user manual or be a separate manual. The data presentation structure (the various fields) must be clearly described. The user interface, menus, windows and other functions intended for the tax authority may be described in the specific manual for the authority.

**Documentary check**
Check from the description of the tax authority’s access point that all payment data is accessible. Check the existence and relevance of the manual intended for the tax authority, describing the means and procedures used to access payment data.

**Functional check**
Check that the means used by the tax authority to access the data works correctly and that all payment data is accessible. Check that this means does not allow payment data to be changed or deleted. Check that the means provided to the tax authority enables data changes to be correctly identified (amendment, insertion, deletion). For example, change an item of data and check that detection of this error occurs smoothly and immediately using the tax authority’s means of accessing the system.

**Robustness check**
Check that the authority’s access means do not compromise the level of security of the cash register system.

---

42 BOI-TVA-DECLA-30-10-30-20180704: points 60 & 100.
43 Defined in Requirement 3, the corrective payment data defined in Requirement 4, the training/test mode data defined in Requirement 5, the cumulative and summary data defined in Requirement 7, the operation traceability data defined in Requirement 15 as well as the traceability data for complete data transmission in the case of a centralised system.
IV.10) Identifying the fiscal scope and minor and major versions

<table>
<thead>
<tr>
<th>Requirement 20: Identifying the fiscal scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>The editor must clearly define the fiscal scope of their cash register system and list all of the source code files, libraries, drivers and modules impacting the functions and requirements set forth in this standard.</td>
</tr>
</tbody>
</table>

**Specific notes:**
If one part of the fiscal scope is protected by a specific operating system configuration, the configuration files concerned must have additional identification.
The non-fiscal scope is the so-called “minor scope”. The source code of the minor scope must be available to the assessors when they assess robustness, so that the consistency of the tax and minor scopes can be verified.

**Examples of acceptable solutions**
The following, for example, must be included in the fiscal scope: all functions for payment data recording and correcting/cancelling transactions; functions linked to saving and securing data generated in training mode; closure functions (daily, monthly and annual); calculating, saving and securing cumulative and summary data; securing and ensuring the inalterability of payment data; securing receipts; archiving; securing archived data; purging; traceability of operations (archiving, purging); data and archive preservation; access to the tax authority and any other function/module/driver/library impacting upon compliance with the requirements in this standard. It is possible to define the fiscal scope as being the entirety of the cash register system source code.

**Documentary check**
Check that the list of components in the fiscal scope is complete so that the certifying organisation and the editor have no doubt as to the portions of the source code whose modification results in a change to the major version.

**Robustness check**
Check by analysing the source code that all regulatory functions (i.e. associated with the certification and requirements of this standard) are implemented in source code files included in the fiscal scope. Check by sampling the source code that there are no regulatory functions in the non-fiscal scope (minor)
### Requirement 21: Identifying major and minor versions

The cash register system must be clearly identified by a major version number and a minor version number inextricably linked to the cash register system. These version numbers must be easily accessible from the cash register system’s standard user interface.

Any change to the code in the fiscal scope or configuration affecting compliance with the requirements in this standard must result in an increase of the major version number.

The editor must generate and provide the fingerprint of each major version.

#### Specific note:
- The major version number of the cash register system is the version number identifier for the fiscal scope of the cash register system.
- The minor version number of the cash register system is the version number identifier of the code not included in the fiscal scope and therefore does not affect the requirements of this standard.
- If the cash register system functions can be deactivated by specific configurations, each function or variant must be identified separately.

#### Examples of acceptable solutions

The following algorithms are the state of the art in creating fingerprints of software or sub-sections of software for the purposes of precise identification: SHA-2, SHA-3, Whirlpool, Blake.

The following algorithms are not acceptable however: SHA-1, MD5, CRC16, CRC32 and any other form of non-cryptographic checks.

It is possible to create the fingerprints used to identify versions from binary or source code. The fingerprint must be stored next to the source code.

In the case of systems that can be accessed directly by final customers (e-commerce, for example), display of the cash register system version number can be limited to a specific profile (tax controller or administrator, for example).

#### Documentary check

Check from the documentation how the system identification by version numbers is created and how it is inextricably linked to the system itself. Check in the documentation what measures are taken to protect the cash register system’s identification against any falsification.

Check that the user manual describes how to display the identification of the major and minor versions of the system from the user interface.

Check that the nomenclature rules of major and minor versions are clearly established and meet requirements.

From the documentation that the editor has provided, check the major version and minor version numbers of the cash register system assessed during the certification audit.

#### Functional check

Check that the identification of the software is displayed in accordance with its description in the documentation. Check that the identification displayed is correct.

#### Robustness check

Check that the mechanism providing system identification via the major and minor version numbers has integrated all the portions of the source code of the system concerned and that it is reliable; in other words, that it meets the criteria in Annex B1 of the RGS, or is at least resistant to conflict attack (i.e. it is not possible to forge two separate sources producing the same fingerprint).

Check that the measures taken to avoid falsification are appropriate in terms of the state of the art.

Check by sampling from the change log or the difference in code between two versions, that the minor modifications have had no impact on compliance with the requirements in this standard.

Check that a fingerprint made by the assessor in the certified code produces the same fingerprint as that issued by the editor.
The certificate is linked to a major version of the cash register system (and assessed during the certification audit) and is valid to certify compliance with the conditions of inalterability, security, conservation and archiving of data for minor versions subsequent to the minor version assessed by the LNE during the certification assessment.
Chapter V: Drafting and validation of the standard

V.1) Mark committee
V.1.1) Operational procedures

A mark committee is formed whose duties are to:

- provide an opinion on the certification rules and changes to the process;
- provide an opinion on potential communication or promotion activities relating to the mark.

The mark committee meets at least once a year in an ordinary meeting. Extraordinary committees may be organised where necessary (in order to amend the certification rules).

Prior to the committee meeting, the LNE will send an agenda for the meeting to members of the committee along with, where applicable, any relevant documents. The LNE drafts the minutes of the comments and proposals made during the committee meeting. These minutes are sent to all members of the committee. Where applicable, a bureau of the committee or working groups may also be involved to improve efficiency.

The composition of the mark committee is approved by the CEO of the LNE or their representative, each member then being informed of this. The members’ mandate is 3 years and is renewable by tacit consent.

Performance of the duties of members of the mark committee is strictly personal. However, in the event of absence, a replacement is nominated and appointed under the same conditions as the incumbent.

V.1.2) Role, commitments and composition of the committee

The members of the committee agree to:

- contribute through their expertise to the living of the cash register system certification mark;
- keep exchanges and information communicated during committee meetings confidential until they are published by the LNE;
- participate regularly in meetings;
- contribute to development of the certification mark and promote certified services.

The committee is composed as following:

- three representatives of certified clients or clients in the process of being certified:
  - one representative of the software editors;
  - one representative of the cash register manufacturers;
  - one representative of cash register manufacturers associated with a regulated measuring instrument;
- two representatives of associations or organisations representing consumers and/or, failing this, the users themselves.

Every college has a vote. None of the interested parties can enforce a right of veto.

The LNE provides secretarial services for the committee.
V.1.3) Working Group

For certain ad-hoc technical work that does not require all members of the mark committee to be convened, a working group may be formed whose members are appointed and chosen from the mark committee. In the case of a working group, professionals or prominent figures from outside the committee may be called in.

The roles of this working group are specified by the mark committee; its role will generally be limited to the creation of drafts, proposals or the provision of additional information on a particular subject on behalf of the mark committee.

V.2) Procedures for drafting and validating the standard

This standard was drafted by LNE, based on working documents resulting from meetings between the group of experts and the committee, including manufacturers of cash register systems, editors of cash register software, customers and users.

It was drafted in accordance with the requirements set out in the Law of 4 August 2008 and the decree of 19 December 2008 governing the certification of products and services. To this end and in accordance with Article L433-3 et seq. and R433-1 and -2 of the Consumer Code, the certification standard is a technical document defining the properties that a product, service or a combination of products and services should possess and the procedures for checking the conformity of these properties.

In terms of validating this standard, the LNE is responsible for:
- identifying the interested parties concerned;
- ensuring the relevance of the interested parties selected;
- ensuring their representativeness, without one of them dominating;
- ascertaining their point of view.

Based on feedback, the standard is reviewed by the mark committee, specifically made-up of all interested parties. It is approved through the same methodology as the initial version.

V.3) Standards and reference documents

- Law no. 2015-1785 of 29 December 2015 on finances for 2016, Article 88, amended by Law no. 2017-1837 Article 105
- Law 2004-575 of 21 June 2004 on confidence in the digital economy
- Consumer Code – version of 1 January 2019 – Articles L433-3 to L433-11, Articles R433-1 and R433-2
- General Tax Code – version of 1 January 2019 – Articles 286, 1770 duodecies
• Tax procedure code – version of 1 January 2019 – Articles L 16-0 BA, L47 A, L80 O, L96 J, L102 B, L102 D

• Decree of 29 July 2013 amending the provisions of Article A. 47 A-1 of the tax procedure code relating to the standards for copies of files on computer media

• BOI-TVA-DECLA-30-10-30-20180704: Obligation to use certified software or cash register systems
• BOI-CF-COM-10-80-20160803: Right of communication with various persons
• BOI-BIC-DECLA-30-10-20-40-20131213: Conservation and representation of books, documents and accounting documents in computer-based accountancy
• BOI-CF-IOR-60-40-20131213: Inspecting computerised accounts

• General security standard version 2.0 –Annex B1 – Cryptographic mechanisms – version 2.03 of 21 February 2014
Chapter VI: Appeals and treatment of complaints

VI.1) Appeal against a decision

The certification holder may challenge the decision taken, by registered letter with acknowledgement of receipt.

The LNE then re-examines the file in light of the facts giving rise to the appeal. It notifies the applicant as to whether this decision is upheld or if there has been a new decision, within 15 working days of receipt of the appeal.

In the event that the applicant wishes to maintain their appeal against the decision, they notify the LNE by registered letter with acknowledgement of receipt, within 15 working days. Reasons must be given justifying this appeal, which is not suspensory of the LNE’s decision. It will be examined by the LNE within 21 working days of receipt and, where it relates to a certification decision, will be examined by the reading committee. The LNE informs the applicant whether or not its decision has been upheld.

In the event that the appeal is upheld following examination and submission to the mark committee for their opinion, the appeal is presented to the LNE’s Certification and Impartiality Committee, which presents its conclusions following examination of the case. The Company is informed of the final decision by the LNE.

Any subsequent dispute may be subject to arbitration by the relevant department of the Industry Ministry or be brought before the competent courts.

VI.2) Treatment of complaints

Any complaint relating to products is examined by the LNE in order to confirm whether the complaint does actually relate to certified products. The entity putting forward a complaint must support this by providing factual proof.

Once this has been received, the LNE examines it and, if applicable, contacts the company concerned.

The company concerned must then inform the LNE of the follow-up actions and make records relating to the complaint as well as the company actions taken to resolve it available to the LNE. Additional examinations to verify that the stated actions have been implemented may take place at the Company’s cost.

As part of the follow-up of the Company, the LNE examines the records relating to complaints and claims and checks that corrections and suitable corrective actions have been undertaken.
### Section VII: Annexes

### VII.1) Glossary

<p>| Archiving | The purpose of the archiving function, intended for users, is to export cash register data fixed in an open format, in order to protect against a loss of data following a hardware fault, security failure or change of cash register system, while guaranteeing the creation date of the archive. It should not be confused with a long-term backing-up solution for data. This is a way for the taxpayer to store data independently from the data collection system and be able to send it to the tax authority in the event of an audit. |
| Archive | File in the open format generated by the archiving function containing cash register data for a set period. The archive cannot contain cash register data for a period of over one year or one tax year. |
| Authenticity | Property of an item of data for which the system can verify the identity of the author. This can be carried out using key fingerprinting or signature mechanisms. |
| Chaining | Algorithm that proves the integrity of an item of data and proof of the integrity of the previous data, thus constituting proof of the integrity of all of the data. This mechanism does not guarantee the integrity of the last item and does not enable the number of missing elements to be counted (links) when the chain is broken. Proof of integrity can also be a proof of authenticity in order also to ensure the authenticity of the chain. |
| Ciphering | The action of writing or transcribing in figures. Not to be confused with encryption. |
| Encryption | Cryptographic mechanism enabling the confidentiality of data to be guaranteed, using a cipher (in the sense of a secret code). Data encryption is not required for this standard. Not to be confused with ciphering. |
| Public and private keys | A digital signature is generated by a private key which is a cryptographic secret and a document to be signed. Signature verification is performed based on the original document and the public key associated with the signature. Knowing a public key does not enable the corresponding private key to be found. |
| Closure | A manual or automatic function offered by the cash register system, the aim of which is to close a daily, monthly or annual period, i.e. to make it impossible to save new transactions or change or cancel a transaction in a closed period. |
| Confidentiality | Characteristic of information or a system meaning that it can only be accessed by authorised people. Confidentiality is not required for this standard. It can be provided by means of encryption. |
| <strong>Coding</strong> | Inserting or masking a hidden meaning in a text or phrase, voluntarily or not. Example: ‘to decode a political speech’. For the anglicism, see encryption. |
| <strong>Cash register data</strong> | The payment data is all the data defined in Requirement 3, the corrective payment data defined in Requirement 4, the training mode data defined in Requirement 5, the cumulative and summary data defined in Requirement 7 and the traceability data for printouts and reprints of the receipts defined in Requirement 9. |
| <strong>Basic data</strong> | Data that is not obtained from other data by calculation. Any basic data that contributes to the creation of an accounting record, evidence of an event or a written transcript in books, registers, documents, documents and declarations is covered by the tax authority's right of inspection. |
| <strong>Editor</strong> | Person who holds the cash register system source code and who manages changes to settings affecting the security conditions, conservation and archiving of payment data. |
| <strong>Fingerprint/hash/condensate</strong> | Result of a function that associates a fixed size datum with a random sized datum. When the fingerprint is cryptographic in nature, it is not feasible to calculate the inverse of this function. |
| <strong>Key fingerprint</strong> | Cryptographic fingerprint created by combining the source data with an authentication secret. This means that only the holder of the secret can generate and check a fingerprint. A key fingerprint guarantees the integrity of a document and guarantees its authenticity, without being able to make out the identities of the secret holders. |
| <strong>Cash register function</strong> | A function that consists in memorising and recording, off the balance sheet, payments received in return for the sale of goods or services. If the payment automatically, compulsorily, instantly and without human intervention triggers the creation of an accounting record at the same time, the function is not considered a cash function, but an accounting record function. |
| <strong>Time stamping</strong> | Ascending monotonic unique time value indicating the date and time an event occurs. This data is presented in a consistent format, making it easier to compare two different records and trace them over time. |
| <strong>Accountability</strong> | Option to attribute responsibility for an action to a person. |
| <strong>Inalterability</strong> | Property of a system whose recorded data cannot be changed without traceability (i.e. without the system detecting it). Alteration of data is an attack on its integrity and authenticity. |
| <strong>Integrity</strong> | Property of data that has not undergone any modification or destruction, voluntarily or accidentally. |
| <strong>Logging</strong> | Recording of a sequence of events impacting upon a particular process. It is a means of ensuring the traceability of events. |
| <strong>Receipt/Receipt document</strong> | Document with data showing the details of the order, sale, purchase and the method of payment for a product or service. |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free software</td>
<td>Software that may be freely used, studied, modified and distributed. These freedoms mean that users can adapt the software to their specific needs. [Source: BOI-TVA-DECLA-30-10-30]</td>
</tr>
<tr>
<td>Agent</td>
<td>A natural or legal person established in the European Economic Area (EEA) who represents the holder outside the EEA and has a written mandate from them signifying that they can act on their behalf in the certifying process, in accordance with provisions of these rules. The agent may also be the distributor or importer of the certified products, their various roles are therefore clearly identified.</td>
</tr>
<tr>
<td>Mode/Training Environment/Test</td>
<td>Optional mode or environment of a cash register system enabling data to be generated or simulated in order to record dummy transactions for testing or training purposes.</td>
</tr>
<tr>
<td>fiscal scope</td>
<td>The source code, libraries, drivers and modules impacting upon the functions and requirements set forth in this standard.</td>
</tr>
<tr>
<td>Proof of authenticity</td>
<td>Item of data that enables the authenticity of a document to be proven. See fingerprint key, signature.</td>
</tr>
<tr>
<td>Proof of integrity</td>
<td>Item of data that enables the integrity of a document to be proven. See fingerprint, signature.</td>
</tr>
<tr>
<td>Purge</td>
<td>Irreversible deletion of saved data from a system.</td>
</tr>
<tr>
<td>Redundancy</td>
<td>Method consisting in duplicating all or part of the data to enable it to be restored to its original state if modified. It can ensure that information is available, which is the capacity of a system to remain operational or to keep the data accessible over time.</td>
</tr>
<tr>
<td>Cryptographic secret</td>
<td>A cryptographic secret is a confidential item of data used to encrypt or authenticate a document. The confidentiality of this secret guarantees the properties (confidentiality or authenticity) of the mechanism that uses it. To be qualified cryptographically safe, this secret must be generated randomly, not used for different uses and have a size defined by the mechanism that uses it.</td>
</tr>
<tr>
<td>Signature</td>
<td>A digital signature is a mechanism that guarantees the integrity of a document and ensures its authenticity. In contrast to a fingerprint key, the verifier does not need to know a secret to verify the authenticity and cannot steal the signatory’s identity.</td>
</tr>
<tr>
<td>Cash register system</td>
<td>A cash register system is a computer system with a cash register function.</td>
</tr>
<tr>
<td>Holder</td>
<td>A legal person who manages and/or is responsible for meeting all of the requirements defined in these certification rules. These requirements cover at least the following stages: design, fabrication, assembly, quality control, marking, packaging as well as the marketing and specifying the critical points of the various stages. Some of these activities may be performed at the holder’s site or at another site by the holder directly or by another organisation to which they have delegated responsibilities. This includes subsidiaries or subcontractors, for example. Regardless of the site or the level of subcontracting, it is important that the holder should be able to present all evidence of compliance with the standard. Paragraph 310 of BOI-TVA-DECLA-30-10-30-20160803 states that the holder is the editor of the cash register system. When the holder is not established in the European Community, they must nominate an agent.</td>
</tr>
<tr>
<td>Aggregate total/Period total</td>
<td>The total turnover for the period accounted for since the opening of the period in question. This is a counter initialised to 0 when the period begins (or the previous period ends), whose value is stored at the end of the period.</td>
</tr>
<tr>
<td>Running total</td>
<td>Total turnover accounted since initialisation of the cash register system. This is a counter that is never reset, which is not directly linked to a period but whose value is recorded at an instant $t$: at each closure (daily, monthly or yearly).</td>
</tr>
<tr>
<td>POS</td>
<td>Point of Sale identified by a unique number (terminal number, till number, balance number, etc.). A terminal records the cash data locally and temporarily (pending transfer of the data to a centralised system) or in keeping with Requirement 16 concerning the storage of data for six years from the date of the final transaction recorded in the current tax year.</td>
</tr>
<tr>
<td>Traceability</td>
<td>Capacity to review the history, the implementation or the location of what is examined. It is linked to logging and accountability.</td>
</tr>
<tr>
<td>X</td>
<td>Term originating from old key-operated cash registers. Basic reading of the daily turnover; it can be carried out at any time and with no impact on recorded transaction data.</td>
</tr>
<tr>
<td>Z</td>
<td>Term originating from old key-operated cash registers. Daily closure of register: no changes to transaction data recorded since the last Z are possible, only cash balances are kept (cash still present in the cash register drawer, for example).</td>
</tr>
</tbody>
</table>
### VII.2) Requirements correspondence table V1.2/V1.4

<table>
<thead>
<tr>
<th>Cond no. v1.2</th>
<th>Req. no. v1.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.1</td>
</tr>
<tr>
<td>10</td>
<td>/</td>
</tr>
<tr>
<td>20</td>
<td>/</td>
</tr>
<tr>
<td>25</td>
<td>/</td>
</tr>
<tr>
<td>30</td>
<td>/</td>
</tr>
<tr>
<td>35</td>
<td>/</td>
</tr>
<tr>
<td>40</td>
<td>/</td>
</tr>
<tr>
<td>LPF</td>
<td>1</td>
</tr>
<tr>
<td>340</td>
<td>20-21</td>
</tr>
<tr>
<td>55</td>
<td>/</td>
</tr>
<tr>
<td>60</td>
<td>3</td>
</tr>
<tr>
<td>100</td>
<td>8</td>
</tr>
<tr>
<td>70</td>
<td>4</td>
</tr>
<tr>
<td>50</td>
<td>/</td>
</tr>
<tr>
<td>75</td>
<td>5</td>
</tr>
<tr>
<td>130</td>
<td>/</td>
</tr>
<tr>
<td>80</td>
<td>6</td>
</tr>
<tr>
<td>90</td>
<td>7</td>
</tr>
<tr>
<td>130</td>
<td>/</td>
</tr>
<tr>
<td>140</td>
<td>12</td>
</tr>
<tr>
<td>/</td>
<td>9</td>
</tr>
<tr>
<td>150</td>
<td>13</td>
</tr>
<tr>
<td>160</td>
<td>14</td>
</tr>
<tr>
<td>170</td>
<td>15</td>
</tr>
<tr>
<td>180</td>
<td>17</td>
</tr>
<tr>
<td>190</td>
<td>/</td>
</tr>
<tr>
<td>200</td>
<td>19</td>
</tr>
<tr>
<td>210</td>
<td>18</td>
</tr>
<tr>
<td>220</td>
<td>10-11</td>
</tr>
<tr>
<td>230</td>
<td>10-12</td>
</tr>
<tr>
<td>240</td>
<td>12</td>
</tr>
<tr>
<td>250</td>
<td>17-13</td>
</tr>
<tr>
<td>250</td>
<td>14</td>
</tr>
<tr>
<td>260</td>
<td>13</td>
</tr>
<tr>
<td>250</td>
<td>12</td>
</tr>
<tr>
<td>260</td>
<td>14</td>
</tr>
</tbody>
</table>