Disclaimer: This translation is not, and do not purport to be, official, and is intended for informational use only. It has no status other than as an informal, unofficial, aid to non-Portuguese speakers in understanding the Portuguese invoicing programs certification law. Only the Portuguese original can be relied on for interpretative purposes, and in any dealings with the Portuguese tax system or its officials.

Order No. 8632/2014 of the 3 of July

Director General of the Tax and Customs Authority

According to paragraph e) of article 3 of Ordinance No. 363/2010, of the 23 of June, the computer invoicing programs and similar programs, even if already certified, hereinafter simply called invoicing programs, shall further obey to the following technical requirements.

1. CREATION OF DOCUMENTS ISSUED BY COMPUTER INVOICING PROGRAMS

1.1. The computer invoicing programs shall use a digital signature on all the documents with external effectiveness, except receipts, pursuant to article 6 and 7 of Ordinance No. 363/2010, of the 23 of June, in particular:

- Invoices and invoice correction documents (debit and credit notes);
- Transport guides, delivery notes or any other documents which function as transportation documents, pursuant to Decree No. 147/2003, of the 11 of July;
- Any other documents, irrespective of their name, to be presented to the client as proofs of delivery of the goods or services, in particular table checks.

1.2. Any other documents which are neither invoices nor invoice correction documents, must clearly indicate their type and, in case of documents susceptible to presentation to the client, including the documents contained in tables 4.2, 4.3 and 4.4 of SAF-T (PT), they must mention “Este documento não serve de fatura” (This document is not an invoice).

1.3. The invoices, documents regarding the movement of goods, verification documents of the delivery of goods or services rendered susceptible to be presented to the client, originated by other issued documents, namely invoices, documents regarding the movement of goods, table checks or other documents susceptible to be presented to the client, should contain the identification of these documents, in structure OrderReferences of tables 4.1 to 4.3, according to the case.

1.4. The invoice correction documents should contain the identification of the document (s) corrected in structure References of table 4.1.

1.5. Whenever the program is used in Training Mode, the issued documents shall, in a specific series, indicate in the header, the data identifying the software developer company instead of the customer’s company and the following expression shall be printed in the documents: “Documento emitido para fins de Formação” (Document issued for Training purposes), even if the documents are printed on the customer’s business writing paper (letterhead).

1.6. All types of documents, identified by their correspondent designations, shall be issued chronologically in one or more series duly referred to, according to the commercial necessities and dated and numbered progressive and continuously within each series, for a period of not less than one fiscal year, notwithstanding the use for longer periods if used until the end of the running fiscal year.

1.7. When identifying the documents, the set of characters must not violate the validation scheme or interpreted as operators of XML. No other information can be part of the numerical sequence (as for example the year or the number of the electronic terminal, etc.) which, if existing, must always be part of the document series identification.

1.8. The identification code of the document series must be specific of each of the establishments and/or programs and may never be repeated for the same taxable person for the same type of document in order to identify uniquely each issued document, even if the documents are issued by more than one invoicing program.

1.9. If for technical or operational reasons a series is discontinued, the program must inhibit its use not allowing the deletion in any way of the correspondent information.

1.10. Unless it is completed and signed, no document can be printed, even if in preparation status or preview mode, according to the procedures listed in 2.1 and 2.2.

1.11. The program cannot allow that on a document that has already been signed, any information with fiscal relevance is edited, in particular the elements mentioned in articles 36 and 40 of the VAT Code, in Decree No. 147/2003, of the 11 July and in articles 6 and 7 of Ordinance No. 363/2010, of the 23 of June.

2. DOCUMENT IDENTIFICATION PROCESS (DIGITAL SIGNATURE) AND SUBSEQUENT RECORDING IN DATABASES

2.1. Signature's process for the identification of documents:

2.1.1. In the identification process of documents, namely an invoice or invoice correction documents, transport documents, valued or not, documents for checking the delivery of goods or of services rendered, etc., a digital signature shall be generated through the RSA algorithm based on the information pursuant to paragraph 1 of article 6 or paragraph 2 of article 7 of Ordinance No. 363/2010, of the 23 of June, and on the private key of the invoicing program developer.

2.1.2. The aforementioned digital signature shall be recorded in the invoicing program data base (which cannot be encrypted and should be kept during the legal archiving period), directly associated to the original document's record, according to paragraph 2 of article 6 of Ordinance No. 363/2010, of the 23 of June.

2.1.3. Additionally the version of the private key (sequential integers) that was used to generate the signature of the respective document shall be recorded, pursuant to paragraph 2 of article 6 of Ordinance No. 363/2010, of the 23 of June.

2.1.4. The key pair used by the certified program may only be changed by the software developer company after communication to the Tax and Customs Authority through a declaration Model 24 and the upload of the correspondent public key.

2.1.5. As a rule, the documents are signed taking into account the Hash of the last document of the same series/type. In case of a first saved document of a series/type of invoicing document, the applicable field Hash in tables 4.1 to 4.3, must be assumed as not filled in. In case of multiannual series, at the beginning of each year, the first document may be signed considering the Hash of the last document issued from the same series/type, during the previous fiscal year.

2.1.6. The amount to be used in the GrossTotal field of tables 4.2 and 4.3, for the signature of documents regarding the movement of goods or checking documents is the same as in the database, regardless of the used print form, both valued or not. In case no amount is shown on the database, the mentioned field must be filled in with "0.00" (without quotes) and considered as such when signing.

2.1.7. In case the document is issued in a foreign currency, the amount must be the counter value in EUR, once this will be the amount exported on the SAF-T (PT) file.

2.2. **Moment for printing or sending an electronic document:**

2.2.1. The documents susceptible of being digitally signed can only be printed after having been duly identified pursuant to article 6 and 7 of Ordinance No. 363/2010, of the 23 of June and complying with point 2.1.

2.2.2. The printed document submitted to the customer or the sent electronic document shall imperatively have four characters of the signature [fields Hash corresponding to the subordinate tables of table 4 – SourceDocuments of SAF-T (PT)] corresponding to positions 1, 11, 21, and 31 and separated by "-" (hyphen) from the expression "Processado por programa certificado n.º <Number of the certificate attributed by the Tax and Customs Authority>/AT". Example: "AxAx-Processado por programa certificado n.º 0000/AT" (Processed by a certified program nº 0000/AT), (without quotation marks), according to a) and b) of paragraph 3 of article 6 of Ordinance No. 363/2010 of 23 of June.

2.2.3. Any document issued by the certified program, printed or sent electronically, not susceptible to be signed according to point 2.1, in particular receipts, must explicitly present the expression – "Emitido por programa certificado n.º <Number of the certificate attributed by the Tax and Customs Authority>/AT". Example: "Emitido por programa certificado n.º 0000/AT" (Issued by certified program nº 0000/AT), (without quotation marks).

2.2.4. The documents mentioned under point 1 must, when printed, indicate the date in format "AAAA-MM-DD" or "DD-MM-AAAA" (without quotation marks) and according to paragraph 3 c) of article 6 of Ordinance No. 363/2010, of the 23 of June, the internal code of the type of document assigned by the program, the series of the document and the own sequential numbering, exclusively numeric.

2.2.5. On the invoices issued according to articles 36 and 40 of the VAT Code, delivered to clients which do not supply their tax identification (final consumers), the line corresponding to the acquirer's tax number must be made unusable or printed the expression "Consumidor final" (Final consumer) (without quotes).

2.2.6. The documents printed by the invoicing program must not present negative amounts. When necessary, invoice correction documents may be used (debit and credit notes, according to paragraph 7 of article 29 of the VAT Code), as documents correcting the purchase and sales transactions, respecting their form, content and finality. The negative amounts may only be printed in case of cancelling registers that are already part of the document or in order to settle the estimates for services provided continuously. The negative amount may never be higher than the positive amount under the same item or service on each

invoice. In case the settlement, by item or service, is higher than the positive amount, a credit note is mandatory for this settlement.

2.2.7. Deductibles, warranty amounts or withholding taxes must appear on the appropriate fields, developed for this purpose on the program, with an unchangeable description. These amounts will not have any influence on the totals of the issued document and must be included after assessing the total of the document with taxes (GrossTotal field of tables 4.1 to 4.4. Under no circumstances may types of products or services be created or the Product table be used for these purposes.

2.2.8. The printing by the integrating program of integrated documents, must mention this feature including the expression “Cópia do documento original” (without quotes) - “Copy of the original document” - notwithstanding other applicable expressions.

2.2.9. The documents created through the procedure mentioned under 2.4. must contain, when printed, the expression – “Cópia do documento original” (Copy of the original document) and separated through a hyphen the elements contained in point 2.4.5.2.

2.2.10. Example: Cópia do documento original -FTM abc/00001

2.2.11. The documents created through the procedure mentioned in 2.5., must contain, when printed, the expression – “Cópia do documento original” (Copy of the original document) and separated through a hyphen the elements mentioned under 2.5.5.2.

2.2.12. Example: Cópia do documento original - FTD XY 2013A/00099

2.2.13. The documents referred to under point 1, if when printed results more than one page, must present on each page the designation of the document type, the correspondent numbering, according to point 2.2.4., the accumulated amounts (transported and to be transported), the respective page number and the total number of pages. The global assessment of taxable bases, tax rates and total value of the document, if existing, must only appear on the last page.

2.2.14. The program must ensure that the content of paragraph 3 of article 6 of Ordinance No. 363/2010, of the 23 of June, is legible when the document is printed. For example, these elements must not be placed on the 1st or last line or near the limits of the document in order to avoid them not being printed due to any malfunctioning of the printer or of the printing area definition.

2.2.15. In case pre-printed paper is used when printing the documents mentioned under point 1, the program must ensure that all the fiscally relevant elements are printed including the mandatory statements, the identifying elements of the issuing taxable person and the type of document. The printing of the logo is not included in this context.

2.2.16. The printing of documents where the transmission of goods or services is VAT exempted, must show the expression foreseen by law, granting exemption or the applicable legal cause. In case the reason for exemption is not presented on the correspondent line, any other type of reference must be used allowing linking the exempted line to the correspondent reason. The same applies when associating any tax rate to the correspondent product/service.

2.2.17. The printed duplicate must preserve the original content as well as an indication that it is not an original. Thus, in case the address or name of a client is changed in the database, the reprinting of a document must respect the original address and name.

2.3. **Documents integrated in the invoicing data base, originated in other solutions:**

2.3.1. Given the existence of various invoicing solutions to meet the taxpayers' different needs, namely the invoicing in decentralized systems or in mobile systems (the so-called mobility solutions), one shall bear in mind rules which aim the definition of the information integration conditions among different invoicing systems.

Thus, the integrating program must not do any recalculation or modification of the content of the documents from other systems, respecting inclusively the unique identification of the document (*InvoiceNo, DocumentNumber* or *PaymentRefNo*), with following exceptions (see 2.3.4).

2.3.2. The signature mentioned under 2.1. is, in this case, a responsibility of the original solutions (integrated solutions).

2.3.3. A certain series/type of invoicing document, movement of goods or any other document susceptible to be presented to the client to prove the delivery of the goods or the service rendered must not contain documents of different origins (example: contain documents created in the system and imported from an external system in a same series/type of invoicing document).

2.3.4. Thus, the central system that performs the integration must:

a) Integrate the documents from other systems, in the series/types of original documents, distinct and autonomous from the ones used for its own issuing, on the correspondent tables of commercial documents (4.1., 4.2. or 4.3) as the integrated documents are understood as copies of the original document, in those tables;

b) Insert the information in field *Hash* just like created in the issuing system, in tables 4.1 to 4.3 where the document is integrated, that is, must be the same in the integrating and integrated system;

c) Fill in the fields *SourceBilling* in tables 4.1 to 4.3 depending on the case, with "I" (without quotes);

d) The *HashControl* Field, in tables 4.1 to 4.3, depending on the case , must be filled in with the number of the certificate which signed the document in the original system and the correspondent private key version;

e) The format of the information to be recorded in the *HashControl* fields of the tables 4.1 to 4.3, pursuant to the previous subparagraph will result of linking together the number of the original certificate + dot + version of the private key used in the original signature of field *Hash* of the mentioned 4.1. to 4.3 tables:

Example: "9999.1" (without quotes), where "9999" is the number of the certificate of the issuing program and "1" is the version of the private key used in the respective signature;

f) In case the information to be integrated comes from a non certified program, the value in field *HashControl* of tables 4.1 to 4.3, applicable to the type of information, must be "Não

certificado" (Not certified) - without quotes. The correspondent value in field *Hash* must be "0" (zero). The documents in these cases should not be reprinted by the integrating program.

2.4. **Integration of documents processed manually in forms issued by authorized printing-offices, in cases of inoperability of the program:**

2.4.1. The integration of invoices or other invoice correction documents and transport documents, manually processed must be made on the certified program in a specific annual series or a series with a higher periodicity and with its own sequential numbering, starting at 1.

2.4.2. Therefore, a new document of the same type must be processed to collect all the elements of the document issued manually, complying with the requirements defined in article 6 of Ordinance No. 363/2010, that is, it must sign the document and print the correspondent expression in paragraph 3 a) and b) of the same article.

2.4.3. In the recovery series, the date of the document corresponds to the date of the manual document and it is recommended to create separate mandatory fields, one for the identification of the manual series and another one for the manual number, in order to avoid mistakes when collecting this type of documents, in particular regarding the series. There may be created as many series as those existing in the manual documents or one single series.

2.4.4. Fill in field SourceBilling of tables 4.1 and 4.2, depending on the case, with value "M" (without quotes).

2.4.5. In these cases, the field HashControl of tables 4.1 and 4.2, depending on the case, shall include the following information:

2.4.5.1. Version number of the private key (1,2, etc.) and separated by a "-" (hyphen);

2.4.5.2. Sequential register of following elements: the acronym in field *InvoiceType* or *MovementType*, regards the correspondent type of document, followed by letter M, a space, the series of the manual document; character "/"; the number of the manual document.

Example: 1-FTM abc/00001, where "abc/00001" is the series/number of the manual document.

2.4.6. In order to refer to a manual document collected in the program, the series and number of the original manual document must be used and not its InvoiceNo or DocumentNumber allocated by the program to the recovered document. (Example: The emission of a credit note should refer the number of the original invoice, issued manually.)

2.4.7. Whenever it is necessary to integrate other types of manual documents, the applicable fields of the table related to these documents must be used, proceeding just as referred to in the previous numbers.

2.5. **Integration of documents through duplicates which do not integrate a backup copy, in case of necessary data recovery due to inoperability of the system:**

2.5.1. In case of error or program inoperability, the series in use must be closed and new ones created, in order to proceed with the emission of documents, after having restored the last security backup.

2.5.2. The integration of issued documents, not part of the backup copy must be done on the certified program, through the duplicates of these documents on a specific annual series and with its own sequential numbering starting at 1.

2.5.3. Therefore a new document will be processed of the same type of the duplicate collecting all the elements of this issued document, complying with the requirements of articles 6 and 7 of Ordinance No. 363/2010.

2.5.4. SourceBilling Field in tables 4.1 to 4.2, depending on the case, must contain value "M" (without quotes).

2.5.5. In these cases, HashControl field in tables 4.1 and 4.2, depending on the case, must contain the following information:

2.5.5.1. Version number of the private key (1,2, etc.) and separated by "-" (hyphen);

2.5.5.2. Sequential register of following elements: the acronym in field InvoiceType or MovementType depending on the case, which must correspond to the type of document to recover via duplicate followed by letter D; a space and the InvoiceNo or DocumentNumber, as appropriate).

Example: 1-FTD XY 2013A/00099, where "XY 2013A/00099" is the *InvoiceNo* (or *DocumentNumber*) of the integrated document.

2.5.6. On the data recovering series, the date of the document corresponds to the date of the duplicate of the document. It is highly recommended to create separate mandatory fields to allocate the internal code of document type, series and number of duplicate in order to avoid failures when collecting this type of documents, in particular of the internal code of the type of document and series. As many series as those existing in the document's duplicates or a single series may be created.

2.5.7. When referring to an original document collected in the program, the originals of the internal code of document type, of the document series and of the number must be used and not the *InvoiceNo or DocumentNumber* allocated by the program to the recovered document.

2.5.8. Whenever it is necessary to integrate other duplicates of other types of documents, the applicable fields must be used and proceed as described in the previous numbers.

2.6. **Exporting a SAF-T (PT) file:**

2.6.1. The XML file of the SAF-T (PT) must comply with Ordinance No. 321-A/2007 with the syntactic structure of data in force and the appropriate validation schema.

2.6.2. All the field elements (tags) defined as mandatory of all the tables applicable to the file type must be part of this file, as well as all the fields which have values in the program even if not defined as mandatory.

2.6.3. The rule to ensure unique values for the elements indicated in the technical notes of the data structure in the correspondent tables must be respected to keep the integrity of the content of the XML SAF-T (PT) file. The elements mentioned in the tables regarding trading documents (4.1 to 4.3) must exist in correspondent master tables (2.2 to 2.5).

2.6.4. The user is not allowed to define the types of documents or information to be entered in the database that are liable to be exported to a SAF-T (PT) file. This definition is assured by the program only.

2.6.5. The XML SAF-T (PT) file must contain in the fields of tables 4.1 to 4.3, of the *SourceDocuments*, regarding the *Hash* and *HashControl* of each structure, respectively, the signature and the version (sequential integers) of the used private key, both previously recorded in the database at the beginning of the document issuing process.

2.6.6. The documents eventually saved in the database of any management solution, but originally created in another system must be exported to the SAF-T (PT) with fields *Hash* and *HashControl* of correspondent tables 4.1 to 4.3, filled in according to 2.3.2 to 2.3.4 and additionally exported from the original solution with the mentioned fields duly filled in accordingly.

2.6.7. The amounts in fields *GrossTotal* of tables 4.1 to 4.3, must be exported with the same value as considered for signature, rounded off to two decimals.

3. OTHER REQUIREMENTS TO BE MET BY THE PROGRAM

3.1. **The program should:**

3.1.1. Have adequate access controls, obliging the user to change the *password* when first accessing and subsequently whenever necessary. The new password cannot be void and the administrator is not allowed to see or know the password. The administrator may start a proceeding of new password creation which must also be changed at the first user login.

3.1.2. Have an implemented policy of security backups of mandatory periodicity in order to minimize the data volume to be recovered in case of database corruption and/or keeping two or more simultaneous databases in case one should be corrupted so the other may allow the invoicing to continue.

3.1.3. Direct or indirect control of the database used and the register of the number of backups, for instance, through control systems that validate the database when closing and starting the program in order to show eventual handling or changes of data in the database by other means than through the program.

3.1.4. Protect in an efficient way the private key, even during the signature process of the documents.

3.2. **The program should ensure:**

3.2.1. The sequenced numbering depending on the evolution of the date and time of the document issued.

3.2.2. The guarantee that there is no more than one active document (with fields – *InvoiceStatus*, *MovementStatus*, *WorkStatus* or *PaymentStatus* – presenting value "N") from the same document in manual version or from the proceeding mentioned under 2.5.

3.2.3. The use, for calculation matters, of a value with more than 2 decimal cases in order to avoid mistakes in rounding off, motivated by discounts, unitary prices under one cent, fractioned quantities, exchange rates or due to the emission of documents which price includes tax.

3.2.4. In mobility solutions, the sequential number as well as the information regarding the signature of the last documents issued for each series after having exported the data into the integration program.

3.2.5. Compliance with the requirements listed in paragraph 1 of article 9 of Ordinance No. 363/2010, of the 23 of June when issuing any conferring document regarding provided services.

3.2.6. The enforceability for the user to present a reason for not assessing tax, if it is the case.

3.2.7. The control over partial credit notes issuing, compared to the quantities and values of the invoices to be corrected.

3.2.8. Discounts, if existing, must range from 0% to 100%.

3.2.9. That the parameterisation and layout of the printing forms of the documents is made by the program developer or, if the user has the possibility of creating new types of documents these must be validated by the program developer, for instance, through digital signature. Forms without this mentioned validation and not complying with 3.3.1. cannot be used.

3.2.10. Maintenance of the information regarding all the documents in its data repository, in particular those in the existent tables in structure 4. – *SourceDocuments* of file SAF-T (PT). The program should have controlling mechanisms to force the external production of file copies whenever the capacity limit of the database or of its physical support is attained, in order to ensure the export capacity of SAF-T (PT) respecting the requirements of the certification ordinance and complying within the deadline defined by paragraph 1 of article 52 of the VAT Code.

3.2.11. That the preview screens for entering and exporting data, consulting and other functionalities available to the user, regardless of their access level to the program, are displayed in Portuguese, multilingual or with a Portuguese translation.

3.2.12. The registration of the date when the goods were made available to the acquirer or when the services were provided, in order to allow the correct filling out of field *TaxPointDate.*

3.3. **The program must not allow:**

3.3.1. The user to define which types of documents are signed and/or exported to the SAF-T (PT), in particular those created or modified by him/her.

3.3.2. Any calculation of the documents collected or resulting from the integration of other systems. For example, in case there should be a wrong tax assessment, the mistake must be presented in the integrating database once it results from a document already issued.

3.3.3. The change of tax number on an existing client file and with already issued documents. A missing tax number can only be entered if the field is empty or filled in with the generic client tax number “999999990”.

3.3.4. The change of name in an existing client file with already issued documents but without indicated tax number. This limitation ends when the correspondent tax number is indicated in the clients file.

3.3.5. The change, in an existing product file with already issued documents, of the *ProductDescription field* on table 2.4.

3.3.6. Reuse of user id (*SourceID)* after relevant fiscal moves made by that user.

3.3.7. Creation of credit notes regarding previously cancelled documents or already fully rectified.

3.3.8. Cancelling documents which have already an issued invoice correction document (credit or debit note) even if partial, without the previous cancelling of the correspondent invoice correction document.

3.3.9. Accepting returns on invoices or transmissions on invoice correction documents.

3.4. **The program should alert the user:**

3.4.1. If any of the compulsory SAF-T (PT) fields has not been filled in by the user, when issuing the documents.

For example: The master data on the client, supplier, product, tax type and tax rates files or reason for tax exemption.

3.4.2. When the document issuing date is later than the current date, or superior than the date on the system. In this case, after having been issued, no other document may be issued with the current or previous date within the same series.

3.4.3. In case the system date and hour is previous to the last issued document, a confirmation must be requested before issuing the document that the system date and hour is correct. This must be validated using the SystemEntryDate of any type of issued document, regardless of the series.

4. TECHNICAL REQUIREMENTS REGARDING THE IDENTIFICATION SYSTEM PROVIDED FOR IN PARAGRAPH B) OF ARTICLE 3 OF ORDINANCE No. 363/2010 , OF THE 23 OF JUNE

4.1. The RSA algorithm (algorithm of data cryptography which uses asymmetric keys, public key and private key) shall be used.

4.2. The public key to be supplied along with the declaration Model 24, must result from its extraction from the private key in PEM format – base 64 and the respective file with the extension ".txt" must be created.

4.3. The program developer must ensure that the private key used for the creation of the signature is known exclusively by him and must be protected in the program.

4.4. The text to be signed on the document must contain the concatenated data in the format specified in the technical notes for each field, separated by ";" (Semicolon).

4.5. The documents issued and included in table 4.1 – *SalesInvoices* mentioned in field *InvoiceType*, must use the information mentioned in article 6 of Ordinance No. 363/2010, of the 23 of June, as exemplified hereunder:

Field in SAF-T (PT)	Format	Data Example
a) ***InvoiceDate***	AAAA-MM-DD	2013-07-01
b) ***SystemEntryDate***	AAAA-MM-DDTHH:MM:SS	2013-07-01T11:27:08
c) ***InvoiceNo***	Composed by the internal document code followed by a space, followed by an identifier of the series of the document (mandatory), followed by a bar (/) and by a sequential number of the document within the series. [^]+ [^/^]+/[0-9]+	FS 001/0009

d) ***GrossTotal***	Numerical field with two decimal points, decimal separator "." (dot) and without any separator for the thousands.	200.00
e) ***Hash*** *Fields of the previous document in the same series, (empty if it is the first document of the series or of the fiscal year)*	Base-64	mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/J8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJ9G6nI=

4.6. Example of the message to be signed for the indicated data:

2013-07-01;2013-07-01T11:27:08;FS 001/0009;200.00;mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJG6nI=

4.7. Documents issued and included in table 4.2 – MovementOfGoods referred to in field MovementType, must use the information mentioned under paragraph 2 a) of article 7 of Ordinance No. 363/2010, 23 of June, as exemplified in following table:

Field SAF-T (PT)	Format	Data Example
a) ***MovementDate***	AAAA-MM-DD	2013-07-02
b) ***SystemEntryDate***	AAAA-MM-DDTHH:MM:SS	2013-07-02T09:37:25
c) ***DocumentNumber***	Composed by the internal document code followed by a space, followed by an identifier of the series of the document (mandatory), followed by a bar (/) and by a sequential number of the document within the series. [^]+ [^/^]+/[0-9]+	GR ABC/00021
d) ***GrossTotal***	Numerical field with two decimal points, decimal separator "." (dot) and without any separator for the thousands. In cases like this one, where the document has no value, this field must be filled in with "0.00" (without quotes).	0.00

e) ***Hash*** *Fields of the previous document in the same series, (empty if it is the first document of the series or of the fiscal year)*	Base-64	mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/J8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJ9G6nI=

4.8. Example of the message to be signed for the indicated data:

2013-07-02;2013-07-02T09:37:25;GR ABC/00021;0.00;mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJG6nI=

4.9. Documents issued and included in table 4.3 – WorkingDocuments referred to in field WorkType, must use the information mentioned in paragraph 2 b) of article 7 of Ordinance No. 363/2010, 23 of June, as exemplified hereafter:

Field in SAF-T (PT)	Format	Data Example
a) ***WorktDate***	AAAA-MM-DD	2013-07-03
b) ***SystemEntryDate***	AAAA-MM-DDTHH:MM:SS	2013-07-03T14:25:00
c) ***DocumentNumber***	Composed by the internal document code followed by a space, followed by an identifier of the series of the document (mandatory), followed by a bar (/) and by a sequential number of the document within the series. [^]+ [^/^]+/[0-9]+	RC 005/001
d) ***GrossTotal***	Numerical field with two decimal points, decimal separator "." (dot) and without any separator for the thousands.	1500.00
e) ***Hash*** *Fields of the previous document in the same series, (empty if it is the first document of the series or of the fiscal year)*	Base-64	mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/J8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJ9G6nI=

4.10. Example of the message to be signed for the indicated data:

2013-07-03;2013-07-03T14:25:00;RC 005/001;1500.00;mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJG6nI=

5. CREATION OF PRIVATE / PUBLIC KEY PAIR

To illustrate the creation of the RSA key pair, the OpenSSL software was used, which is performed directly on the command line with parameters (Windows / Linux, etc.), and can be obtained at www.openssl.org.

Among other functionalities it allows to create RSA, DH and DSA keys, X.509, CSRs and CRLs certificates, to sign digitally, to encrypt and to decrypt, etc...

In the analysis of the presented examples, we must take into account that:

a) They are merely illustrative. It does not mean that the program developer has to use the OpenSSL software;

b) The respective command lines were prepared and tested either in Linux or Windows, and the same final result was achieved;

c) The use of the command ECHO applied on the commands line of the Windows/DOS, may present results different from those obtained in Linux, so it must not be used for test purposes;

d) They are carried out with the PEM format.

5.1. In order to create the private key:

Simply operate the OpenSSL command with following parameters:

openssl genrsa -out PrivateKey.pem 1024

Where “PrivateKey.pem” is the file name which is going to contain the private key and “1024” is the size in bits.

In this case, as a result was obtained the following information, of which is shown a part:

-----BEGIN RSA PRIVATE KEY-----

MIICXQIBAAKBgQCjgbQG27+lNWKdW5SXLFzFgqZu+xFWTkx0Woloo6z1gD5DhllRgQ5hxitOW0QV1L
AGlHVMfZ8PDk9e+N4YJ7cDwW4D+iflyCAEvi4xvKejEGVEInEsnA7actmg9ORORMHXKqy
7mA41P//.....

-----END RSA PRIVATE KEY-----

5.2. In order to create the public key based on the previous private key:

Simply operate OpenSSL command with the following parameters:

Openssl rsa-in PrivateKey.pem -out PublicKey.pem -outform PEM –pubout

Where “PublicKey.pem” is the file which contains the public key.

To upload the Public Key together with the declaration Model 24, it is enough to rename its extension from “pem” to “.txt” (without quotations).

In this case, as a result, was obtained the following information, of which is shown a part:

-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCjgbQG27+lNWKdW5SXLFzFgqZu+xFWTkx0Woloo6z1gD5
DhllRgQ5hxitOW0QV1LAGlHVMfZ8PDk9e+N4YJ7cDwW4D+iflyCAEvi4xv KejEGVEInEsnA7actmg9ORO ...

-----END PUBLIC KEY-----

5.3. In order to verify the public key

Simply execute OpenSSL command with following elements:

openssl rsa -in PublicKey.pem **-noout -text -pubin**

6. CREATION OF THE CERTIFICATE

6.1. The used key pair does not require the issue of a certificate by an authorized entity. The program developer may generate a self-signed certificate for certification purposes and from this certificate the public key can be extracted to submit to the Tax and Customs Authority, with the.txt extension.

6.2. For the creation of the certificate from the private key, the RSA algorithm must be used with the following specifications in the parameters:

- Format = x.509
- *Charset* = UTF-8
- *Encoding* = Base-64
- *Endianess* = *Little Endian*
- OAEP *Padding* = PKCS1 v1.5 *padding*
- Size of the private key = 1024 bits
- Format of the *Hash* of the message = SHA-1

7. PRACTICAL EXAMPLE OF THE SIGNATURE MECHANISM FOR DOCUMENTS INCLUDED IN TABLE 4.1 – SALESINVOICES

7.1. Creation of the digital signature by means of a private key

Independently of the RSA implementation that is adopted and that is more adequate to each solution, it must be ensured that the signatures have 172bytes, without any lines separating characters.

FIELDS IN SAF-T (PT)	RECORD 1	RECORD 2
InvoiceDate	2010-05-18	2010-05-18
SystemEntryDate	2010-05-18T11:22:19	2010-05-18T15:43:25
InvoiceNo	FAC 001/14	FAC 001/15
GrossTotal	3.12	25.62
Hash	See "1st record"	See "2nd record"

The elements to be signed (*InvoiceDate*, *SystemEntryDate, InvoiceNo*, *GrossTotal* and *Hash*) must be concatenated by the separator "; "(Semicolon) only, between each of the fields, and must not include quotation marks or any end of line character, when they are to be encrypted, in order to obtain the signature.

1st Record

Being the first record, *Hash* field is filled in with the hash resulting from the use of the private key previously created, to sign digitally the fields (*InvoiceDate*, *SystemEntryDate*, *InvoiceNo* and *GrossTotal*).

The text to be signed will be as follows:

2010-05-18;2010-05-18T11:22:19;FAC 001/14;3.12;

1st Step:

Save the message to be signed

2010-05-18;2010-05-18T11:22:19;FAC 001/14;3.12;

In a text file (which in this example is named Record1.txt), ensuring that in the end of the message there is no line breaking, only the ";" (Semicolon) without quotation marks.

2nd Step:

To sign the message contained in the file Record1.txt with the following command:

openssl dgst -sha1 -sign PrivateKey.pem -out Record1.sha1 Record1.txt

The file Record1.sha1 must contain the hash in binary generated by the OpenSSL software.

3rd Step:

Afterwards it is necessary to do the encoding for base 64 of file Record1.sha1:

openssl enc -base64 -in Record1.sha1 -out Record1.b64 -A

The file named as Record1.b64 is the one that contains the 172 characters in ASCII of the signature which must be recorded to the data base and later on exported to the *Hash* field of the SAF-T (PT).

The parameter –A is used to generate the signature by the OpenSSL in just one line avoiding the additional line breaks.

Consequently the file Record1.b64 will have the following signature:

oso2FoOw4V941CwKTrv6xwzUrOtxBWCwU0yLVAqKwf0CNKZHMETG1XZZC4spRSyby1uDXBggpIogrl8gHnvevA00UEoAvGJo9Fa3DOA0MhZNDa9/rNvu71pp+0zHmN2ra5lWpiHcgmUYxm5qamLBk49rkgvI7h1myKCYBKqgu60=

This signature must be recorded in the *Hash* field of the above table in the position corresponding to Record 1.

2nd Record

Using an identical procedure, but now with the data of Record2 and the hash of the previous record we should have as a message to be signed in the file Record2.txt:

2010-05-18;2010-05-18T15:43:25;FAC 001/15;25.62;oso2FoOw4V941CwKTrv6xwzUrOtxBWCwU0yLVAqKwf0CNKZHMETG1XZZC4spRSyby1uDXBggpIogrl8gHnvevA00UEoAvGJo9Fa3DOA0MhZNDa9/rNvu71pp+0zHmN2ra5lWpiHcgmUYxm5qamLBk49rkgvI7h1myKCYBKqgu60=

Using the procedures abovementioned for Record1, from step 1 to step3, file Record2.sha1 and file Record2.b64 were created.

Consequently, this last file, Record2.b64 shall have the digital signature of record 2:

Y2ogVAC9rcmm9hilZCGGrxjpkZP9NHn5shhp9phBIVWln+Ta2zKf+O+05brA6VU0LULtMQP98P29q+vcSwVtxSzLDbmmkHMt4l6nQmh91QaOJwPpz2uMqtR3aMkWYPK4Ntc/yfnXpY1cSeUGbQkqAsJOFSidRE4+DibJaC7WMpw=

Which must be recorded in *Hash* field of the above table and in the position corresponding to Record 2.

7.2. Validation of the created digital signature

To confirm the validity of the signatures it is enough to operate the command:

openssl dgst -sha1 -verify PublicKey.pem - signature Record1.sha1 Record1.txt

8. REVOCATIONS

Circular Letter No. 50001/2013, of the 4 of July is hereby revoked.

The 24th of June, 2014. — The Director-General, José A. Azevedo Pereira.