The authenticity, integrity and legibility of electronic invoices in Europe from 1 January 2013

Qualified Electronic Signatures and Continuous Auditing
Dr. Umberto Zanini

Certified Public Accountant and Auditor in Italy


Since 2006, director of technical and regulatory research at the “Observatory on Electronic Invoicing and Dematerialisation” at the Polytechnic of Milan

Member of the ICT commission of the Italian Accountancy Profession (CNDCEC)

I provide the following services in relation to e-invoicing and EDI:

- Consultancy in relation to international legislation and regulations
- Monitoring of legislative and regulatory developments
- Feasibility studies and analyses
- Project/process auditing
- Software/service auditing

For further information: www.umbertozanini.com

Please forward any remarks and suggestions to u.zanini at tin.it

Legal Information

Parts of this document may be reproduced on condition that the source is cited.

This document is purely educational in scope, and therefore does not constitute a form of professional consultancy, nor may it be used for any such purposes.
Table of contents

Table of contents .................................................................................................................................. 3
Summary of figures .................................................................................................................................. 4
List of abbreviations .............................................................................................................................. 5
1. Introduction ...................................................................................................................................... 8
3. Qualified Electronic Signature (QES) ........................................................................................... 15
   3.1. Principal aspects of QES ......................................................................................................... 15
   3.2. How QES works ...................................................................................................................... 23
      3.2.1. Hash functions .............................................................................................................. 23
      3.2.2. Creating the QES ........................................................................................................... 24
      3.2.3. Verifying the QES .......................................................................................................... 25
   3.3. Centralised use of HSM in a MNE or SP ................................................................................ 26
   3.4. The Time-Stamp Token .......................................................................................................... 27
4. BCRATIS ....................................................................................................................................... 29
   4.1. Definitions ............................................................................................................................... 29
      4.1.1. Business controls .......................................................................................................... 30
      4.1.2. The reliable audit trail .................................................................................................... 31
      4.1.3. The electronic audit evidence ......................................................................................... 33
   4.2. What BCRATIS is .................................................................................................................. 34
   4.3. How to implement a BCRATIS .............................................................................................. 35
      4.3.1. The fundamental principles ............................................................................................ 35
      4.3.2. Methodology ................................................................................................................... 37
   4.4. The BCRATIS run with Continuous Auditing ....................................................................... 47
      4.4.1. What Continuous Auditing is .......................................................................................... 47
      4.4.2. CARATIS ....................................................................................................................... 49
5. Conclusions ..................................................................................................................................... 53
Documents ......................................................................................................................................... 56
Summary of figures

Figure 1. Methods for ensuring authenticity, integrity and legibility ............................................................... 12
Figure 2. The grace period .............................................................................................................................. 22
Figure 3. QES creation process ..................................................................................................................... 24
Figure 4. QES verification process ............................................................................................................... 25
Figure 5. Centralised use of an HSM ......................................................................................................... 27
Figure 6. TST creation process .................................................................................................................... 28
Figure 7. TST verification process .............................................................................................................. 29
Figure 8. The reliable audit trail ............................................................................................................... 32
Figure 9. Documents exchanged .............................................................................................................. 35
Figure 10. The life cycle of a document ..................................................................................................... 36
Figure 11. Definition of the Matches between the documents ................................................................... 39
Figure 12. Matching matrix ......................................................................................................................... 41
Figure 13. Risk and control matrix ............................................................................................................ 43
Figure 14. The Control Activities Flowchart ............................................................................................. 45
Figure 15. Overview of the operation of a CARATIS .............................................................................. 51
Figure 16. An Auditor’s CARATIS Report ................................................................................................. 52
List of abbreviations

AdES  Advance Electronic Signature

BCRATIS  Business Controls which create a Reliable Audit Trail between an Invoice and a Supply of goods or services.

CA  Continuous Auditing

CAATs  Computer Assisted Audit Techniques

CARATIS  Continuous Auditing which create a Reliable Audit Trail between an Invoice and a Supply of goods or services

CRL  Certificate Revocation List

CSP  Certification Service Provider, as defined in Article 2.11 of Directive 1999/93/EC ("certification-service-provider’ means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures)

CSP/QC  Certification Service Provider which issues Qualified Certificates, in conformity with the provisions of Annex II of Directive 1999/93/EC

EDI  Electronic Data Interchange


ERP  Enterprise Resource Planning
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES</td>
<td>Electronic Signature</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>MNE</td>
<td>Multinational Enterprise</td>
</tr>
<tr>
<td>O2C</td>
<td>Order-to-Cash</td>
</tr>
<tr>
<td>O2I</td>
<td>Order-to-Invoice</td>
</tr>
<tr>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>P2I</td>
<td>Purchase-to-Invoice</td>
</tr>
<tr>
<td>P2P</td>
<td>Purchase-to-Pay</td>
</tr>
<tr>
<td>QC</td>
<td>Qualified Certificate</td>
</tr>
<tr>
<td>QES</td>
<td>Qualified Electronic Signature as defined in Article 5.1 of Directive 1999/93/EC (&quot;advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device&quot;).</td>
</tr>
<tr>
<td>REM</td>
<td>Registered E-Mail</td>
</tr>
<tr>
<td>SCF</td>
<td>Supply Chain Finance</td>
</tr>
<tr>
<td>SME</td>
<td>Small and Medium Enterprise</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>SSCD</td>
<td>Secure Signature Creation Device</td>
</tr>
<tr>
<td>TL</td>
<td>Trust List</td>
</tr>
<tr>
<td>TM</td>
<td>Time Mark</td>
</tr>
<tr>
<td>TSA</td>
<td>Time Stamping Authority</td>
</tr>
<tr>
<td>TST</td>
<td>Time Stamp Token</td>
</tr>
</tbody>
</table>
Foreword

The idea of providing a document summarising the new legislation to be enacted on 1 January 2013, following reception by the Member States of the new Directive 2010/45/EU, is a response to the question posed by many companies and service providers: “What are business controls?”, “How do business controls work?”, “When is an audit trail considered reliable?” and “Which is better, Qualified Electronic Signature or business controls?”.

The aim of this essay is thus to provide a simple, clear and independent explanation of the main amendments to art. 233 of Directive 2006/112/EC, the operation and critical aspects of the Qualified Electronic Signature (QES), the nature of business controls and their implementation, and Continuous Auditing.

I believe it to be important to explain the main features of the electronic invoicing process, above all for companies which have yet to grasp the benefits of this solution, mostly Small and Medium Enterprises (SME), which account for 99.8% of European companies1.

This paper will not, therefore, cover other matters, however important and interesting, such as EDI, the legislation of the individual Member States and non-EU States, the critical aspects of cross-border electronic invoicing, other technological solutions and their pros and cons, etc.

I have also attempted, as far as possible, to avoid using a highly technical approach, in order to enable lay persons to clearly understand, for instance, how a Qualified Electronic Signature (QES) works, what a Time-Stamp Token (TST) is, and how business controls and continuous auditing (CA) work.

---

1 Eurostat, Statistics in focus, 2008
1. Introduction

With the globalisation of production and services, which inevitably leads to strong international competition and hence increased attention to costs, the importance of tools like electronic invoicing, with its considerable benefits for accounting processes and attendant cost savings, is very evident. In order to simplify, modernise and harmonise invoicing methods, Directive 2001/115/EC was adopted in 2001 - the directive which introduced and regulated electronic invoicing in Europe for the first time.

Ten years later, electronic invoicing has been adopted by only a minority of European companies, and this has led the European Commission to review certain fundamental principles of the process. The publication in the Official Journal of the European Union of Directive 2010/45/EU, dated 13 July 2010, which amends Directive 2006/112/EC, introduced numerous important changes which must be adopted by Member States by 1 January 2013.

The most significant changes are related to article 233 of Directive 2006/112/EC, especially in relation to the equal treatment of paper and electronic invoices, the principle that the taxable person decides which solution to adopt in guaranteeing the authenticity of the origin and the integrity of the content, and the option of adopting new methods, such as business controls.

It is clear that Directive 2010/45/EU will be accepted by the various Member States, and thus harmonised with local legislation, which reflects the diversity of the various national cultures, but it is equally clear that it is in the interest of the entire European Union that Directive 2010/45/EU be adopted without modifications.

The first part of this document will examine the new Article 233 of Directive 2006/112/EC, with special reference to the concepts of authenticity, integrity and legibility, the second part will review QES in terms of its operation and criticalities, the third part will analyse the concept of “business controls” and propose a practical method for implementing them, while the last part will consider the concept of “continuous auditing” and how it may be employed in e-invoicing processes.

A final aspect I wish to consider, which is never given sufficient weight, is that e-invoices not only lead to considerable benefits and savings, but are a powerful “key enabler” in at least three ways:

a- in enabling the introduction of Purchase-to-Pay and Order-to-Cash processes, eSupply Chain Finance and Financial Collaboration Systems;

2 “COUNCIL DIRECTIVE 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax”.

3 According to the report “E-Invoicing/E-Billing in Europe and abroad”, published by Koch Bruno-Billentis in March 2011, the level of adoption of e-invoicing in B2B is 12%, whereas in B2C it is 9%.

4 For the cost savings and benefits, refer to the annual reports of the “Observatory on Electronic Invoicing and Dematerialisation” of the Milan Polytechnic:

- Electronic Invoicing as a “keystone” in the collaboration between companies, banks, and PA, 2008
- Joint collaboration: a powerful driver for electronic invoicing in Italy, 2009
- Electronic invoicing in Italy: reporting from the field, 2010
- Beyond the invoice, 2011

5 According to ACT – Association of Corporate Treasurers, in their “Supply Chain Finance - Report of the supply chain finance working group” published in July 2010, “Supply chain finance (SCF) is a term used to define the financial relationship linking the buyer and the supplier together in terms of payables and receivables”. SCF services include pre-shipment finance, post-shipment finance, reverse factoring, and so on.
b- in enabling the adoption of effective solutions for monitoring taxpayers and reducing VAT evasion⁷ ⁸;

c- in enabling constant monitoring of public spending, if made obligatory for suppliers of goods and services to public authorities.

E-invoicing is thus not simply something to be dealt with or postponed to the future, but is rather a new way of thinking about accounting, logistical and financial processes, which can create a win-win solution for the various stakeholders: solutions of “financial collaboration” with one's suppliers and buyers, solutions which will enable financial institutions to offer innovative eSCF services, solutions which will enable the Tax Authorities to increase the efficiency of monitoring taxpayers, and solutions which will allow improved control of public spending.

It may seem premature but, for all the above reasons, it may well be time to discuss whether e-invoicing should (or not) be made obligatory for all commercial transactions in the EU.

---

⁶ By “Financial Collaboration Systems”, we mean solutions which enable the supplier and buyer to interact to their mutual financial advantage, which do not require the mediation of banks or financial institutions.

⁷ The total IVA revenue of the Member States in 2008 amounted to around 862 bn euro, and according to a study commissioned by the EU and conducted in 2009 on 2006 data (Study to quantify and analyse the VAT gap in the EU-25 Member States, Reckon LLP-London, 2009), it is evident that there is a 12% gap between actual VAT revenue of the Member States and what they should have collected, based on their own data, spread between states with small VAT gaps (Luxembourg 1%, Spain and Ireland 2%, Holland and Sweden 3%, Denmark and Portugal 4%), and others with very high VAT gaps indeed (Greece 30%, Slovakia 28%, Hungary 23%, Italy 22%).

⁸ European Commission, Green Paper On the future of VAT-Towards a simpler, more robust and efficient VAT system, COM (2010) 695
2. The new Article 233 of Directive 2006/112/EC

With Directive 2010/45/EU of 13 July 2010 published on 22 July 2010 in the Official Journal of the European Union, the European Commission has improved and simplified the use of e-invoicing by the Member States, which are required to adopt it by 1 January 2013.

The new Art. 233 of Directive 2006/112/EC states that:

“Article 233
1. The authenticity of the origin, the integrity of the content and the legibility of an invoice, whether on paper or in electronic form, shall be ensured from the point in time of issue until the end of the period for storage of the invoice.

Each taxable person shall determine the way to ensure the authenticity of the origin, the integrity of the content and the legibility of the invoice. This may be achieved by any business controls which create a reliable audit trail between an invoice and a supply of goods or services

“Authenticity of the origin” means the assurance of the identity of the supplier or the issuer of the invoice.

“Integrity of the content” means that the content required according to this Directive has not been altered.

2. Other than by way of the type of business controls described in paragraph 1, the following are examples of technologies that ensure the authenticity of the origin and the integrity of the content of an electronic invoice:

(a) an advanced electronic signature within the meaning of point (2) of Article 2 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (*), based on a qualified certificate and created by a secure signature creation device, within the meaning of points (6) and (10) of Article 2 of Directive 1999/93/EC;

(b) electronic data interchange (EDI), as defined in Article 2 of Annex 1 to Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects of electronic data interchange (**), where the agreement relating to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data”.

Before analysing this article, we must remember that the two basic principles of the revision, the principle of technological neutrality and the principle of equal treatment of paper and electronic documents are by no means novelties. Indeed, during the Ottawa Ministerial Conference of 1998, the OECD⁹ emphasised that these two principles are fundamental to the taxation of e-commerce, a principle which the OECD then extended also to information transactions¹⁰, noting that they “should be technologically neutral and should not inhibit the development of new and emerging technologies”, and “there should be no effective additional burden placed on transaction information provided electronically to that provided on traditional paper documents, recognising that there may be different data elements necessary in an electronic environment to maintain the same overall level of integrity and auditability in the system”.

---

⁹ Organisation for Economic Co-Operation and Development
¹⁰ OECD, Transaction Information Guidance, 2003
In relation to the new art. 233 of Directive 2006/112/EC, we must emphasise the following:

1- It is established that the general principle is that it is the taxable person who will determine “the way” to ensure the authenticity, integrity and legibility of the invoice, and that the said guarantees “may be achieved” by adopting certain “business controls”.

The choice of the "way" adopted in ensuring these guarantees is thus delegated to the taxable person himself, and given that no list of possible ways is given, this freedom of choice evidently requires closer analysis. The taxable person is effectively required to exhibit greater awareness in relation to the manner of ensuring the authenticity, integrity and legibility, the type of solution (in-house or full-outsourcing), the type of technology, etc.

This greater awareness does not however mean greater liability, given that whether he chooses between 2 or 10 methods, his responsibility remains the same; what changes, on the other hand, is the investment required for the analysis and evaluation of the increased range of solutions, and therefore choosing the best one.

It is clear that the evaluation will involve in-house factors, such as in which State the head offices are located, the number of invoices issued/received, the periodicity of issue/reception, the types of suppliers and buyers, the company's capacity to enforce a given solution on its suppliers and buyers, and so on, just as it will involve external factors, such as the manner in which the Member State has adopted Directive 2010/45/EU, local electronic archiving standards, legislation governing the use of Secure Signature Creation Devices (SSCD), auditing regulations, etc..

We must also consider the following three important points:

a- it must always be possible to change, over time, the manner in which the authenticity, integrity and legibility are guaranteed, for example by changing over from QES to EDI or from BCRATIS to Registered e-mail (REM);

b- it must always be possible to employ different methods for sale and purchase invoices, since the two invoicing processes may well have different degrees of complexity. This applies, for instance, to a company which builds ships, with thousands of purchase invoices and maybe only one sales invoice per year or, to give a counter-example, a company which scraps ships, which may book only one purchase invoice a year and thousands of sales invoices;

c- it must always be possible to employ different methods for the various types of sales (or purchase) invoices. This would apply, for instance, to a company with just a few large clients, in which one client requires the use of EDI, another QES, and yet another REM.

2- the "principle of equal treatment of paper and electronic invoices” is introduced, which establishes that the guarantees of authenticity, integrity and legibility apply to both paper and electronic documents.
It has often been asked whether it has sense to extend the said guarantees also to paper invoices, or whether this principle has been introduced simply to encourage more companies to use electronic invoices.
Personally, I believe it to be only proper that companies that adopt a paper invoicing system should be required to guarantee the authenticity, integrity and legibility of their documents, especially since the most elementary principles are often not implemented, for example:

- authenticity: opening the envelope in such a way as not to render the sender's address illegible, keeping envelopes with their invoices, etc.;

- integrity: issuing invoices with ink which cannot be cancelled (they are sometimes even written in pencil!), when correcting an entry the cancelled entry remains legible, etc.;

- legibility: keeping paper invoices in safe long term storage, checking the condition of the stored documents from time to time, etc..

3- The “way” proposed to ensure the above guarantees, with relation both to paper and electronic documents, is the adoption of “any Business Controls which create a Reliable Audit Trail between an Invoice and a Supply of goods or services” (BCRATIS).

This important concept is clearly restated in the recital of Directive 2010/45/EU, which states that "Invoices must reflect actual supplies and their authenticity, integrity and legibility should therefore be ensured. Business controls can be used to establish reliable audit trails linking invoices and supplies, thereby ensuring that any invoice (whether on paper or in electronic form) complies with those requirements”.

In effect, after introducing the general principle that even companies which issue paper invoices must guarantee their authenticity, integrity and legibility, BCRATIS is proposed as a method applicable to all types of invoices, whether paper or electronic, while for electronic invoices alone, two “examples of technologies”, QES and EDI are proposed.

![Figure 1. Methods for ensuring authenticity, integrity and legibility](image-url)
4- while QES can guarantee the authenticity and legibility of the document (if an unstructured electronic invoice) or data (for structured electronic invoices), EDI or REM can guarantee them during transmission, while BCRATIS can guarantee authenticity and legibility of the entire P2P or O2C process.

This is far from insignificant if we consider the growth of eSupply Chain Finance solutions and Financial Collaboration Systems, the adoption of which is often no longer centred on invoices, but on other P2P/O2C documents.

As a simple example, consider “pre-shipment finance” (or “purchase order financing”), where the bank or financial institution finances the supplier on the basis of a purchase order issued by the buyer. In such a situation, a method capable of guaranteeing the authenticity and integrity of the entire O2C process could be of critical importance to the bank in setting up “pre-shipment finance”.

5- in relation to the guarantee of “legibility of an invoice”, as distinct from its authenticity and integrity, Directive 2010/45/EU does not specify its meaning, whereas definitions of “legibility” and “readability” are given in Revenue Procedure 97-22 of the Internal Revenue Service, which states:

- “The term ‘legibility’ means the observer must be able to identify all letters and numerals positively and quickly to the exclusion of all other letters or numerals”;

- “The term ‘readability’ means that the observer must be able to recognize a group of letters or numerals as words or complete numbers”.

Note that the meaning of “readability” will depend on the type of “reader”, and indeed ETSI TS 101 533-1 V1.1.1 (2011-05)\(^\text{11}\) in its definitions states that: ”readability (document readability): possibility for a document to be visually read by human beings and/or to be machine processed”.

With the publication of the “Explanatory notes\(^\text{12}\)” while it must be recalled that “They are not legally binding and are only practical and informal guidance about how EU law is to be applied on the basis of views of DG TAXUD”, the meaning of “legibility” is definitively established:

“Legibility of an invoice means that the invoice is human readable. It must remain so until the end of the storage period. The invoice should be presentable in a style where all the VAT contents of the invoice are clearly readable, on paper or on screen, without the need for excessive scrutiny or interpretation, e.g. EDI messages, XML messages and other structured messages in the original format are not considered human readable (after a conversion process they may be considered human readable – see below)”.

It follows that if e-invoices in XML or TXT format are transmitted/received, not only the issued/received flows must be stored for the duration of the storage period, but also the software (or other tools) required to read them, such as “viewers” (in their various releases), the tools required to produce style sheets, and so on.

The guarantee of legibility does not thus apply solely to e-invoices (as can be deduced from article 233), but also to the technologies and methods employed to guarantee their authenticity and integrity, including:

---

\(^\text{11}\) ETSI TS 101 533-1 V1.1.1 (2011-05) “Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management”

\(^\text{12}\) “Explanatory notes VAT invoicing rules”, 5 October 2011
- for QES, the Qualified Certificates must guarantee legibility;
- for BCRATIS, the electronic audit evidence and audit trail must guarantee legibility;
- for REM, the system must guarantee legibility.

The guarantee of legibility of an invoice, “shall be ensured from the point in time of issue until the end of the period for storage of the invoice”, however:

a- it should always be possible to transmit invoices which are illegible due to encryption with a secret key, as long as the key is available to one or more members of staff clearly designated in the “Signature policy”, able to render the invoices legible when requested to do so;

b- the guarantee of legibility must be ensured throughout the period of storage of the e-invoices, but in this case, since the legislation of the individual Member States applies to electronic archiving, some Member States do not admit the electronic archiving of documents which are illegible because they have been encrypted with a secret key.

6- it is specified that “Integrity of the content” means that the content required according to this Directive has not been altered”.

Two aspects must be considered:

a- the content of an invoice is not solely the information required by Directive 2006/112/EC (for example, that given in art. 226), but includes other information, such as may be required by local legislation or by the industrial sector in which the company is operating.

In such cases, the guarantee of “Integrity of the content” must cover the entire contents of the invoice;

b- the content of an invoice “has not been altered” - meaning that the data may not be changed, must remain unaltered, although the manner in which they are laid out and ordered (their syntax), may vary according to the standards in use.

Indeed, whereas QES crystallises the document, when EDI, BCRATIS and REM are used, the standards (UBL 2.0, CII v.2, etc.) used by the SPs to transmit data may vary, although the data itself is not affected.

For example, suppose that:

- issuer “X” with offices in the USA employs SP No.1 which transmits data using EDI standard ANSI X12 to network Alpha;
- inside network Alpha, the data is handled by SP No.2, which converts them to standard UBL 2.0, and transmits them to SP No.3 which is part of network Beta;
- SP No.3, which receives the data in standard UBL 2.0, converts them to standard CII v.2., and transfers them to the final user “Y” based in the UK using standard CII v.2.

While it is clear that the manner in which the data are ordered and laid out (syntax) cannot be the same throughout the process, given that various standards apply, the important thing is that user “Y” receives the same data as that transmitted originally by user “X”.
This is very important, because the automation of P2P and O2C processes requires documents in structured form and the possibility of converting them between standards. Introducing restrictions on these two basic rules would eliminate large part of the advantages and benefits of e-invoicing and the automation of accounting and financial procedures.

7- The authenticity of the origin and the integrity of an invoice must be verifiable, i.e. the system must be able to guarantee their “auditability”. Using software, tools and other IT procedures, it must be possible for the “verifier” (who may be an auditor, accountant, Tax Authority employee, etc.), to check that the guarantees have been satisfied.

It is thus necessary to ensure at least that:

a- auditability be “simple”, given that not all accountants and Tax Authority employees are IT experts;

b- auditability be “quick”, in “real-time” or “near real-time”, to enable many documents to be verified in a short time;

c- auditability produce the same “output” if run several times on a given e-invoice (input);

d- auditability produce an “output” which can be printed and transferred to other media (CD, DVD, etc.).

e- auditability produce an “output” in both the local language of the Member State and in English.

### 3. Qualified Electronic Signature (QES)

#### 3.1. Principal aspects of QES

One of the two “examples of technologies” proposed by the new article 233 of Directive 2006/112/EC is the Qualified Electronic Signature (QES), which is an Advanced Electronic Signature (AdES) based on a Qualified Certificate (QC) and created by a Secure Signature Creation Device (SSCD).

“(a) an advanced electronic signature within the meaning of point (2) of Article 2 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (*), based on a qualified certificate and created by a secure signature creation device, within the meaning of points (6) and (10) of Article 2 of Directive 1999/93/EC’’;


“Point 2: ‘advanced electronic signature’ means an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the
data is detectable”;

“Point 6: ‘secure-signature-creation device’ means a signature-creation device which meets the
requirements laid down in Annex III”;

“Point 10: ‘qualified certificate’ means a certificate which meets the requirements laid down in
Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in
Annex II”.

In relation to using QES in the e-invoicing process created using SSCD, a number of important
aspects of this technology should be considered, which may create criticalities, especially in cross-
border e-invoicing.

1- The addressee of the e-invoice, in order to be able to verify “the authenticity of the origin” and “
the integrity of the content”, must check and control the data and information contained in the
Qualified Certificate (QC).

According to Directive 1999/93/EC, “qualified certificate’ means a certificate which meets the
requirements laid down in Annex I and is provided by a certification-service-provider who fulfils
the requirements laid down in Annex II”, while according to Annex I of the same Directive
1999/93/EC, a QC must contain:

“(a) an indication that the certificate is issued as a qualified certificate;
(b) the identification of the certification-service-provider and the State in which it is established;
(c) the name of the signatory or a pseudonym, which shall be identified as such;
(d) provision for a specific attribute of the signatory to be included if relevant, depending on the
purpose for which the certificate is intended;
(e) signature-verification data which correspond to signature-creation data under the control of the
signatory;
(f) an indication of the beginning and end of the period of validity of the certificate;
(g) the identity code of the certificate;
(h) the advanced electronic signature of the certification-service-provider issuing it;
(i) limitations on the scope of use of the certificate, if applicable; and
(j) limits on the value of transactions for which the certificate can be used, if applicable”.

Given that numerous European and international standards have defined the profile and contents of
a QC, such as ETSI TS 102 280\textsuperscript{13}, ETSI TS 101 86\textsuperscript{14}, RFC 3739\textsuperscript{15}, RFC 3280\textsuperscript{16} (including its
updates RFC 4325\textsuperscript{17} and RFC 4630\textsuperscript{18}) and ITU-T X509\textsuperscript{19}, and since there is no single interpretation

\textsuperscript{13} ETSI TS 102 280, X.509 V3 Certificate Profile for Certificates Issued to Natural Persons
\textsuperscript{14} ETSI TS 101 862, Qualified Certificate Profile
\textsuperscript{15} RFC 3739, Internet X.509 Public Key Infrastructure: Qualified Certificate Profile
\textsuperscript{16} RFC 3280, Internet X.509 Public Key Infrastructure-Certificate and Certificate Revocation List (CRL) Profile
\textsuperscript{17} RFC 4325, Internet X.509 Public Key Infrastructure Authority Information-Access Certificate Revocation List (CRL)
Extension
\textsuperscript{18} RFC 4630, Update to Directory String Processing in the Internet X.509 Public Key Infrastructure-Certificate and
Certificate Revocation List (CRL) Profile

16
of the said standards and their contents, just as there is no clear and agreed guidelines for the use of these standards, a situation has arisen in which the various European CSP/QCs issue QCs with varying contents and information.

In other words, while the QCs issued by the various European CSP/QC conform to Annex I of Directive 1999/93/EC, they do not have the same content, and thus at the present time there is no perfect interoperability of QC auditablety, and the addressee of the e-invoice is unable to check, using “machine processable” solutions, the data and information contained in a given QC.

2- A second verification which the addressee of an e-invoice must run to ensure that the QES conforms to Directive 1999/93/EC, is to check that the SSCD employed by the issuer conforms to Annex III of Directive 1999/93/EC and hence to check whether this conformity is declared in the QC.

Although article 3.4 of Directive 1999/93/EC states that “The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States.(…)”, it should be noted both that numerous Member States have so far failed to designate the “bodies” charged with declaring, verifying and ascertaining the conformity of the SSCD to standard CWA 14169, and that there is no obligation to produce, publish or update any list of SSCDs conforming to standard CWA 14169.

It should be added that it would be advisable both to establish the requirements not only for the SSCD, but also for the “environment” in which the SSCD operates, and to draw up a new version of CWA 14169 (the most recent version of which goes back to 2004) which accounts for SSCDs other than smart-cards, such as USB Tokens, HSMs, etc..

3- Article 3 subsection 3 of Directive 1999/93/EC, states that “Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification service-providers which are established on its territory and issue qualified certificates to the public”, while recital 13 of the same states that “Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme”.

In effect, since Directive 1999/93/EC leaves completely open the question of what is meant by “appropriate system”, and gives no guidance on “how they ensure”, the individual Member States have inevitably produced divergent procedures, rules, methodologies and practices for supervising the CSP/QCs. It is clear that the absence in the EU of a “shared supervisory model” to be adopted by the various “Supervisory Bodies” of the Member States inevitably compromises the mutual

---

19 ITU-T X.509, Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks

20 The verification of the QC by the “verifier” can be done both manually (“human verification”) and automatically (“machine verification”).

21 The Annex to Commission Decision 2003/511/EU of 14 July 2003 states that:

"B. List of the generally recognised standards for electronic signature products that Member States shall presume are in compliance with the requirements laid down in Annex III to Directive 1999/93/EC
— CWA 14169 (March 2002): secure signature-creation devices”.

22 Point 15 of the recitals of Directive 1999/93/EC state that “Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate;(…)".
recognition (including legal) of QES and other services offered by the CSP/QCs, including Timestamping, REM, etc.

4- In order to verify whether a QES issued by a CSP/QC established in another member State conforms to Directive 1999/93/EC, the verifier must be able to access further information which is not included in the QC and which relates to the CSP/QC.

This further information regarding the CSP/QC is included in the so-called Trust Lists (TL) created pursuant to specific standards (ETSI TS 102 231 v.3 1.2\textsuperscript{23}), containing information such as: information about the TL itself (release number, information about the Member State Issuing Body, information regarding the supervisory scheme, date of issue, etc.), information about the CSP/QC (denomination, address (physical and electronic), etc.), information about the certification service provided by the CSP/QC (type and denomination of certification service, etc.), history and current situation of CSP/QC.

Article 2 subsection 1 of Commission Decision 2009/767/EC of 16 October 2009, states that “Each Member State shall establish, maintain and publish, in accordance with the technical specifications set out in the annex, a ‘trusted list’ containing the minimum information related to the certification service providers issuing qualified certificates to the public who are supervised/accredited by them”, while Commission Decision 2010/425/EU of 28 July 2010 sets out how the Member States are to establish, maintain and publish the TLs, providing that “Member States shall establish and publish both a human readable and a machine processable form of the trusted list in accordance with the specifications set out in the Annex”.

Thus, while in the EU, the trust lists make it possible with “machine processable” procedures to obtain further information not included in the QC but relevant to the CSP/QC and required to verify the QES itself, if e-invoices are received from Non-EU suppliers, the problem may well persist.

5- when using QES in e-invoicing, it is important not to confuse the guarantee of “integrity of the content”, with the guarantee of “immutability of the visual representation” - i.e. how the e-invoice is displayed to the verifier (or signer).

Indeed, if an e-invoice contains data which may render its visual representation dynamic (such as “macros”, “hidden codes”, ”active components”, etc.), while the integrity of the data may be unaltered (so that the QES is still valid), its representation on the screen may change.

For example, it is possible to transmit an e-invoice signed with QES, but which contains “macros” or “hidden codes” which, after 10 days, modify the total of the invoice, the supplier and the bank account to which payment is to be made.

This means that the employee who checks the invoice on the fifth day will find no discrepancy and authorise its payment, while his colleague, who is to pay it after 30 days and views it on his screen, will find that the “macros” or “hidden codes” make it display a total amount, supplier, and bank account which are different from before, although the file is the same and - and this is the crucial point - signed with a QES.

All of this can be avoided if the issuer adopts either of the following two simple solutions:

\textsuperscript{23} ETSI TS 102 231 v3.1.2 (2009-12) “Electronic Signatures and Infrastructures (ESI), Provision of harmonized Trust-service status information”.
a- using a “static and not modifiable” format, that is, a format which does not allow for macros and hidden codes, or which can deactivate them

b- implementing a procedure to check for macros and hidden codes and alert the operator, obviously before the QES is issued.

It is clear that if the issuer fails to adopt either of these two solutions, and this can be ascertained by checking the format or the agreement with the addressee, it is advisable that the addressee check for macros and hidden codes in the e-invoices he receives.

6- The creation of QES for e-invoices, as for any other document, can be achieved in two different ways:

a- by applying the principle that *What You See Is What You Sign*” (WYSIWYS), which means that the procedure only allows the signer to sign the document which is currently on-screen, and hence the signer signs the document only after having carefully checked it;

b- by applying the principle that “*What You Don’t See Is What You Sign*” (WYDSIWYS), which means that the signing procedure does not allow the signer to display the document he is signing at that time, since the signer simply launches the process to sign multiple documents, and hence his signature is applied in batch mode, i.e. automatically to a large number of documents.

In the case of e-invoicing, in which even millions of invoices may be issued annually, it is important to determine whether or not it is possible to apply the WYDSIWYS principle during the QES creation procedure. And if it is, to understand why.

To this end, one should recall two important factors:

a- Article 5 subsection 1 of Directive 1999/93/EC states that “Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

(b) are admissible as evidence in legal proceedings”.

It is well-known that, while in a paper world the declaration of a commitment (contract, agreement, will, etc.) is made by applying a handwritten signature (usually accompanied by the first and last names of the signer and the date and place of signature), in a digital world one can use QES, which attributes to the signed digital document the same probatory value as a paper document signed by hand.

b- Art. 233 of Directive 2006/112/EC, in permitting the use of QES as “examples of technologies”, indicates that the objective is to guarantee “The authenticity of the origin, the integrity of the content (...)

- “Authenticity of the origin” means the assurance of the identity of the supplier or the issuer of the invoice”.

---

24 An example of such a format is PDF/A per International Standard ISO 19005-1:2005
“Integrity of the content” means that the content required according to this Directive has not been altered”.

The QES, precisely due to its technical characteristics which enable it to guarantee authenticity and integrity, can thus be used not only as a replacement for the handwritten signature, but as a genuine “electronic seal” or “electronic stamp” which makes the content of the document unmodifiable. It thus has the same function as a “lead seal” on a package, or mediaeval sealing wax and seal.

In the context of electronic invoicing, QES is thus not used because it replaces the handwritten signature and thus makes the signatory responsible for the content of the signed document, but rather for the dual purpose of:

- guaranteeing the “Identity of the supplier or the issuer”, so that the identity of the signer is what enables the identity of the supplier (or issuer of the invoice) to be determined, which is the real guarantee required;

- guaranteeing the “Integrity of the content”, so that the identity of the signer identifies the person who has “crystallised” the content of the document, which has rendered it immutable which, once more, is the real guarantee requested.

For these reasons, then, in electronic invoicing processes:

a- the WYDSIWYS principle is considered admissible in the creation of QESs, so that invoices can be signed automatically or in batch mode;

b- the physical signatory, having used his own QES to sign the invoices, is not responsible for the content of the invoice he has signed.

In order to avoid inconvenient consequences of the fact that the signatory, in a batch or automatic signing process, may apply his QES also to other documents than electronic invoices, one may adopt certain simple precautions:

a- Annex I of Directive 1999/93/EC provides that a QC must contain “(i) limitations on the scope of use of the certificate, if applicable”, while document RFC3280, in relation to Extended Key Usage, states that “This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. In general, this extension will appear only in end entity certificates”.

In effect, when the QC is issued by the CSP/QC, it may be possible to enter the information necessary to render the QC (and hence the QES) valid for electronic invoices only (or other documents, such as Order Confirmations, Despatch Advices, etc.).

b- One can implement simple checks, for instance by checking that the number of QESs applied over a given period of time (e.g. a day) is equal to the number of invoices issued over the same period.

7- Annex I of Directive 1999/93/EC provides that a QC must contain “(f) an indication of the beginning and end of the period of validity of the certificate”, and in any case we must recall that a
QC may be revoked before the expiry of its validity because, for instance in case of loss or theft of the SSCD, the security of the private key has been compromised, or for other reasons.

The addressee of the electronic invoice, then, who must check that the QC was valid at the time of creation of the signature, and hence that it was neither revoked nor expired at that time, must be able to determine the exact time of creation of the QES, or the moment immediately succeeding it. This means associating a “time reference” with the QES to attest the exact time of its creation or the moment immediately succeeding it.

There are two types of time reference, applied at the time of creation of the QES or immediately thereafter:

a- a Time Stamp Token (TST) issued by a Time Stamping Authority (TSA), which is a “data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time” (ETSI TS 101 733 V1.8.3 (2011-01)).

As stated in paragraph 1 of document RFC 3161 “The TSA's role is to time-stamp a datum to establish evidence indicating that a datum existed before a particular time. This can then be used, for example, to verify that a digital signature was applied to a message before the corresponding certificate was revoked thus allowing a revoked public key certificate to be used for verifying signatures created prior to the time of revocation. This is an important public key infrastructure operation”;

b- a Time Mark (TM), in other words “Information in an audit trail from a Trusted Service Provider that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time” (ETSI TS 101 733 V1.8.3 (2011-01)).

For the issuer of an electronic invoice, the TST or TM can be applied to invoices signed with a QES in two distinct manners:

1- directly, by applying the TST or TM to each invoice issued;

2- indirectly, by applying the TST or TM to a file (called, for instance, “time reference”) which contains the hash values of a given number of invoices issued. The addressee must thus receive not only the invoices, but also the “time reference” file containing the hash values of the invoices issued, including those addressed to him. The addressee's ability to check that the hash value of his invoice matches the value in the “time reference” file, itself stamped with a TST or TM, guarantees that the QES was applied at a time before the TST or TM. The “time reference” file, in addition to the hash values for a certain number of invoices and the issuer information (no other data need be included), could also contain the means of generation of the TST or TM employed.

If the TST or TM is not applied to the electronic invoice or the “time reference” file containing the hash values for several invoices by the issuer, then it can be applied by the addressee. The validity of the QC is thus not checked for the time at which the QES was created (which is unknown), but with reference to the time at which the TST or TM was applied. It is clear that even a long time may have passed, and the QC check could thus fail to give correct results, since the QC may have expired or been revoked after the QES but before application of the TST or TM.
One final aspect linked to the above is due to the fact that some time passes between the time the QC is revoked and the time in which it is possible to ascertain its revocation by checking the CRL\textsuperscript{25}, (the “Grace period”), which means that the checker must wait before definitively ascertaining whether the QC was valid at the time of signing.

An addressee of an electronic invoice who wishes to check the validity of the QC at the time of signing, must not only know the duration of the Grace period (which is available in the company’s “Signature policy”, for instance), but must also postpone the check until the Grace period expires or run a second check thereafter.

![Figure 2. The grace period](source)

8- The increasing use of QES by businesses, both to replace handwritten with electronic signatures, and to use QES as an “electronic stamp” which can guarantee the authenticity and integrity of documents (e-ordering, e-invoicing, etc.), requires that companies establish and enforce a “Signature policy”.

According to the definitions of document ETSI TR 102 045 V1.1.1 (2003-03)\textsuperscript{26}, a “Signature policy” is : “a set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid”.

In effect, the “Signature policy” is a document (human readable and machine processable) containing the technical rules, conditions and procedures adopted by the company in creating valid

\textsuperscript{25} The Certificate Revocation Lists (CRL) are lists of revoked QCs (identified by the QC serial number) and their revocation dates, which are issued by the CSP/QC at given intervals of time: hourly, every 4 hours, every 8 hours, every day, every 3 days, weekly, etc..

\textsuperscript{26} ETSI TR 102 045 V1.1.1 (2003-03) Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model
electronic signatures (signature creation policy) and to enable their verification by the verifier (signature validation policy).

To take an example in relation to the use of QES in electronic invoicing, the “Signature policy” of the company issuing the invoices must indicate the signer's (or signers') identity, the rule used to enable the verifier to ascertain the date of signature (whether a TST or TM has been used), the grace period, etc.

In order to totally automate verification of the invoice by the addressee, it is best that the “signature policy” also be in a “machine processable” format.

At this time Directive 1999/93/EC does not consider signature policies, but given the increasing use of QES (as well as ES and AdES) and the inefficiencies caused by poor interoperability between the various Member States, it would certainly be useful, as well as promoting their use by businesses, to propose the adoption of a shared model of “Signature Policy”.

3.2. How QES works

To understand the basic principles of QES, without going too far into technical details which are not the concern of this document, we give below the main passages regarding the creation and verification of QES.

3.2.1. Hash functions

In the creation of QES, as in other processes in which the integrity of data is to be guaranteed (such as data transmission via EDI), one often makes use of hash functions. So, what are hash functions, especially one-way hash functions?

One-way hash functions are functions which, regardless of the size of the input (text, file, image, etc.), produce an output (hash value) of fixed length (160 bit, 256 bit, 384 bit, 512 bit, etc.).

In addition to the above, one-way hash functions have the following 3 characteristics:

a- “Pre-image resistance”: given the hash value (output), it is impossible to find the input;

b- “Second pre-image resistance”: given the hash value (output) of a known input, it is impossible to find a different input with the same hash value (output);

c- “Collision resistance”: two different inputs cannot have an identical hash value (output).

For example:

a- the hash value of the text Umberto Zanini calculated with the SHA-1\(^{27}\) algorithm (160 bit) and expressed in base 16, appears as: 431ab49fc92f2dbe1e59f62f071dd159fada9e1f

\(^{27}\) Secure Hash Algorithm 1 (SHA-1)
b- the hash value of the text **Umberto zanini** calculated with the SHA-1 algorithm (160 bit) and expressed in base 16, appears as: \texttt{c57e8f15fb0f3483a923462c02e9e5d5617c964d}

c- the hash value of the text **umberto zanini** calculated with the SHA-1 algorithm (160 bit) and expressed in base 16, appears as: \texttt{44a3473eebada2c6dfa18c39a37b59d23e8613ee}.

### 3.2.2. Creating the QES

Creating the QES for any document, for example an electronic invoice, involves the following steps:

1st step: The electronic invoice is subjected to a hash function (e.g. SHA-1) in order to calculate its hash value;

2nd step: The hash value is encrypted inside the SSCD, i.e. run through the signature algorithm (e.g. RSA\textsuperscript{28}), and a private key known only to the signer is used to create the QES;

3th step: After the QES has been created, it is associated with the invoice.

![Figure 3. QES creation process](image)

\textsuperscript{28} Rivest-Shamir-Adleman (RSA) is an asymmetric cryptography algorithm
The visual representation of a QES created with “sha1withRSA” (1024), and expressed in base 16 appears as:

```
0A60 E8F6 C799 6317 3677 C3A6 5606 2263 9717 38D7 AE8D 5F8A FA72 87F1 C235 4C7D B36A 7157 1611 6C19 1353 FE3B 8190 C046 8556 C5A9 5238 D5EA ECFC 5810 A3CF C904 47C1 E6D3 C4FE 618F 2594 513A 4EE8 05C8 0506 B53F AFCF 45C0 3726 0DA6 6014 B68D 9326 9355 D8B8 31FB 691F 0C78 CA37 7A4D CEB9 900E 0CF8 DE7E 19DB 566A B2DA E91F
```

### 3.2.3. Verifying the QES

Verifying the QES involves the following steps:

1st step: After having verified the authenticity of the QC, the QES is subjected to verification using the 2 same algorithms used to create it.

One uses the same signature algorithm (e.g. RSA) and public key contained in the QC to decrypt the QES, thus returning the original hash value;

2nd step: The electronic invoice is subjected to the same hash function (e.g. SHA-1) to calculate its hash value;

3th step: The two hash values are compared: that obtained by decrypting the QES and that calculated from the electronic invoice. If the two hash values agree, the check is passed.

![Figure 4. QES verification process](image-url)
3.3. Centralised use of HSM in a MNE or SP

As described above, the QES creation process involves two steps:

1st step: calculate the hash value of the invoice;

2nd step: encrypt the hash value with the signature algorithm (e.g. RSA) to obtain the QES.

While step 2 must always occur inside the SSCD (and hence the QES is created in the location in which the SSCD resides), step 1 can also be done outside the SSCD, for example in another country or continent.

This enables us to introduce a particular solution to optimise resources and investments in a multi-country electronic invoicing project by an MNE or SP.

To summarise:

1- Install just one Hardware Security Module\(^{29}\) (HSM) at the MNE's head offices;

2- Install in the HSM the QCs of the various signers who will sign the electronic invoices issued by the branch offices;

3- Create the invoices at the branch offices;

4- Create the hash values for the invoices at the branch offices;

5- Transmit the hash values to the MNE's head offices over a secure channel (as we have seen, if the hash value is intercepted, it is anyway impossible to reconstruct its input, i.e. the original invoice);

6- Create the QES in the HSM;

7- Securely transmit the QES to the branch, if necessary;

8- Electronically archive the electronic invoices (which have never left the branch office) and QES at the branch office itself, or archive the invoices at the branch and the QES at head offices.

\(^{29}\) The Hardware Security Module is a special type of SSCD which can contain a large number of QCs and create thousands of QES per second.
3.4. The Time-Stamp Token

As stated in the definitions of document ETSI TS 101 733 V1.8.3 (2011-01)\(^{30}\), a Time-Stamp Token (TST) is a “data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time”.

In contrast with the QES, which is generated inside the SSCD and thus requires no internet connection, an internet connection is required to generate a TST, since it is created TST by the Time Stamping Authority (TSA).

Furthermore, the TSA does not include any information in the TST which can identify the applicant, and hence the TST, although it guarantees the integrity of the document (it is a QES applied by the TSA), does not provide applicant identification.

Creating the TST involves the following steps:

1st step: The TST applicant creates the hash value of the document and transmits it to the TSA (the hash value alone, not the document itself);

---

\(^{30}\) ETSI TS 101 733 V1.8.3 (2011-01) “Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)”
2nd step: The TSA receives the hash value, adds the UTC time data 31 (YYYYMMDDhhmmss), and applies a QES, thus generating the TST;

3th step: The TSA sends the applicant the TST within a few seconds (the QES and the UTC time data).

Verifying the TST involves the following steps:

1st step: Using the public key contained in the QC, the QES generated by the TSA is decrypted and returns the original hash value;

2nd step: The hash value of the document is generated, to which the UTC time data is added (YYYYMMDDhhmmss), and the resulting hash value is recalculated;

3th step: The two hash values are compared: if they match, the check has been passed.

---

31 The Coordinated Universal Time (UTC) is an international time standard.
4. BCRATIS

4.1. Definitions

Article 233 subsection 1 of Directive 2006/112/EC states that:

“Each taxable person shall determine the way to ensure the authenticity of the origin, the integrity of the content and the legibility of the invoice. This may be achieved by any business controls which create a reliable audit trail between an invoice and a supply of goods or services”.

To understand what is meant by “Business Controls which create a Reliable Audit Trail between an Invoice and a Supply of goods or services” (BCRATIS), we must first define some terms, in particular “business controls” and “reliable audit trail”, and examine the linked matter of “electronic audit evidence”.

Figure 7. TST verification process
4.1.1. Business controls

As explained in the Explanatory notes, “Business control is a wide concept”, and the use of the term by the EU legislator is probably due to the desire not to specify a precise framework or methodology. In effect, just like the principle of “technological neutrality” adopted previously, in this case it was also preferable to use a "procedural neutrality" principle.

Businesses are thus left free to decide the types of business controls they wish to adopt, also, as explained in the Explanatory notes, in relation to the size of the business, its activity, type, number and value of transactions, and type of suppliers and customers, etc.

However, a framework which is of value in understanding the underlying principles of BCRATIS is the “Internal Control-Integrated Framework, Guidance on monitoring internal control systems” issued by COSO (The Committee of Sponsoring Organizations of the Treadway Commission)32:

As given in the document: “Internal control is a process, effected by an entity’s board of directors, managements and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
-Effectiveness and efficiency of operations,
-Reliability of financial reporting, and
-Compliance with applicable laws and regulations”

The 10 principal steps which usually compose an “Internal control” activity, regardless of the area subject to auditing (IT, accounting, finance, payroll, etc.), can be summarised as follows:

1\textsuperscript{st} - Understanding the environment
2\textsuperscript{nd} - Understanding the internal control effectiveness
3\textsuperscript{rd} - Understanding the risks
4\textsuperscript{th} - Prioritizing the risks
5\textsuperscript{th} - Identifying the key controls
6\textsuperscript{th} - Identifying the key information
7\textsuperscript{th} - Designing monitoring procedure
8\textsuperscript{th} - Implementing monitoring procedure
9\textsuperscript{th} - Evaluation of the internal control system
10\textsuperscript{th} - Assessment and audit report

---

32 COSO (The Committee of Sponsoring Organizations of the Treadway Commission), is an initiative which aims to “develop frameworks and guidance on enterprise risk management, internal control and fraud deterrence”. The initiative includes participants from: American Institute of Certified Public Accountants, American Accounting Associations, Financial Executives International, the Association of Accountants and Financial Professionals in Business, and the Institute of Internal Auditors.
4.1.2. The reliable audit trail

There are various definitions of “audit trail”, including:

- an audit trail is a “set of audit records each referable to a precise point in time and containing evidence pertaining to and resulting from the execution of a process or system function”33;

- an audit trail is “A chronological record of system activities that shows all additions, deletions and changes to both data and software. It enables the reconstruction, review and examination of a transaction from its inception to output and final results. The audit trail can be used to trace data from its input into the system to its output, or vice versa”34;

- an audit trail is “A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result”35;

- an audit trail is “A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source”36.

It should be added that the concept of audit trail is also present in accounting systems:

- “An audit trail that records the processing of an entry from source information or documents to final recording in ledgers (and vice versa)”, and “Production of audit trails to prove events and transaction values by recording the progress of individual entries from inception to final recording in the accounts (and reverse), together with amendments to standing data held in master files”37;

- “For example, the information maintained in an electronic storage system and the taxpayer’s books and records must be cross-referenced in a manner that provides an audit trail between the general ledger and the source”38.

An audit trail will thus be “reliable” when it is able to guarantee all 5 of the following conditions:

1- creating, registering and conserving all events, operations and activities, whereby activities means at least the following: create, change, delete, approval, and release;

2- associating with each event, operation or activity, “logs” to attest the exact time at which the event, operation or activity occurred, the operator or user who actuated it, the software used, any links to other documents or data, and so on.

According to the ISACA39, “logs” or “log files” mean “Files created specifically to record various actions occurring on the system to be monitored, such as failed login attempts, full disk drives and e-mail delivery failures”;

---

33 ETSI TS 101 533-1 V1.1.1 (2011-05) “Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management”
34 CICA-The Canadian Institute of Chartered Accountants, Electronic Audit Evidence, 2003
35 National Information Assurance (IA) Glossary, 2010
36 ISACA, Glossary of Terms, 2012
37 OECD, Guidance and Specifications for Tax Compliance of Business and Accounting Software, 2010
38 Internal Revenue Service (IRS), Revenue Procedure 97-22
39 ISACA, Glossary of Terms, 2012
3- enabling the reconstruction, review and examination, at any time, in a simple and highly precise manner, of any given past event, operation or activity;

4- enabling the reconstruction, review and examination, at any time, in a simple and highly precise manner, of all past events, operations and activities in chronological order, even backtracking;

5- guaranteeing the legibility and integrity of the data (events, operations, activities, logs, etc.), and prevent their modification or cancellation, whether it is voluntary or involuntary.

The figure shows an audit trail which enables the verifier to:

1- verify the sequence of events in chronological order (a1, a2, a3);
2- verify the sequence of events in backtracking chronological order (b1, b2, b3);
3- find individual events (c1, c2, c3, c4);

Figure 8. The reliable audit trail
4.1.3. The electronic audit evidence

The auditor’s opinion as submitted after auditing (and this also applies to BCRATIS), is supported by evidence identified and collected by the auditor, which is generally known as the “audit evidence”.

The “audit evidence”, as defined in the CICA Handbook – Assurance, “consists of the source documents and accounting records underlying the financial statements and all other information which is pertinent to the audit. The accounting records, of themselves, do not provide sufficient appropriate audit evidence”.

However, given that BCRATIS is run in a fully digital environment (although this might not be true in the case of paper invoices), a new concept must be introduced: that of “electronic audit evidence”.

As stated in the CICA Research report-Electronic Audit Evidence, “Electronic audit evidence is information created, transmitted, processed, recorded, and/or maintained electronically that supports the content of the audit report. Unless a printout is made, the information is only accessible through hardware and software systems that can run and read the data”.

The electronic audit evidence used by the auditor to support his auditor’s opinion may thus consist of data, electronic documents (XML, PDF, etc), electronic messages (e-mail, REM, etc), logs, etc., and the "audit trail” itself is a type of electronic audit evidence, indeed, the most important and relevant type.

The electronic audit evidence employed by the auditor in supporting his auditor’s opinion must be “reliable”, and to this end we consider at least 5 important principles:

1- The electronic audit evidence collected by the auditor is the most reliable;

2- The electronic audit evidence obtained from a source external to the company is more reliable than that obtained from the company itself;

3- Documented electronic audit evidence is more reliable than verbal evidence (for example, that resulting from recorded interviews);

4- The electronic audit evidence obtained from documents originated digitally is more reliable than that obtained from scans of paper documents;

5- The electronic audit evidence obtained from electronic documents which attest the date of their creation (using TST/TM) is more reliable than that obtained from documents which cannot do so.
4.2. What BCRATIS is

We might define a BCRATIS as an “internal control capable of verifying and “providing reasonable assurance” that, for each invoice issued and received, goods and services have been supplied”.

Before examining the steps involved in implementing a BCRATIS, we must consider the following important aspects:

1- article 233 of the Directive 2006/112/EC states that “This may be achieved by any business controls which create a reliable audit trail between an invoice and a supply of goods or services”. A BCRATIS does not, therefore, include the payment of an invoice because, since the payment is made after issue/reception of the invoice, it is of no value in determining the authenticity and integrity of the invoice itself. This is not totally true, however, since, as we will see below, some of the information contained in an invoice may only be verified in relation to its actual use, for instance, of the remittance advice,

2- as given in the Explanatory notes: “The business controls should be appropriate to the size, activity and type of taxable person and should take account of the number and value of transactions as well as the number and type of suppliers and customers. Where relevant other factors should also be taken into consideration”.

In effect, there cannot be a single model of BCRATIS, since there are various types of internal control, audit trail, etc., and the choice of BCRATIS will depend on a variety of factors, such as the size of the business, its activity, type, number and value of transactions, the type of suppliers and customers, type of Information System, Member State in which it resides, format of invoice (structured/unstructured), and so on.

We should add that it will always be possible for a given company to employ a variety of models of BCRATIS, for example, one for sales and one for purchase invoices.

---

40 According to the Trust Services Principles and Criteria, drawn up by AICPA/CICA, “A system consists of five key components organized to achieve a specified objective. The five components are categorized as follows:
(a) infrastructure (facilities, equipment, and networks),
(b) software (systems, applications, and utilities),
(c) people (developers, operators, users, and managers),
(d) procedures (automated and manual), and
(e) data (transaction streams, files, databases, and tables)”. 

34
4.3. How to implement a BCRATIS

4.3.1. The fundamental principles

As indicated above, since various models of BCRATIS may be adopted, we will concentrate on the model that is most likely to be adopted, i.e. that of “Matching supporting documents and Application Controls”.

This model starts from a number of simple considerations which arise whenever a business sells or buys goods and services, whether in a paper or digital environment, as follows:

1- the transfer of goods or provision of a service requires both parties to exchange a certain number of documents, depending on the type of company, industry, size, etc., of which the invoice is only one.

The following image shows an example of the documents exchanged between a supplier and buyer in relation to the transfer of goods.

![Diagram of documents exchanged]

Figure 9. Documents exchanged

2- Each document exchanged, whether paper or electronic, has its life cycle, composed of a beginning and an end, and many intermediate steps which vary in relation to the type of document in question.
3- Each party applies numerous actions to the individual documents they exchange: create, change, delete, approve, release, issue, etc.

This introduces the importance of making sure, for example, that the ERPs do not present criticalities in data input or document creation, or failures in the “segregation of duties”, so that a user may change without authorisation an invoice which has already been issued, or approve a Purchase Order.

Thus, if specific controls are not enforced on the various “applications” used in the P2P/O2C cycle, the authenticity and integrity of the documents exchanged between the parties may be compromised.

This means adopting “Application Controls”, where, as defined by The Institute of Internal Auditors, “Application controls are those controls that pertain to the scope of individual business processes or application systems, including data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting”.

---

41 According to the The Institute of Internal Auditors, Auditing Application Controls, 2007, “An application or application system is a type of software that enables users to perform tasks by employing a computer’s capabilities directly”.

42 The Institute of Internal Auditors, Auditing Application Controls, 2007
4- The totality of documents exchanged, logs created to register actions taken with documents, the audit trail, etc., constitute the set of data which enables the auditor to identify the electronic audit evidence to be employed in supporting his auditor’s opinion.

5- BCRATIS can assure “the authenticity of the origin”, since, if we take a purchase invoice as an example, it can control the supplier data throughout the P2I cycle:

a- the supplier details given in the purchase invoice match those of the ERP entered after stipulation of the contract governing the purchase of the goods;
b- the supplier details given in the purchase invoice match those in the Purchase Order issued by the company;
c- the supplier details given in the purchase invoice match those in the Order Confirmation issued by the supplier;
d- the supplier details given in the purchase invoice match those in the Despatch Advice issued by the supplier;
e- the supplier details given in the purchase invoice match those in the Receipt Advice issued by the company.

6- BCRATIS can assure “the integrity of the content”, since, continuing to take a purchase invoice as an example, it can control the data contained in the documents exchanged with the supplier throughout the P2I cycle:

a- some of the data contained in the purchase invoice match those of the ERP entered after stipulation of the contract governing the purchase of the goods;
b- some of the data contained in the purchase invoice match those in the Purchase Order issued by the company;
c- some of the data contained in the purchase invoice match those in the Order Confirmation issued by the supplier;
d- some of the data contained in the purchase invoice match those in the Despatch Advice issued by the supplier;
e- some of the data contained in the purchase invoice match those in the Receipt Advice issued by the company.

4.3.2. Methodology

Solely in order to enable us to understand what a BCRATIS is actually composed of, this paragraph considers a sample methodology.

There are 5 main steps:

1st step: Definition of the matches between the documents exchanged

2nd step: Filling out the “Matching matrix”
3th step: Filling out the “Risk and control matrix”

4th step: Compilation of the “Control Activities Flowchart”

5th step: Compilation of the “BCRATIS Policy”

It is important to note the connection with the two matrices, in particular:

a- The matches between the various documents exchanged are given in the “Matching matrix”; 

b- The control activities contained in the “Risk and control matrix” are given in the “Control Activities Flowchart”.

The production, updating and display of the above documents may be done with software, tools, and so on, to simplify, speed up and automate the procedure.

**1st step:**

**Definition of the matches between the documents exchanged**

The first thing to be done is to list the documents to be exchanged, determine which of them are to be used for the BCRATIS, and list the data contained in these documents and in the invoice. We must then establish the “matches” between the invoice data and that of the various documents employed, to ensure the authenticity of the supplier and the integrity of the data contained in the invoice.

We must attribute a number to each “match”, so as to be able to link this activity to the “Matching matrix”.

We consider the case of the P2I cycle as an example, with reference to the “matches” between the invoice and the Despatch Advice and Remittance Advice.
### Content of Despatch Advices (CWA 15672)
- Despatch advice number
- Despatch advice issue date
- Supplier
- Customer
- Carrier
- Gross weight consignment
- Net weight consignment
- Goods value
- Number of pieces
- Number of packages
- Total invoice amount
- Final despatch
- Country of destination
- …etc…

### Content of invoices
(Article 226 – Directive 2006/112/EC)
- The date of issue
- A sequential number, based on one or more series, which uniquely identifies the invoice
- The VAT identification number referred to in Article 214 under which the taxable person supplied the goods or services
- The customer's VAT identification number
- The full name and address of the supplier
- The full name and address of the customer
- The quantity and nature of the goods supplied
- The extent and nature of the services rendered
- The date on which the supply of goods or services was made or completed
- The taxable amount per rate or exemption, the unit price exclusive of VAT and any discounts or rebates if they are not included in the unit price
- The VAT rate applied
- The VAT amount payable
- In the case of an exemption or where the customer is liable for payment of VAT, reference to the applicable provision of this Directive, or to the corresponding national provision

### Content of Remittance Advices (CWA 15670)
- Remittance advice number
- Remittance advice issue date
- Invoice issue date
- Invoice number
- Payer
- Payee
- Payment date
- Payment currency
- Payment order number
- Total amount remitted
- Payer financial institution
- Payee financial institution
- …etc…

Figure 11. Definition of the Matches between the documents
2nd step:

Filling out the “Matching matrix”

After defining the “matches”, we must compile a matrix containing the main information about the actions to be taken.

The “Matching matrix” must include at least the following information:

1- “No.”: the “Match number”, a progressive alphanumerical code identifying the match: M1, M2, M3, etc;

2- “Content of invoices”: the data contained in the invoice;

3- “Objective”: indicates whether the matching is used to guarantee the authenticity of the supplier, the integrity of the data or the legibility of the invoice;

4- “Document”: indicates with which document the match is done;

5- “Type of Matching”: the various types of matching, for example Manual (M), Automated (A), Both (B), or Semiautomatic (S);

6- “Controller”: the person responsible for the matching;

7- “Frequency of Matching Activity”: the frequency with which the matching is done: continuous, hourly, daily, weekly, monthly, etc.;

8- “Output”: the outcome of the matching: documents, logs, etc.

We continue to consider the previous example of the P2I cycle, with reference to the “matching matrix” between the invoice and the Despatch Advice and Remittance Advice.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>M6</td>
<td>The date of issue</td>
<td>Integrity of the content</td>
<td>Matching with Remittance Advice</td>
<td>A</td>
<td>Mrs Red</td>
<td>Daily</td>
<td>Logs</td>
</tr>
<tr>
<td>M7</td>
<td>A sequential number, based on one or more series, which uniquely identifies the invoice</td>
<td>Integrity of the content</td>
<td>Matching with Remittance Advice</td>
<td>A</td>
<td>Mrs Red</td>
<td>Daily</td>
<td>Logs</td>
</tr>
<tr>
<td>M1</td>
<td>The VAT identification number referred to in Article 214 under which the taxable person supplied the goods or services</td>
<td>Authenticity of the origin</td>
<td>Matching with Despatch Advice</td>
<td>A</td>
<td>Mr White</td>
<td>Daily</td>
<td>Logs</td>
</tr>
<tr>
<td>M2</td>
<td>The customer's VAT identification number</td>
<td>Authenticity of the origin</td>
<td>Matching with Despatch Advice</td>
<td>A</td>
<td>Mr White</td>
<td>Daily</td>
<td>Logs</td>
</tr>
<tr>
<td>M3</td>
<td>The full name and address of the supplier</td>
<td>Authenticity of the origin</td>
<td>Matching with Despatch Advice</td>
<td>A</td>
<td>Mr White</td>
<td>Daily</td>
<td>Logs</td>
</tr>
<tr>
<td>M9</td>
<td>The full name and address of the supplier</td>
<td>Authenticity of the origin</td>
<td>Matching with Remittance Advice</td>
<td>A</td>
<td>Mrs Red</td>
<td>Daily</td>
<td>Logs</td>
</tr>
<tr>
<td>M4</td>
<td>The full name and address of the customer</td>
<td>Authenticity of the origin</td>
<td>Matching with Despatch Advice</td>
<td>A</td>
<td>Mr White</td>
<td>Daily</td>
<td>Logs</td>
</tr>
<tr>
<td>M8</td>
<td>The full name and address of the customer</td>
<td>Authenticity of the origin</td>
<td>Matching with Remittance Advice</td>
<td>A</td>
<td>Mrs Red</td>
<td>Daily</td>
<td>Logs</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Figure 12. Matching matrix
3rd step

Filling out the “Risk and control matrix”

The company's “IT Policy” (or equivalent document) states which controls are to be applied to the P2I/O2I processes, in order to mitigate the risks associated with the use of IT (e.g. controls on “segregation of duties”, access controls, data entry controls, etc.).

One then compiles the “Risk and control matrix”\textsuperscript{43}\textsuperscript{44}, which details the “Control Objectives”, “Risks”, and “Control Activities” in relation to the entire P2I/O2I cycle.

The matrix must include at least the following information:

1- “No.”: the “Control Number”, a progressive alphanumeric code which is later entered into the “Control Activities Flowchart”.
   It is advisable to use a “Control Number” which refers to the type of document, for example for Purchase Orders one might use PO1, PO2, PO3, etc., for invoices I1, I2, I3, etc.

2-“Document”: the type of document to which the control refers;

3-“Control Objectives”: the objectives the control activity is to assure;

4-“Risks”: the risks the control activity is to eliminate or mitigate;

5-“Risk Rating”: the level of risk, scored from 1 to 5 (1= minimum, 5= maximum), or using the letters H (High), M (Medium), L (Low);

6-“Control Activities”: describes the Control Activities employed;

7- “Type of control”: the various types of control, for example Manual (M), Automated (A), Both (B), or Semiautomatic (S);

8- “Controller”: the person responsible for the controls;

9- “Frequency of Control Activity”: the frequency with which the controls are run: continuous, hourly, daily, weekly, monthly, etc.;

10- “Output”: the outcome of the controls: documents, logs, etc.

Below, as an example, is a matrix compiled by the buyer regarding the Purchase Orders process, containing certain “Control Objectives” and “Control Activities”.

Note that over the entire P2P or O2C cycle one may implement hundreds of Control Activities.

\textsuperscript{43} The Institute of Internal auditors, \textit{Auditing Application Controls}, Florida, 2007

\textsuperscript{44} IT Governance Institute, \textit{IT Control Objectives for Sarbanes-Oxley}, 2006
<table>
<thead>
<tr>
<th>No.</th>
<th>Document</th>
<th>Control Objectives</th>
<th>Risks</th>
<th>Risk Rating</th>
<th>Control Activities</th>
<th>Type of control</th>
<th>Controller</th>
<th>Frequency of Control Activity</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO1</td>
<td>Purchase Orders are created by authorized personnel</td>
<td>Unauthorised persons may create, change or cancel a Purchase Order</td>
<td>M</td>
<td>The controls do not allow access to unauthorised persons</td>
<td>A</td>
<td>Logs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO2</td>
<td>Purchase Orders are changed by authorized personnel</td>
<td>A Purchase Order may be issued without an approved requisition</td>
<td>H</td>
<td>The controls do not permit the issue of a Purchase Order without an approved requisition</td>
<td>A</td>
<td>Logs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO3</td>
<td>Purchase Orders are cancelled by authorized personnel</td>
<td>A Purchase Order may be issued and not processed</td>
<td>M</td>
<td>The controls do not permit the issue of a Purchase Order without its being processed</td>
<td>M</td>
<td>Logs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO4</td>
<td>Purchase Orders are placed only for approved requisitions</td>
<td>A Purchase Order may be issued without an approved requisition</td>
<td>H</td>
<td>The controls do not permit the issue of a Purchase Order without an approved requisition</td>
<td>A</td>
<td>Daily</td>
<td>Logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO5</td>
<td>All Purchase Orders issued are processed</td>
<td>A Purchase Order may be issued and not processed</td>
<td>M</td>
<td>The controls do not permit the issue of a Purchase Order without its being processed</td>
<td>M</td>
<td>Daily</td>
<td>Logs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 13. Risk and control matrix
4th step

The Control Activities Flowchart

In order to determine at which point of the process the “Control Activities” are to be run, one must draw up a flowchart of the entire P2I/O2I process, specifying the respective “Control Number”.

It may be of value to support the flowchart with a detailed description of the P2I/O2I cycle.

As an example, we give a flowchart of the order cycle per standard UBL 2.0\footnote{OASIS-Universal Business Language v2.0, 2006}, specifying some of the “Control Activities” run by the buyer (PO1, PO2, PO3, PO4, PO5).
Figure 14. The Control Activities Flowchart
5th step

The BCRATIS Policy

The BCRATIS policy is a document which describes the rules and procedures adopted by the company to guarantee "the authenticity of the origin, the integrity of the content and the legibility" of invoices.

The BCRATIS policy must include at least:

a- Modification history
b- Definitions
c- Legislation
d- Objectives
e- Roles and responsibilities
f- Rules and procedures
g- Components of BCRATIS
h- Matches between documents exchanged
i- The matching matrix
j- The risk and control matrix
k- The control activities flowchart
l- Appendix
4.4. The BCRATIS run with Continuous Auditing

4.4.1. What Continuous Auditing is

Once a company has implemented BCRATIS to guarantee the authenticity of its suppliers and integrity of the data contained in invoices, it must be audited periodically, and the auditor will then produce an audit report containing his auditor’s opinion.

The activity of auditing and compilation of the audit report, if done carefully and thoroughly, using traditional methods (potentially with the support of CAATs), requires a great deal of time and lengthy analysis.

In recent years, the increasing use of structured and processable data (e.g. XML), along with the increasing requirement from management for continuously updated reporting in support of their decisions, has led to the definition of this type of environment as a “Real-Time-Economy46.”

In the “Real-Time Economy”, the “Real-Time Enterprises” exchange only structured and processable electronic documents (XML), P2P and O2C processes are completely automated and integrated, and accounting is totally automated (“Real-Time Accounting”), etc.

It is clear that auditing itself has been forced to evolve, indeed it is not possible to employ traditional auditing methods in an environment which requires “Real-Time” reporting. A “Real-Time-Economy” composed of “Real-Time Enterprises” necessarily requires “Real-Time Auditing”.

In response to this requirement, Continuous Auditing (CA) applications have emerged in recent years, as stated by the AICPA 47 “A continuous audit is a methodology that enables independent auditors to provide written assurance on a subject matter, for which an entity’s management is responsible, using a series of auditor’s reports issued virtually simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter”.

CA provides numerous advantages, including:

- faster auditing with “real-time” (or “Near real-time”) discovery of errors, mistakes, fraud, malfunctions, omissions, suspicious activities, etc.;
- reduced time and expense required for auditing;
- more efficient error controls and reduction;
- accuracy and reliability in the generation of electronic audit evidence.

The main characteristics of Continuous Auditing can be summarised as follows:

1- Auditing is “continuous”, since it is run over all “events” (100% of events), simultaneously with (“real-time”) or immediately after (“Near real-time”) the event in question.

46 The Economist, The real time economy, January 2002
47 CICA/AICPA, Research Study on Continuous Auditing, 1999
However, CA is not always in real-time or near real-time, and often, in order not to overload the Information System, a periodic analysis system is opted for (e.g. daily, every two days, etc.);

2- Auditing is centred on discovering events (“exceptions”), which deviate from the parameters of the “Continuous Audit rules” and which may conceal errors, mistakes, fraud, malfunctions, omissions, etc.

If, for example, the Continuous Audit Rules state that all Purchase Orders greater than €100,000.00 must be approved by both users “X” and “Y”, the issue of a Purchase Order for €101,000.00 approved solely by user “X” constitutes an exception.

The definition and “prioritization” of exceptions is of great importance, since it is the exceptions that generate the alarms, determine the auditor's opinion, and interact with the Risk Assessment form;

3- The discovery of an exception generates a series of alarms and alerts which are communicated according to fixed rules, the so-called “notification rules” which are part of the Continuous Audit Rules.

The notification rules must be able to report the results of the Continuous Auditing effectively and efficiently, so that one must define the various types of alarms according to the risk rating of the exceptions, and specify to whom alarms are to be reported without thereby inundating them with insignificant reports, along with how to periodically update management on the progress of CA, etc.;

4- The Continuous Auditing is based on the principle that the auditor’s opinion is determined by the exceptions: the so-called “auditing by exceptions”.

The auditor’s opinion is a permanent opinion (or “evergreen opinion”), since it is always valid until exceptions occur which, due to their severity or number, mean that the auditor’s opinion may no longer be considered valid.

The rules which determine changes in or the expiry of the auditor’s opinion are also contained in the Continuous Audit Rules;

While, in traditional auditing, a certain amount of time is required to reach the auditor’s opinion, so that fraud may be committed multiple times, in CA the fraud is discovered in real-time and consequently the auditor’s opinion is modified in real-time.

5- Since the company operates in a continuously changing environment, due both to external and internal factors, it is important that there be continuous risk monitoring and assessment, with a continuous interaction with the Continuous Audit rules which govern the CA.

In order to be efficient and effective, CA must have dynamic Continuous Audit rules, which are continuously evolving and able to adapt to changes in the company's operating environment. Hence the parameters may change, the frequency of CA may change, the prioritization of the exceptions may be revised, etc.,

6- If the adopted frequency is real-time, the audit report and auditor’s opinion are also real-time, since they refer to CA of events which have only just occurred;
7- The audit report and auditor’s opinion may be on-line, and hence immediately available to users for reference;

8- The CA software, to do its job, must process the data from the ERP (or other systems), and hence must be able to interact directly with the ERP database (Embedded Audit Module), use data stored in other databases updated in real time or periodically (Monitoring Control Layer), or a combination of both.

The CA activity, may not only be run by Internal Auditors, but also by External Auditors, or by a specialised company which offers full outsourcing on-line CA services.

9- The CA software used by the auditors employs dashboards and graphs which allow the CA to be compared with previous years, and to view the progress of the CA activity, of exceptions, alarms and reconstruct activities run at any time in the past, etc..

### 4.4.2. CARATIS

Like nearly all internal controls, BCRATIS may also be implemented with a Continuous Auditing procedure, and hence “the authenticity of the origin, the integrity of the content and the legibility of the invoice” may be achieved by Continuous Auditing “which create a Reliable Audit Trail between an Invoice and a Supply of goods or services” (CARATIS).

We might define a CARATIS as “Continuous auditing capable of verifying and “providing assurance” that, for each invoice issued and received, goods and services have been supplied”.

It is clear that our remarks on Continuous Auditing also apply to CARATIS, since CARATIS is simply a special type of Continuous Auditing.

However we must emphasise some special aspects of CARATIS:

1- Using CARATIS gives all the advantages and benefits of Continuous Auditing, for example reductions in time and expense of auditing, more effective error checking and reduction, accuracy and reliability in generating the electronic audit evidence, real-time (or near real-time) discovery of errors, mistakes, fraud, malfunctions, omissions, etc.

2- The use of CARATIS guarantees the authenticity and integrity, in real-time (or near real-time), not only of received and issued invoices, but of the entire P2P/O2C cycle.

CARATIS may thus be a strategic choice for companies adopting or intending to adopt a Supply Chain Finance solution, since it provides greater control and more thorough verification of the entire process, and thus both greater success in SCF, and potentially lower cost of the service itself. The bank itself may be enabled to consult the auditor’s opinion on-line, and thus verify in real-time (or near real-time) the authenticity and integrity of the entire P2P/O2C cycle.

The Tax Authorities themselves may benefit from CARATIS, since they need only check the auditor’s opinion (or verify it with reference to a given period of a previous year), to make sure that
"the authenticity of the origin, the integrity of the content and the legibility” not only of a given invoice, but of all invoices issued/received up to that time has been guaranteed.

3- At this time there is no Guidance or Best Practices describing the characteristics of a CARATIS or how to implement it, and this certainly does nothing to promote its adoption.

Given that there are several international Software Houses specialised in the production of CA software, especially following the publication of the “Sarbanes-Oxley Act of 2002”, and since CARATIS is a new matter and opportunity, one would have to adapt existing software to the new requirements.

4- For the entire duration of the period of storage of the invoices, one must also keep the electronic audit evidence, exceptions, alarms, the audit trail, and so on, guarantee their integrity throughout the period and make sure that no data or documents are changed, cancelled or replaced.

Note that many electronic audit evidences must be kept, regardless whether CARATIS is employed, including exchanged documents such as Purchase Orders, Order Confirmations, Despatch Advices, etc.

5- The audit report may be made public, for example by being published on the corporate website so that anyone can consult the auditor’s opinion, as is done for SysTrust and WebTrust.

The information contained in the audit report may then be made available per type of stakeholder, as follows:

- anyone can consult the auditor’s opinion;
- only suppliers and buyers may consult the CARATIS policy;
- only banks may consult the CARATIS policy and the exceptions;
- only the Tax Authority may consult all documents.

The operation of a CARATIS can be briefly summarised in the following 10 steps:

1st: Extraction of P2P/O2C cycle data and documents from the ERP (or other system) and conversion, if necessary, and storage in a format processable by the “Analyzer”;

2nd: Analysis of the data and documents per the CARATIS rules (the CARATIS rules include the Matching matrix and Risk and control matrix);

3rd: Discovery of exceptions;

4th: Reporting of alarms to auditors, and periodic reporting to management;

5th: Continuous risk assessment;

6th: Continuous updating of the CARATIS rules;

7th: Collection of electronic audit evidence;
8th: Storage of electronic audit evidence, exceptions, alarms, the audit trail, etc.;

9th: Monitoring of the CARATIS by the auditors, using the dashboard;

10th: On-line verification of the Auditor’s CARATIS report by the users and other stakeholders.

Figure 15. Overview of the operation of a CARATIS
The authenticity of the origin, the integrity of the content and the legibility of the electronic invoices, are ensured by Continuous Auditing, which creates a Reliable Audit Trail between an Invoice and a Supply of goods or services (CARATIS)

Continuous Auditing has been done in accordance with the “CARATIS Policy” and auditing standards generally accepted in UK and Europe, and on examining the events reported up to 21st August 2012 at 13.00.27, NO exceptions have been encountered.

In our opinion, up to 21st August 2012 at 13.00.27, the CARATIS provided assurance that the authenticity of the origin, the integrity of the content and the legibility of the electronic invoices had been correctly ensured.

The CARATIS policy is available at http://www.XYZ.com/CARATIS/policy

The exceptions are available at http://www.XYZ.com/CARATIS/exceptions

The Audit Trail is available at http://www.XYZ.com/CARATIS/audit-trail

The dashboard is available at http://www.XYZ.com/CARATIS/dashboard
5. Conclusions

1- The individual Member States must adopt the new Art.233 of Directive 2006/112/EC without modifying or changing it, otherwise the factors which have so far slowed down or prohibited the adoption of electronic invoicing will persist.

Uniform adoption by the various Member States would also reduce (if not eliminate) the current legislative diversity between them, and create within the European Union a single large market, with more competition between SPs and hence better priced services for business.

In effect, it is necessary that electronic invoicing become a “commodity”, given that it is a powerful “key enabler” in at least three ways:

a- in enabling the introduction, in Purchase-to-Pay and Order-to-Cash processes, of eSupply Chain Finance and Financial Collaboration Systems;

b- in enabling the adoption of effective solutions for monitoring taxpayers and reducing VAT evasion48;

c- in enabling constant monitoring of public spending, if made obligatory for suppliers of goods and services to public authorities.

2- The guarantees of authenticity, integrity and legibility of invoices issued and received must be ensured in reference to both paper and electronic invoices (principle of parity between paper and electronic documents), and the method proposed in Art.233 of Directive 2006/112/EC for both formats is that of adopting “any business controls which create a reliable audit trail between an invoice and a supply of goods or services”.

With regard to both paper and electronic invoices, then, one can adopt BCRATIS, or CARATIS if one intends to employ Continuous Auditing.

With reference to electronic invoices alone, QES and EDI are only “examples of technologies” (principle of technological neutrality), since other suitable technologies are available, including REM, SSL, etc..

3- QES guarantees the authenticity and integrity to a very high level of certainty, but as we have seen, still has a number of criticalities, especially in relation to cross-border electronic invoices. Although some of these criticalities have been resolved by the solutions proposed by the some SPs, one must recall that the European Commission, specifically to eliminate the said criticalities, is soon to publish a "revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems"49.

49 European Commission, A digital Agenda for Europe, COM (2010) 245
4- To this date, there is no Guidance or Best Practices agreed by the Member States able to support and direct businesses in implementing a valid BCRATIS, or a valid CARATIS if one intends to employ Continuous Auditing.

This is a factor of considerable importance, but I believe it can be overcome once the benefits and advantages of CARATIS are demonstrated.

Any future Guidance should:

a- be approved or at least verified by the Tax Authorities of the Member States;

b- not only outline the guiding principles, but also give practical examples, at least regarding the size of the businesses (MNE, SME) and types of activity (goods, services);

c- give information to aid in adopting Continuous Auditing (CARATIS);

d- account for the new eSCF services, increasingly used by companies.

5- QES can guarantee the authenticity and integrity of a single document (or datum) for which it is created. Adopting only QES without providing specific controls along the P2P/O2C cycle thus signifies guaranteeing the authenticity and integrity of a single document (however important), while leaving the remaining documents in the P2P/O2C cycle without any such guarantee, thus leaving the door open to errors, fraud, double payment, failure to get paid, etc. BCRATIS, on the other hand, guarantees the authenticity and integrity not only of the invoices exchanged, but of the entire P2P/O2C cycle, and if one adopts CARATIS these guarantees are ensured in real-time (or near real-time). By simply referring to the auditor’s opinion, one can verify that the said guarantees have been extended not only to a single invoice, but to the entire P2P/O2C cycle and thus to all invoices and other documents exchanged.

For companies that have adopted, or that intend to adopt, Supply Chain Finance solutions, this is an important consideration, since the most innovative solutions often use other documents than merely invoices, so that the authenticity and integrity of the entire P2P/O2C cycle must be guaranteed.

6- QES is very simple to implement in electronic invoicing processes, and while a certain amount of training is required during start up, its everyday use requires no special qualifications or dedicated staff.

BCRATIS and CARATIS are different, inasmuch as their implementation may require more extensive support and their everyday use may require specialised staff.

Note however, that CARATIS, not only guarantees “the authenticity of the origin” and “the integrity of the content” of the invoices, but yields further benefits and advantages, such as greater effectiveness in the checking and reduction of errors, real-time (or near real-time) discovery of errors, mistakes, fraud, malfunctions, omissions, and so on.
7- The pros and cons of one solution compared to another have been reviewed above, at least in part, but the comparison will be more detailed and structured when we start to consider other methods and technologies.

The freedom of the taxable person to decide which method to use means, first and foremost, “awareness”, and hence a good understanding of what an electronic invoice is, which methods may be used, their pros and cons, which is best suited to the business in question, what impacts and implications they have, and so on.

The research and analysis, during the planning stage, is thus greater than it has been in the past, and this is perhaps the real novelty - the fact that businesses must make a greater investment in understanding what is really meant by the term "electronic invoice".
Documents


CEN-European Committee for Standardisation, *CWA 16461, Electronic invoice processes in Europe and enablement of SMEs to use them efficiently*, May 2012


CICA-The Canadian Institute of Chartered Accountants, *Electronic Audit Evidence*, 2003


CROBIES, *Study on Cross-Border interoperability of eSignatures*, 2010

ETSI TS 101 533-1 V1.1.1 (2011-05), *Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management*

ETSI TS 101 733 V1.8.3 (2011-01), *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAoES)*

ETSI TS 101 862 *Qualified Certificate Profile*

ETSI TR 102 045 V1.1.1 (2003-03), *Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model*

ETSI TS 102 231 v3.1.2 (2009-12), *Electronic Signatures and Infrastructures (ESI), Provision of harmonized Trust-service status information*

ETSI TS 102 280, *X.509 V3 Certificate Profile for Certificates Issued to Natural Persons*
IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley*, 2006

ISACA, *Glossary of Terms*, 2012

ITU-T X.509, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*


OASIS, *Universal Business Language v2.0*, 2006


OECD, *Guidance and Specifications for Tax Compliance of Business and Accounting Software*, 2010

Polytechnic of Milan, *Observatory on Electronic Invoicing and Dematerialisation*, *Electronic Invoicing as a “keystone” in the collaboration between companies, banks, and PA*, 2008

Polytechnic of Milan, *Observatory on Electronic Invoicing and Dematerialisation*, *Joint collaboration: a powerful driver for electronic invoicing in Italy*, 2009

Polytechnic of Milan, *Observatory on Electronic Invoicing and Dematerialisation*, *Electronic invoicing in Italy: reporting from the field*, 2010

Polytechnic of Milan, *Observatory on Electronic Invoicing and Dematerialisation*, *Beyond the invoice*, 2011

RFC 3739, *Internet X.509 Public Key Infrastructure: Qualified Certificate Profile*


RFC 4325, *Internet X.509 Public Key Infrastructure Authority Information-Access Certificate Revocation List (CRL) Extension*


The Economist, *The real time economy*, January 2002

The Institute of Internal auditors, *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*, GTAG # 3, Florida, 2005

The Institute of Internal auditors, *Auditing Application Controls*, Florida, 2007

Reckon LLP, *Study to quantify and analyse the VAT gap in the EU-25 Member States*, UK, 2009
The authenticity, integrity and legibility of electronic invoices in Europe from 1 January 2013

Qualified Electronic Signatures and Continuous Auditing