CEN

WORKSHOP

AGREEMENT

CWA 16047

December 2009

ICS 35.240.60

English version

E-Invoicing Compliance Guidelines - Commentary to the Compliance Matrix

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No.:CWA 16047:2009 E

Contents

Foreword

This CEN Workshop Agreement (CWA) has been prepared by the CEN/ISSS Workshop on 'e-Invoicing Phase 2' (WS/eInv2)

The CWA has been approved at the final Workshop plenary meeting on 10 September 2009.

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN: AENOR, AFNOR, ASRO, BSI, CSNI, CYS, DIN, DS, ELOT, EVS, IBN, IPQ, IST, LVS, LST, MSA, MSZT, NEN, NSAI, ON, PKN, SEE, SIS, SIST, SFS, SN, SNV, SUTN and UNI.

This CWA is part of a set of CWAs that has been prepared by Phase II of the CEN/ISSS Workshop on Electronic Invoicing in the European Community (the Workshop).

The objective of this phase of the Workshop is to help to fill gaps in standardization for the use of electronic invoice processes, to identify the various practices in Member States, to integrate the emerging technical and practical solutions into effective good practices, and to define and disseminate these good practices for e-invoices in close coordination and cooperation with private industry, solution providers and public administrations.

Five initial Projects have been established with a view to supporting the:

1. Enhanced adoption of electronic invoicing in business processes in Europe;
2. Compliance of electronic invoice implementations with the Directive on the Common System of Value Added Tax 2006/112/EC [1] as well as Member States national legislation as regards electronic invoicing;

   ► **NOTE**: *This document also takes into account proposals for the amendment of this Directive as specified in "Proposal for a Council Directive amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing" COM(2009) 21* [2].

3. Cost-effective authenticity and integrity of electronic invoices regardless of formats and technologies;
4. Effective implementation of compliant electronic invoice systems in using emerging technologies and business processes; and
5. Emerging network infrastructure of invoice operators throughout Europe.

This CWA was jointly developed by the groups working on the projects 2 and 3 listed above.

In addition, the Workshop has assumed the overall responsibility, as far as CEN is concerned, for the standards aspects of the European Commission's Expert Group on Electronic Invoicing, complementing and linking with the relevant Commission groups, and ensuring the relevant global standards activities are correctly informed and primed. In this activity, the Workshop aims to ensure collaboration with other CEN/ISSS groups, including WS/BII and WS/eBES, with UN/CEFACT (TBGs1 and 5), ISO TC 68 and ETSI/TC ESI.

The CWA TG2 Compliance
Sub Group 1: e-Invoicing Compliance Guidelines

Joost Kuipers	Leader	Netherlands Tax and Customs Administration *Belastingdienst*,
David Chambers (pre 1st June 2008)		HM Revenue & Customs (HMRC)
Kevin Thornton (post 1st June 2008)		HM Revenue & Customs (HMRC)
Christiaan van der Valk		TrustWeaver
Olaf Schrader		Crossgate / Ariba
Jacqueline Wijnands		Netherlands Tax and Customs Administration *Belastingdienst*
Danny Kuijper		Netherlands Tax and Customs Administration *Belastingdienst*
Patrick Frijns		Netherlands Tax and Customs Administration *Belastingdienst*
René de Waard		Netherlands Tax and Customs Administration *Belastingdienst*
Tony Nisbett		IBM /EDIFICE
Mounir El-Khoury	Technical Editor	MKE

CEN/TG3 Cost-effective authentication and integrity of electronic invoices

Johan Borendal	Leader	TrustWeaver
Adrian Mueller		Mueller Consulting
Andrea Caccia		Innovery
Christiaan van der Valk		TrustWeaver
Eloy Ruiz Madueño		Spanish Tax Administration
Marc Straat		Adobe
Nick Pope	Technical Editor	Thales e-Security
Paul Hojka		APACS

The input provided by OFS Portal in reviewing and providing a number of useful comments on this document is gratefully acknowledged.

Companies supporting the current CWA

Accelya, France
ACEAT, Tax Agency of Spain, Spain
Adobe Europe, United Kingdom
Agenzia della Entrate, Italy
AITI, Association of the Italian Corporate Treasurers, Italy
ARIBA, Germany
Atos Origin, The Netherlands
AUDI AG, Germany
Austria Pro, Austria
B2boost SA, Belgium
BMW AG, Germany
Campus 02, Austria
CBI Consortium, Italy
Datacert, United Kingdom
Deutsche Post, Germany
Dr. Otto Mueller Consulting, Switzerland
EDIFICE
ELMA, Finland
EQUENS, The Netherlands
FHNW, Fachhochschule Nordwestschweir, Switzerland
Fidal Direction Internationale, France
FIR-DIG Consultants, Italy
FMS Group, Italy
France Telecom, France
GS1 international, Belgium
Hilti A.G., Liechtenstein
IBM, United Kingdom
Infocert spa, Italy
Innovery spa, Italy
Itella Information AS, Estonia
Legal Counsel Engel-Flechsig, Germany
Ministerio de Industria, Turismo y Comercio, Spain
MKE, Belgium
Odette International ltd., United Kingdom
OFS-Portal, USA
RBS, The Netherlands
SFTI, Sweden
STS Group, France
Sofid/eact, Italy
TecCom GmbH, Germany
Thales, United Kingdom
The Netherlands Tax and Customs Administration, The Netherlands
Tieke, Finland
Trustweaver, Sweden
VAT Forum cv, Belgium
Verband der Automobilindustrie e.V., Germany
XFT GmbH, Germany

Introduction

The use of electronic methods instead of paper for exchanging, processing and storing tax-relevant invoices is increasingly viewed as a policy objective towards EU competitiveness, economic efficiency and protection of the environment.

While there are many organisations that carry out their e-invoicing in their own in-house data processing centres, the tendency is growing for companies to outsource all or part of their business processes including invoicing to various types of Service Providers. In this CWA, both in-house and outsourced e-invoicing operations are considered.

This CWA seeks to reduce some of the principal areas of uncertainty and resulting inefficiencies on the e-invoicing market with one single set of 'Compliance Guidelines' for both businesses, Service Providers and tax administrations. Such compliance guidelines are needed for the following reasons:

- Regardless of the regulatory framework in place, and regardless of the media used (paper, electronic or a mix thereof), VAT audits will generally require reasonable assurances that invoices are prepared, created, sent or made available, received, processed and stored in ways that allow tax administrations to verify during the storage period that invoices are unique, real, unchanged and accurate.

- Conceptually, electronic invoicing does not differ significantly from paper-based invoicing processes;

- Because electronic invoicing methods can improve both business efficiency and auditability, it is in the interest of all parties to make electronic invoicing as easy as possible.

- Paper-based invoicing has used the same well-known and accepted techniques for many centuries. Businesses that implement electronic invoicing, on the other hand, are often faced with thousands of technical and process implementation options that do not benefit from such historical antecedence or acceptance.

- Legal frameworks around the use of electronic media are not yet fully mature and questions sometimes remain about the compliance or enforceability of certain e-business methods.

- In the absence of implementation-relevant rules emanating from tax administrations or standards bodies, companies and Service Providers are often uncertain that their choices are accepted as sufficiently auditable and VAT-compliant by Tax Administrations. This uncertainty creates a significant barrier to investment in electronic invoicing.

- Corporate e-invoicing users and Service Providers feel insecure about their e-invoicing solutions. They want to be (VAT-) compliant, however today most tax administrations do not provide accreditation services or self-assessment programmes to assist such parties to ascertain that e-invoicing systems are VAT-compliant.

- Tax Administrations also often seek guidance on how to audit e-invoicing solutions.

These E-Invoicing Compliance Guidelines Commentary and the Compliance Matrix have been developed by a team of Tax Administration officials, businesses representatives and tax lawyers drawing on present day knowledge from Member States and business communities. The purpose of these E-Invoicing Compliance Guidelines, see Annex 1, is to provide practioners with an instrument for (self-) certification and to ensure cost-effective auditability. The Guidelines are a solid foundation to start a tax audit in situations where e-invoicing solutions are used. See further the scope of this CEN Workshop Agreement in section 1.3.

The Guidelines provide a framework for a range of approaches to e-Invoicing. While acting in accordance with the Guidelines cannot be a substitute for meeting specific obligations under applicable national law (see 1.4), they can be a strong basis for practices complying with the current legal requirements across Europe and aim to be flexible so that future legal requirements can be accommodated within the Guidelines. They support the range of techniques in use for e-Invoicing. They are applicable to different market sectors which may employ sector specific e-Invoicing practices, technologies and e-Invoice formats within the general EU legal framework.

1 Scope

1.1 Structure of this CWA

This Commentary complements a spreadsheet-based tool (***the Compliance Matrix, given in Annex 1***) developed by CEN in cooperation between companies and tax administrations. The two documents together constitute a multipart CWA called E-Invoicing Compliance Guidelines Commentary and the Compliance Matrix (***the Guidelines***)[1].

This Commentary consists of the following sections:

- **Section 4, Objectives and Process Model**
  Provides an overview of the objectives and process model used as the basis of good practices.

- **Section 5, e-Invoicing Basics**
  Provides basic guidance on good practices for e-invoicing. This is a simplified version of the comprehensive guidance given in section 6. This is particularly relevant to SMEs but also provides a general process basis for and introduction to the comprehensive description of risks and controls given in section 6.
  Whilst section 5 is targeted at SME's, where an SME is trading exclusively with large organisations or using a Service Provider, it may be sufficient for the SME to ensure that practices such as those provided in section 6 are applied by their trading partners or Service Provider.

- **Section 6, Comprehensive Guidance**
  Provides comprehensive guidance on good practices for e-invoicing using the Compliance Matrix. This section is primarily targeted at large organisations and Service Providers to select compliance appropriate to their environment.

- **Section 7, Further Technical Guidance**
  Provides further technical guidance on the use of various business control techniques.

- **Annex 1, E-Invoicing Compliance Guidelines Matrix**
  Provides practioners with an instrument for (self-) certification and to ensure cost-effective auditability

1.2 Target audience

The Guidelines are addressed to:

- Organisations engaged in, or about to introduce, e-invoicing.
- Internal and external auditors.
- Solution and service providers offering e-invoicing functionality.
- Tax Auditors in Tax Administrations.

Readers not familiar with electronic invoicing basics are advised to read Section 5 before reading this whole document or the Compliance Matrix.

1.3 Substantive scope

Companies exchange electronic invoices in a variety of ways. Many large companies carry out their e-invoicing in their own in-house data processing centres; however the tendency is growing for companies of all sizes to outsource all or part of their business processes including invoicing to various types of Service Provider. Also, a range of solutions have been adopted across Europe including those based around use of different types of control mechanisms that best fit each company's unique circumstances.

[1] The E-Invoicing Compliance Guidelines where initially developed by the Netherlands Tax Administration for Fiscalis. Fiscalis is EU Commission initiative to disseminate good practices across Member State tax administrations For more information about Fiscalis see http://ec.europa.eu/taxation_customs/taxation/tax_cooperation/fiscalis_programme/index_en.htm

The Guidelines seek to provide a single coherent framework for companies to perform electronic invoicing in a cost-effective manner while maintaining a sufficient degree of auditability and legal compliance through good practices in the implementation of business controls. These good practices may be adapted to cover a range of business environments covering SMEs to large organisations. The Guidelines are primarily about ensuring a smooth process from a tax (and in particular EU VAT) perspective; hence, whilst guidance is provided about business processes, the goal is always to balance business-internal goals with the specific legal and auditability requirements arising from VAT.

Specifically, the Guidelines are meant to serve as guidance for companies to ensure cost-effective auditability, and for tax administrations to ensure smooth audits. Importantly, the Guidelines do not address the substantive and core administrative aspects of VAT (determining applicable VAT law, VAT rates, reporting, payment, reclaims etc) but rather the process and technologies required to ensure that a business can prove – and a Tax Administration verify – that the invoices that form the critical component of most countries' tax audit frameworks are reliable.

While some audit techniques allow tax administrations to rely less on the invoice and more on general control frameworks as proof of transactions, such techniques are not expected to reduce the need for organizations to maintain the ability to prove to a tax auditor that the dataset they present as the formal invoice for tax audit purposes (hereinafter referred to as the "Invoice", see 3.2 Definitions) is the real and unchanged Invoice that they issued or received. Generally speaking, companies must therefore be able to prove not only that Invoices were processed or stored correctly within the Supplier's and Buyer's individual spheres of governance and liability, but also that these trading parties' administrative processes were ***aligned to ensure a trustworthy end-to-end process***. While each taxable person has a clearly defined set of responsibilities under VAT laws in the EU and beyond, trading parties must ensure that they have a common understanding of the processes and methods they will apply for ensuring auditability.

The Guidelines provide a common basis for organisations to agree on practices for the handling of invoices so that a coherent and easily auditable approach may be adopted.

1.4 The Guidelines as voluntary self-regulation

The Guidelines are not specific to any Member State and they are not substitute for complying with Member States' individual requirements, but they may assist in clarifying the basics for compliant e-invoicing processes underlying EU Member States' laws relating to e-invoicing and intra community e-invoicing.

While the drafters of these documents hope that this work will contribute to a more homogeneous legal landscape across EU Members States and beyond, the Guidelines are proposed merely as voluntary self-regulation. In case of conflict between the Guidelines and applicable law, the latter shall always prevail. ***For this reason, every requirement and associated control in the Guidelines should be applied with the caveat "To the extent permitted under applicable law,..".*** Future versions of the Guidelines may incorporate specific notifications or amendments in response to conflicts with Member State laws brought to the attention of the group responsible for maintaining the Guidelines.

The Guidelines are not intended as "regulation through the back door" – they will be equally or even more useful in a regulatory environment characterized by free choice of ways in which companies can satisfy reasonable tax requirements. The Guidelines are voluntary and fully neutral as regards technologies and processes companies may choose to adopt. The Guidelines represent just one technique among many other, equally valid and acceptable business process analysis techniques.

The Compliance Matrix is merely a checklist that could be used for self-evaluation and/or self-certification. Not all 100-line-items are applicable for all companies. A business should make a selection suitable for its own business model. To support this selection process, a filter is added based on the most frequently encountered business models in the market today. This does not mean these business models are the only accepted business models. This is a living document; if relevant, other business models will be added and companies practicing alternative models are encouraged to submit these for consideration.

Companies with well functioning processes in place could use the Guidelines as a voluntary check. If this check reveals that certain functional objectives are not currently met, the business could use the good practices of the Guidelines for inspiration to further improve their processes. This is always an individual decision of a business that must take into account that business's unique circumstances.

This CWA supports and is fully compatible with the proposal for a Council Directive amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing (Brussels (2009)21) [2] and endorsed by the European Commission's Expert Group on e-Invoicing (MidtermReport-2009_01_27 [3]).

Although an invoice is an important document and often the only trade document specifically mentioned in VAT legislation, in most cases it is not a standalone document in a sales / purchase process. The Guidelines are built around a trustworthy end-to-end process that business partners may agree to deploy. The Guidelines focus on the e-invoicing process itself, but it is recognized that the invoice process is part of the procurement process.

Some Member States allow companies in certain circumstances to deduct VAT without a secured end-to-end process, purely on the basis of business controls in place (based on the full e-procurement process). The Guidelines acknowledge that, in such Member States, companies that exercise and can prove a high level of internal control do not need to rely on end-to-end controls of transactions in order to prove that transactions were performed. However, every transaction involves two parties and, to use internal controls as the principal mechanism for proving transactions, each party must ensure such internal controls individually. The Guidelines identify four business implementation "classes" for compliant e-invoicing, including good practices for companies that choose to base their approach primarily on internal controls (see Sections 6.2 and 7.2.1).

1.5 Cost-effectiveness

This CWA addresses methods that can be cost-effective to different companies' individual circumstances. The actual cost of maintaining a proper and auditable business process depends on a combination of factors, for example:

- The complexity of a company's existing or planned e-invoicing processes.
- The nature of a company's business (many ad hoc trading relationships or stable supply chain; the average size of trading partners etc).
- A company's existing level of risk (including regulatory compliance) management controls already in place.
- A company's existing resources in relation to VAT/taxation generally. For example, a company with local tax managers in each country where it operates might be more comfortable with a solution that does not strictly meet the letter of the law, but which it believes can nevertheless be explained, while a very centralized company without such resources might want to avoid any risk of explanations to local tax authorities.
- The degree to which a company can re-use e-invoicing controls for other business purposes.

Every company is driven by a natural desire to increase shareholder value and, thus, to maximize sales while reducing costs and risks to the largest possible extent under applicable law. While real and de facto standards around accounting and other back-office operations have created a high level of similarity among administrative business processes, the uniqueness of each company creates a combination of circumstances that to a large extent determine the cost-effectiveness of any set of invoicing controls. It is therefore very difficult to make general statements about the cost-effectiveness of any control set.

The solutions in the Guidelines have been selected to cater to this diversity by describing a variety of approaches that are considered to have the highest potential to be cost effective in many corporate circumstances. Nevertheless, the authors of this CWA have paid specific attention to the needs of Small and Medium sized enterprises (SMEs). SMEs are a key focus of the European institutions and, increasingly, the appropriateness of regulation to SMEs is viewed as a test for the effectiveness and fairness of policy initiatives. SMEs consistently represent 50-70% of EU GDP and provide two thirds of jobs in Europe (NORMAPME March 2008). SME needs are addressed by:

a) Taking a cost / risk balanced approach.

b) Taking a "functional equivalence" approach allowing use of available technologies and processes that achieve the same level of trustworthiness. From these alternatives solutions can be deployed to match the needs of companies of all sizes, with or without the intervention of Service Providers.

c) Providing reference wherever possible to standard solutions which can easily be obtained from a wide variety of vendors.

d) Using procedures which are based on existing recognised business practices.

The cost factors and how they impact on a company's business costs are significantly different. For process-based controls the costs of establishing the appropriate security controls generally involve time from personnel in defining the appropriate security practices as part of the overall business process. In addition systems involved in the process must be adapted to produce appropriate audit trails. Strict auditing and review of the application of the security practices can be very costly if any degree of assurance is required that these practices are properly applied. Data-level controls, on the other hand, can have the benefit of making many such process-level controls unnecessary, but they may require a process and technology to be used that may not have been part of the original design of an information system and business process.

2 References

The following non-exhaustive list of examples of normative documents contains provisions that, through reference in this text, constitute provisions of this CWA. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties using this CWA in setting up or evaluating their e-invoicing processes are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies.

[1] COUNCIL DIRECTIVE 2006/112/EC of 28 November 2006 on the common system of value added tax

[2] Proposal for a Council Directive amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing" COM(2009) 21
http://ec.europa.eu/taxation_customs/resources/documents/common/whats_new/com_2009_21_en.pdf,
http://ec.europa.eu/taxation_customs/taxation/vat/traders/invoicing_rules/index_en.htm

[3] European Commission's Expert Group on e-invoicing; MidtermReport-2009_01_27
http://ec.europa.eu/internal_market/payments/docs/einvoicing/report-2009_01_27_en.pdf

[4] CWA 14171 General guidelines for electronic signature verification

[5] CWA 15579:2006 E-invoices and digital signatures

[6] ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates

[7] ETSI TS 101 733 CMS Advanced Electronic Signature

[8] ETIS TS 101 903 XML Advanced Electronic Signature

[9] ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates

[10] ETSI TS 102 231 Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information

[11] ETSI TS 102 640 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies;

[12] ETSI TS 102 734 Profile for CMS Advanced Electronic Signature

[13] ETSI TS 102 904 Profile for XML Advanced Electronic Signature

[14] ETSI TS 102 176-1 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

[15] ETSI TS 102 778 PDF Advanced Electronic Signature Profiles Parts 1 to 5

[16] ISO/IEC 27001 Information technology – Security techniques – Information Security Management Systems – Requirements

[17] AICPA SAS 70 Statement on Auditing Standards No. 70, Service Organizations

[18] OECD Guidance on Tax Compliance for Business and Accounting Software

[19] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[20] IETF RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

[21] IETF RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[22] IETF RFC 3125 Electronic Signature Policies

[23] IETF RFC 3161 Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)

[24] IETF RFC 3335 MIME-based Secure Peer-to-Peer Business Data Interchange over the Internet (AS1)

[25] IETF RFC 3851 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification, Applicability Statement 1 (AS1)

[26] IETF RFC 3852 Cryptographic Message Syntax (CMS)

[27] IETF RFC 4130 MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)

[28] IETF RFC 4823 FTP Transport for Secure Peer-to-Peer Business Data Interchange over the Internet, Applicability Statement 3 (AS3)

[29] IETF RFC 5246 Transport Layer Security

[30] ISO 6422 Layout key for trade documents

[31] ISO 9735 Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules

[32] ISO 32000-1 Document management - Portable document format - Part 1: PDF 1.7

[33] W3C Recommendation XML Signature Syntax and Processing
http://www.w3.org/TR/xmldsig-core/

[34] Commission Recommendation EDI 94 820 EC dated October 19th 1994 on the legal aspects related to electronic data interchange (EDI),

[35] Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (Including WebTrust® and SysTrust®)
www.webtrust.org

[36] ITU-T X.400 | ISO/IEC 10021-1 Message Handling System and service overview

[37] OFTP ODETTE File Transfer Protocol

[38] OFTP2 ODETTE File Transfer Protocol 2

3 Definitions and abbreviations

3.1 Abbreviations

AdES	Advanced Electronic Signature
AICPA	The American Institute of Certified Public Accountants
B	Buyer
BPA Matrix -	Business Process Analysis Matrix developed by the Netherlands Tax and Customs Administration (*Belastingdienst*) and provided as input to this project
CA	Certification Authority
CAdES	CMS Advanced Electronic Signature (see TS 101 903 [7])
CICA	Canadian Institute of Chartered Accountants
CMS	Cryptographic Message Syntax (see RFC 3852 [26])
CP	Certificate Policy
CRL	Certificate Revocation List (see RFC 3280 [21]
DUNS	D-U-N-S® Number (Data Universal Numbering System),
EDI	Electronic Data Interchange
ETSI	European Telecommunications Standards Institute
GL	General Ledger
ITU	International Telecommunications Union http://www.itu.int/library/
OCSP	Online Certificate Status Protocol (RFC 2560 [20])
PAdES	PDF Advanced Electronic Signature (see TS 102 778 [15])
PDF	Portable Document Format (see ISO 32000-1 [32])
REM	Registered mail
RFC	Request for Comment http://www.rfc-editor.org/rfc.html
RP	Relying Party
S	Supplier
SME	Small and Medium Enterprise
S/MIME	Secure/Multipurpose Internet Mail Extensions
SSCD	Secure Signature Creation Device
SSL / TLS	Secure Socket Layer / Transport Layer Security (see RFC 5246 [29])
TSA	Time-Stamping Authority
TSL	Trust Status List
TS	(ETSI) Technical Specification
XAdES	XML Advanced Electronic Signature (see TS 101 733 [8])

3.2 Definitions

The following terms have the following meanings in these compliance guidelines (the Guidelines):
(Where necessary, substitute “Supplier” with “Buyer in the case of self-billing”).

a) **Advanced Electronic Signature**: An electronic signature which meets the following requirements:

   - it is uniquely linked to the signatory;
   - it is capable of identifying the signatory;
   - it is created using means that the signatory can maintain under his sole control; and
   - it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. (Electronic Signatures Directive [13])

b) **Agreed Format of an electronic invoice**: The format that the Trading Partners have agreed to use as the format of the data to be exchanged between them.

c) **Archiving, Storage, Record or Document Retention**: The keeping of E-Invoices and related audit trails and materials under the conditions and for the period required by a Tax Administration and other applicable law.

d) **Audit of an E-Invoice or associated business processes**: The process of inspection of an E-Invoice and/or the processes and systems used for handling or storing an E-Invoice during its life cycle by a Tax Administration to ascertain the compliance of that E-Invoice and the underlying sales / purchase transactions with applicable law.

e) **Audit trail**: Information or data (whether in the form of logic, e.g. an algorithm or computer code, or a process, or a set of transactions, or a recording e.g. an event log, a video etc) that allows an auditor to verify that a process was performed in accordance with pre-defined expectations.

f) **Auditability of an E-Invoice or associated business process**: The ability for an E-Invoice or associated business process to be audited.

g) **Buyer**: An organization to which the Supplier makes a supply and that may be obligated to receive and store an Invoice, as well as being required to report and declare and being entitled to deduct/reclaim applicable input tax VAT.

h) **Conversion**: The act of automatically converting the format of an electronic invoice from the format of the sender to the format of the recipient (Format Conversion), or converting the encoding of content (e.g. different code list or units of measure), using agreed mapping processes that do not alter the information represented by the document (Content Conversion).

i) **E-Invoice life cycle**: A process comprising of (1) the creation or issue of the electronic invoice by, or in name and on behalf of the Supplier; (2) receipt of the invoice by or on behalf of the Buyer; and (3) storage of the electronic invoice during the storage period by or on behalf the Supplier and the Buyer.

j) **E-Invoicing Service Provider or Service Provider**: An organisation that, based on a contractual agreement, performs certain processes in relation to the E-Invoice life cycle on behalf of a Trading Partner, or that is active in the provision of support services necessary to realise such processes.

   Trading Partners can use multiple e-Invoicing Service Providers; see 3-corner model and 4-corner model definitions. An e-Invoicing Service Provider can subcontract all or parts of its services to other providers; such subcontractors can also be e-Invoicing Service Providers if they meet the criteria set out in this definition.

k) **Electronic data interchange (EDI)**: The transfer of commercial, administrative and business information between computer systems, using data formats which have been mutually agreed by the parties. EDI exchanges of invoices are normally used between trading partners to (partially) automate their supply chain. In most interpretations, the use of structured data alone does not make a process EDI.

A key element of an EDI system is the Interchange Agreement between the EDI trading partners making provision for the use of various technical, security and business procedures including those aimed at ensuring and proving the authenticity of the origin and integrity of the data.
In this context, Electronic data interchange or EDI is a generic term that covers conventional EDI file formats (UN/EDIFACT [31], ANSI-X12) as well as later developments using XML (Extended Markup Language) using UN/CEFACT or other formats.

Web EDI covers the techniques used to facilitate EDI via the Internet that may include forms EDI accessed via a web browser (see 7.3.5).

l) **Electronic invoice**: An electronic dataset prepared by or on behalf of a Supplier listing items sold and presented to the Buyer for payment, which contains all details agreed between the Trading Partners.

m) **Electronic invoice data**: A dataset not yet or no longer representing an Electronic Invoice, but which is intended to become an Electronic Invoice or which has been derived from an electronic Invoice.

n) **Electronic Signature**: Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. (Electronic Signatures Directive [12])

o) **Electronic Tax Invoice**: The designated electronic invoice for tax audit purposes with at a minimum all the properties that are legally required. In this Commentary and the Compliance Matrix, the Electronic Tax Invoice is referred to as **E-Invoice**; further the corresponding terms E-Invoicing and Invoice/Invoicing are used where appropriate.

p) **European Model Interchange Agreement, 94/820/EC**: Commission Recommendation of 19 October 1994 relating to the legal aspects of electronic data interchange.

q) **Format**: The organization or formatting of electronic data in an electronic document according to preset syntax and/or schema such as UN/EDIFACT, UNCEFACT, xCBL, cXML or PIDX.

r) **Interchange Agreement**: The provisions of Interchange Agreements are intended to govern the rules of conduct and methods of operation between the Parties in relation to the interchange of data by EDI. Several models of Interchange Agreement have been developed by European and International bodies:

s) **Internal control**: A process, effected by an organization's people and information technology (IT) systems, designed to help the organization accomplish specific goals or objectives.

t) **Invoice header data**: Data that relates to the whole invoice, e.g. invoice date, invoice number, Supplier and Buyer identification, name and address, bank account details etc. Some data is typically made available at header level in an invoice because it may be valid for all detail lines, but may be overridden as necessary by making the data available at detail line level, e.g. discount, currency code, VAT rate, delivery address, tax point, etc..

u) **Invoice line data**: Data that relates to the goods item or service being invoiced, e.g. goods item identification, quantity, price, description, etc… Some invoice line data may be made available in the header if it is valid for several invoice line items, but may be overruled at line level.

v) **Issue of an E-Invoice**: This is a legal term that is defined differently in different jurisdictions. The E-Invoice starts its life cycle as a formal document for VAT purposes when it has been issued. See section 6.6 for more explanation of the importance of the moment of issue in an e-invoicing process.

w) **Issuer of an E-Invoice**: The party issuing the electronic invoice (the Supplier or a party – a Service Provider or, in the case of Self-Billing, the Buyer – issuing the e-invoice in its name and on its behalf).

x) **Issuing an E-Invoice in name and on behalf of the Supplier**: The process whereby a party other than the Supplier issues the invoice in the Supplier's stead without taking over the Supplier's accountability for that invoice vis-à-vis the Tax Administration. The issuing third party may be a Service Provider or, in the case of Self-Billing, the Buyer or its Service Provider.

y) **Master data**: In this context for Trading Partners, Master Data are data that are stable over longer periods of time such as the names, addresses, and identifications, e.g. VAT numbers, DUNS number, GS1 GLN numbers. For product or services, Master Data may include product names, descriptions, tax category, and identifications such as GS1 identifier.

z) **Phishing**: A fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

aa) **Public Key Certificate (certificate)**: A set of structured data that has been electronically signed by a "certification authority" to "bind" the identity of a legal or natural person to a "public key" that can be used e.g. to verify electronic signatures created by that person.

bb) **Readability of an E-Invoice**: The ability of an auditor (e.g. Tax Administration or accountant) to interpret the content of an E-Invoice.

cc) **Self-Billing**: A method of invoicing whereby the Buyer issues the invoice in name and on behalf of the Supplier. Self-Billing may be facilitated by a Service Provider contracted by the buyer. See further section 6.4.

dd) **Source Transaction Data**: Relatively dynamic or transaction-specific business documents and information that are typically required to create an E-Invoice. This may included a contract, an order, dispatch information, delivery information, customer and product files, and possibly other details.

ee) **Spoofing**: A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

ff) **Storage period of an E-Invoice**: The amount of time that applicable law requires an E-Invoice to be stored and available for audit.

gg) **Supplier**: An organization that supplies goods or services to the Buyer and that may be obligated to issue and store an Invoice, as well as to report, account for and pay applicable output tax VAT.

hh) **Trading Partner**: Supplier or Buyer.

ii) **UN-Layout Key (UNLK)**: United Nations Layout for Trade documents, including the invoice. UN Recommendation 1 and Recommendation 6; ISO 6422 [30].

jj) **Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission (UNCID)**: As adopted by the International Chamber of Commerce and the United Nations Economic Commission for Europe.

kk) **VAT or Value-Added Tax**: A consumption tax that is levied at each stage of production based on the value added to a product or service at that stage.

ll) **3-Corner Model**: An invoicing process set-up whereby Trading Partners have separate contractual relationships with the same Service Provider.

mm) **4-Corner Model or Multi-corner Model**: An invoicing process set-up whereby each Trading Partner has contracted with one or several separate Service Providers, whereby the Service Providers ensure the correct interchange of invoices between the Trading Partners.

4 Objectives and Process Model

The descriptions of processes and models in Sections 4 and 5 aim to set a baseline for *all implementations* of E-Invoicing. Therefore, all implementation "classes" defined in Sections 6.2 and 7.2 should incorporate these baseline processes. The principal distinction among the implementation classes is where organizations place the emphasis of their controls for auditability purposes.

4.1 High Level Objectives

The high level objective of the Guidelines is to help organisations to establish practices to ensure:

- **Auditability:** the current and historical operation of an organisation's Invoicing process, including resulting Invoices, is auditable;
- **Authenticity:** the authenticity of the origin of Invoices is maintained;
- **Integrity:** the integrity of the content of Invoices is maintained;
- **Continuity:** the Tax Invoicing process correctly handles Invoices (including ensuring their uniqueness) and related documentation through their stages;
- **Legal requirements**: invoice requirements under applicable law, including for storage and access are complied with.

4.2 Overview of Process Model

The process model that has been used to analyze different steps in the E-Invoice life cycle is shown below. It represents the different steps in the information flow from Supplier, on the left, to the Buyer on the right.

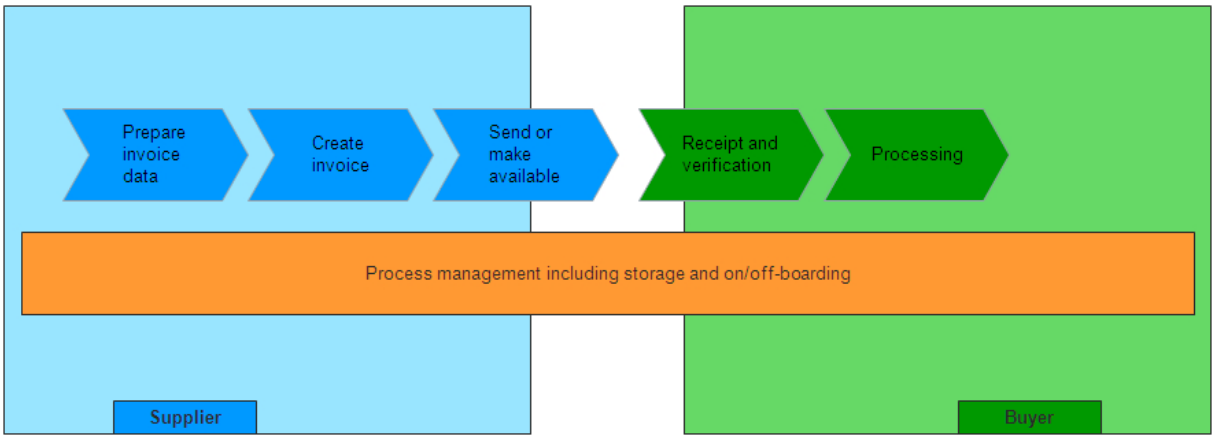


Figure 1 - End-to-end process model

This model is used as a tool for analyzing the requirements and describing the controls recommended for E-Invoicing. It does not imply that an implementation of the Guidelines must follow this process sequence. It is only an aid to relate the recommendations in the Guidelines to the real life processes that typically constitute in an invoicing system. ***In particular, certain aspects of the process steps described in the Guidelines may be carried out in a different order or may not be relevant in some implementations.***

This process model can be extended to incorporate one or more Service Providers which may support one or more stages of the process. An extended form of this process model is described further in Section 6 of this document.

4.3 Objectives in the context of the Process Model

In order to meet the high-level objectives specified in section 4.1 above throughout the appropriate phases of an e-invoice life cycle, the following specific objectives need to be taken into account for any E-Invoicing process:

1) When preparing the sales Invoice.

   a) Continuity of the information used in a Invoice with the other trading processes (e.g. purchase orders, delivery notes).

2) When creating the sales Invoice.

   a) Continuity of the creation process with the preparation process

   b) Verifiable authenticity of the Invoice once issued

   c) Verifiable integrity of the Invoice once issued

3) When sending Invoices or making them available.

   a) Authenticity of the Invoice during transfer verifiable upon receipt

   b) Integrity of the Invoice during transfer verifiable upon receipt

4) When receiving a Invoice and processing it.

   a) Continuity of all the processes concerned with handling a received Invoice

   b) Authenticity of the Invoice verified and maintained

   c) Integrity of the Invoice verified and maintained

5) When storing a Invoice and during the storage period

   a) Continuity of the process of storing a Invoice with the creation or receipt process

   b) Verifiable authenticity of the Invoice maintained throughout storage period

   c) Verifiable integrity of the Invoice maintained throughout storage period

   d) Invoice available in legible form for tax inspectors on request

6) Across the processes

   a) Auditability of all the processes carried out at every stage of Invoicing

   b) Invoices handled in accordance with applicable law through every process in the life cycle

Means to meet these objectives are first addressed (without mapping to the Compliance Matrix) through a basic E-Invoicing process description in Section 5. Section 6 provides guidance that is more detailed for professionals and should be read in conjunction with the Compliance Matrix.

5 e-invoicing Basics

5.1 Introduction

Invoices have multiple purposes. For an organization, invoices are primarily to request payment or paying. However, organizations also require invoices as a basis for meeting value-added-tax (VAT) obligations. To be sure that organization calculate, report, pay and reclaim VAT correctly, Tax Administrations need to be satisfied that such organizations have good control over the process for creating, sending, receiving and archiving invoices. By law, Tax Administrations often have the right to verify that an organization's Invoices and / or associated processes are correct, are an accurate reflection of their sales and purchases, and that VAT is administered correctly in their business.

The EU legal regime for VAT permits traders to send and receive Invoices electronically. In these Guidelines, a distinction is made between the generic term electronic invoicing – meaning any invoicing process handled electronically – and Electronic Tax Invoicing (E-Invoicing), which refers to the life cycle of an E-Invoice as defined in section 3.2.

This section 5 presents a simplified version of the comprehensive guidance given in section 6, addressing basic business processes and risks. This is particularly relevant to SMEs but also provides a basic introduction to the comprehensive description of risks and controls expanded on in section 6.

In addition, this section 5 addresses processes and procedures that small and medium sized companies (SMEs) are advised to have in place to be able to demonstrate and prove quickly to tax inspectors that they are compliant with VAT law.

SMEs have a broad range of possibilities to perform their Invoicing processes. They can either send or receive E-Invoices using in-house systems or outsource (some or all of their) processes to a Service Provider.

For E-Invoicing through Service Providers, SMEs are recommended to request candidate Service Providers for a third party assessment or self-assessment against the Comprehensive Guidance (see section 6).

This document is **not country-specific**; EU Member States may impose conditions that are either different from or that are more exacting than the good practices described herein (see also section 1.4).

5.2 General Invoicing principles

A company is strictly speaking only responsible for its side of the Invoicing exchange – a Supplier should issue an Invoice and a Buyer must receive and process it; both parties are generally required to store the Invoice as sent or received (see section 6.6 for more information on the topics of "original" invoices, the moment of issue and conversion).

The Buyer depends on the Supplier's ability to send an Invoice that is legally correct and technically suitable for the Buyer in his purchase process. Therefore, it is very important that organizations have a clear common understanding of the way they do business together. From a compliance point of view, there is no difference whether they operate a paper-based or an electronic Invoicing process.

Whilst many options are available, under different Member State laws and tax administration guidelines, to combine paper and electronic Invoicing processes, companies are recommended to classify their Invoicing processes as either paper-based process or electronic in principle. In a paper-based process, the Invoice is in principle the paper invoice as sent or received. In an electronic invoicing process, the Invoice is electronic.

It is recommended and in some countries, it is required, to maintain an up-to-date high-level description of the E-Invoicing processes used. As a general rule, the scope and level of detail of the process description document should be in relation to the size of the company and business volume, the complexity of the invoicing processes, the value of the transactions, etc. To ensure a smooth VAT audit, a company should be able to explain the overall process used in:

- Creating and sending their Invoices.
- Receiving and processing their incoming Invoices from all Suppliers.
- Storing the Invoices for the duration required under applicable law.

On request by a VAT administration, each trading partner must be able to make Invoice available for inspection in a readable format within a reasonable period of time during the storage period. Each party must also be able to demonstrate the consistency between Invoices, as sent or received, and the company's accounts.

5.3 Sales invoices

Suppliers of goods or services should take into account the following fundamental guidance.

WHEN PREPARING THE INVOICE – Use a process that allows Invoices to be complete and accurate by ensuring continuity with the other trading processes and compliance with applicable law.

Suppliers[2] must ensure that the process of preparing Invoices is coherently based on available transaction information (such as contracts, orders, delivery evidence etc). It is important that controls be in place so that computers and software used in this creation process are adequately protected from unauthorized access, and that any automated processes are well tested.

The Invoice should contain at a minimum the information required by applicable law (this includes the VAT law from the Member States where the supply is made, as well as the VAT and other relevant laws of the Member State where the Supplier is established).

WHEN CREATING THE INVOICE – It should be clear;

- **who creates the Invoice, the Supplier or a third party;**
- **if a Service Provider creates the Invoice on the Supplier's behalf, there should be an explicit contract with this Service Provider;**
- **whether both parties agree that the Invoice is in paper or electronic format;**
- **the creating party must ensure that the Invoice is created in compliance with applicable law and that there is continuity with the preparation process;**
- **the creating party must take measures to ensure maintenance and verifiability of the integrity of the Invoice;**
- **the creating party must take measures to facilitate maintenance and verifiability of the authenticity of the Invoice;**
- **it should be clearly defined at which moment in the process the Invoice is finally created prior to sending it (or making it available) to the customer;**
- **what is the Agreed Format of the Invoice and, if it will be converted between the Sending and Processing by the Buyer.**

The Supplier, in consultation with the Buyer, has to decide whether the Invoice will be on paper or in electronic format. In the case that E-Invoicing is chosen, an acceptance of this form is required. The choice for paper or E-Invoicing determines which measures are available to enable the recipient of the Invoice to verify it was the Supplier or a third party acting on his behalf that created the Invoice and not someone pretending to be the issuer (authenticity), as well as to make it impossible for anyone to change the invoice without this being detected (integrity).

---

[2] Or, in the case of self-billing: Buyers. Self-billing is not explicitly addressed in this document. Please refer to the comprehensive Guidelines in section 6 for a detailed description of the way(s) in which self-billing affects the distribution of roles and responsibilities in an invoicing process.

For both paper and electronic Invoices, integrity and authenticity can be achieved through internal and data exchange controls, but for E-Invoices there is the option to apply an “electronic signature” on the Invoice data itself, which as well as protecting the data exchange, may reduce the need for internal controls as regards ongoing integrity and authenticity of the signed data.

Such a signature keeps integrity and authenticity verifiable throughout the next process steps all the way to the Buyer and potentially during the storage period. If an electronic signature is used, this should be applied as soon as is practical from the moment the invoice is created. It should also not be possible for anyone to remove or replace the created Invoice, except in a controlled manner. There must be a process to avoid creation of duplicate Invoices for the same supply: each serial number must correspond to a single original invoice. See Annex B for further technical details.

WHEN SENDING INVOICES OR MAKING THEM AVAILABLE – Make sure that the Invoice is issued and registered within legally prescribed time limits, and that the integrity and authenticity of the Invoice are maintained and verifiable.

The Invoice as sent (also called “issued”, which in most countries designates the moment the invoice has been sent or made available to the Buyer; see section 6.6.2) with its unique number should be administratively registered. The moment of issue is legally significant and determines whether the Supplier has complied with its legal obligation to issue an Invoice within a specific period after the supply.

The Supplier must ensure that a Buyer can receive the Invoice exactly as it was issued, and that the Buyer can verify who issued the invoice. Reliable delivery at the Buyer’s address must be ensured. In case of E-Invoices, if no electronic signature has been applied in the creation step, the Supplier should use another solution to ensure that the Invoice remains intact during the transmission, such as one described in 7.3.8.

In cases where it is allowed under applicable legislation for a Invoice to be converted, this conversion must ensure that the information represented remains intact (see section 6.6.3).

AFTER SENDING THE INVOICE - Have administrative capabilities, for example, to issue a credit note or corrective Invoice or make a clearly identified copy Invoice available.

If the Buyer rejects the Invoice because it is incorrect for business or legal reasons, the Supplier should send a credit note and/or a corrective Invoice. Credit notes and corrective Invoices must meet the same requirements as those applicable to Invoices, and should refer to the rejected Invoice so that the sequence of events in relation to a specific supply can be externally verified. (See further section 7.4).

Upon the Buyer’s request, the Supplier may make a copy of the Invoice available. Technical or process measures must be taken to ensure that such a copy Invoice can be clearly distinguished from the Invoice. For example, the copy Invoice may include a clear indication it is a ‘Copy’ or ‘Duplicate’ or equivalent appropriate term. (See further section 7.4)

WHEN STORING THE INVOICE - Keep the Invoice for the period prescribed by law. Maintain integrity and authenticity and the verifiability thereof, and be able to present Invoices for tax inspection.

The Supplier should be able to at any time during the storage period prove that the process, through which the Invoice was prepared, created, sent and archived, made it impossible for anyone to change or replace the Invoice throughout the storage period

In principle, the Supplier should store a paper Invoice if he sent the Invoice on paper and an electronic Invoice if he sent the invoice electronically.

In some countries the Supplier may choose to keep electronic source data of sales invoices (whether paper or electronic) and allow the Invoice as sent to be reproduced identically, while in other countries the Supplier must always store a (paper or electronic) Invoice that is identical to the invoice he sent or made available. Either way, the Supplier should ensure that the Invoices are properly protected from theft, destruction, corruption and change.

Once stored, the Invoice in the Agreed Format should never be changed – not through human intervention or error, and not due to changes in master data. If an electronic archive is used, that archive must provide integrity protection of stored Invoices through use of appropriate secure storage or by building on the inherent security of any existing electronically signed Invoice.

In the case that Invoices are permitted to be converted by national law, it should be possible to make stored Invoices available for audit inspections to confirm that the converted Invoices received by the Buyer were

correctly mapped representing the same information. The recipient should store converted Invoices it has received so that an auditor can compare the received Invoices with the stored Invoices to confirm proper conversion.

It should be possible to make stored Invoices available for inspection Invoice in a format that the Tax Administration can verify. There must be an easy way to find a specific Invoice in an archive (e.g. an indexing system making it easy to search on criteria such as customer name, date or invoice number).

5.4 Purchase invoices

Buyers of goods or services must take into account the following fundamental guidance.

WHEN RECEIVING THE INVOICE - Use a process that ensures continuity and allows the legal compliance and correctness of Invoices received to be determined. Integrity and authenticity of the Invoice should be verified, maintained and remain verifiable.

Buyers must know how and through what channel (physical mail, email, and posting on a web server…) their Suppliers will send them Invoices or make them available. Each Invoice should be checked to ensure beyond reasonable doubt that it comes from a recognized Supplier (or third party sending it on his behalf), does not appear to have been changed since it was issued and is complete. If the Invoice was electronically signed, such an electronic signature should be verified unless the Buyer has verified authenticity by other means.

Buyers should further verify the coherence of the Invoice with available transaction information (such as contracts, orders, delivery evidence etc). Controls must be in place so that computers and software involved in this verification process are adequately protected from unauthorized access, and that any automated processes are well tested.

Measures must be taken to detect and avoid processing duplicate invoices for the same supply. All Invoices, whether processed or rejected, must be registered in the Supplier's administration. If there is any reasonable doubt as to the authenticity or (formal or material) correctness of the Invoice arises, the Buyer must inform the Supplier of such problems and request a credit note and/or corrective Invoice.

WHEN STORING THE INVOICE - Keep the Invoice for the period prescribed by law. Maintain integrity, authenticity and the verifiability thereof, and be able to present Invoices for tax inspection.

Buyers should be able to at any time during the storage period to prove that the process, through which the Invoice was verified, processed and, archived, made it impossible for anyone to change or replace the invoice.

In principle, the Buyer should store a paper Invoice if he received the Invoice on paper and an E-Invoice if he received the Invoice electronically. The Invoice must always be stored exactly as received unless there are local regulations that permit alternative arrangements.

Invoices must be properly protected from loss, destruction, corruption and change. The Invoice should never be changed. If an electronic archive is used, that archive must provide integrity protection of stored Invoices through use of appropriate media or by building on the inherent security of any existing electronically signed Invoice.

It should be possible to make Invoices available for inspection in a format that the Tax Administration can verify. There must be an easy way to find a specific Invoice in an archive (e.g. an indexing system making it easy to search on criteria such as customer name, date or invoice number.

6 Comprehensive Guidance

6.1 Introduction

In the absence of implementation-relevant rules emanating from tax administrations and standards bodies, it is hard for companies and solution providers to make any value judgment as to how “compliant” E-Invoicing processes are. Service providers, solution vendors and their corporate customers that are taking steps to develop and implement VAT-compliant services naturally have a desire to be recognised, but very few Tax Administrations provide accreditation services or self assessment programmes to assist Service Providers or businesses to ascertain that E-Invoicing systems are VAT compliant.

The Fiscalis e-Audit Project Group “audit of e-invoicing” activity task team was established to address the need for further harmonization and sharing of ‘Good practice’ experience for Member State tax authorities in the area of audits relating to electronic invoicing and VAT.

The Compliance Matrix draws heavily on the Dutch language draft of the Fiscalis “Business Process Analysis [BPA] matrix e-invoicing” document, developed by the Netherlands Tax Administration (Belastingdienst) for the FISCALIS [3] E-Audit Project Group. It is addressed to Tax Administrations for the audit of VAT invoice solutions. The BPA Matrix has been modified and complemented with input from Task Group members, Fiscalis members and stakeholders having provided comments in the CEN process to make the Guidelines applicable to all EU Member States' practices and to aspects of good practice that are unique to Service Providers.

The Guidelines should make it possible for all parties involved to check whether their E-Invoicing processes, in-house or outsourced, are VAT-compliant, and if not, what corrective measures are available.

The Guidelines identify the main issues in question at each processing step during the E-Invoice life cycle for different invoicing methods (direct invoicing from Supplier to Buyer as well as self-billing) and providing detailed process guidance for a variety of implementation options including web publication, the use of various integrity and authenticity-enhancing methods, and the retention of electronic invoices. For each discrete processing step, the Guidelines define the ‘Risks’ (of inappropriate practices to companies and tax administrations); ‘Requirements’ (for companies to mitigate the risk); and ‘Controls’ (from which companies can choose to meet the requirements).

Filters have been added within the Compliance Matrix to allow the user to select a specific process or sub-process for which he wishes to view the details – for example: what are good practices for a Supplier in a self-billing process? What should I think of as a Buyer when on-boarding Suppliers to my e-invoicing solution? Use of the Compliance Matrix is addressed in section 6.8 below and in the Introduction of the Matrix document.

The issues surrounding self-billing are presented in more detail in section 6.4, as this way of invoicing is being introduced more frequently at present, but the issues and problems are not always clearly understood by the parties concerned.

6.2 Classification of Business Implementations

The Guidelines allow for use of a wide choice of alternative controls to meet the objectives identified in section 4. Whilst a broad spectrum of business solutions supporting e-invoicing is possible through the Guidelines, they can be broadly classified into four classes to which the controls recommended in the Guidelines may be related.

The following classification assumes and builds on a minimum level of basic E-Invoicing processes as described the E-Invoicing basics in Section 5. These basic processes, which every company will have in place, tie an E-Invoicing process to a sales / purchase transaction and include normal content checking against orders, contracts etc. In addition to such basic controls, organizations should focus on the following “classes” of control mechanisms to ensure auditability:

[3] FISCALIS: EU Commission initiative to disseminate good practices across Member State tax administrations.

A) Business solutions exclusively relying on the transparency of individual trading partners' *internal* business controls to prove sales transactions to tax administrations (note that Class A is not explicitly referenced in the Compliance Matrix for reasons explained in Section 6.3.1). Such solutions may also involve the conversion of the E-Invoices between sending and processing E-Invoice following receipt;

B) Business solutions relying on basic business controls augmented by controlled data exchanges (e.g. EDI) to ensure that real and unchanged Invoices exist between trading partners and can be made available to Tax Auditors;

C) Business solutions relying on basic business controls augmented by data level controls (e.g. Advanced Electronic Signatures) to ensure that real and unchanged Invoices exist between trading partners and can be made available to Tax Auditors;

D) Business solutions relying on basic business controls augmented by central "safe-keeping" of E-Invoices to ensure that real and unchanged E-Invoices exist between trading partners and can be made available to Tax Auditors.

Further classifications may be added as business practices are identified or evolve.

These classes are considered from the perspective of the parties involved in the VAT-able sales transaction.

Business solutions in practice can be mixed and matched from the above classes – for example, a Supplier could use solution class D (the Invoice does not move from the "safe-keeping" environment) while the Buyer uses a class A solution (exclusive reliance on process controls). It is nevertheless important that the manner in which the Invoices are exchanged be clearly agreed between the parties in order to avoid mismatches.

6.3 Outline of Practices for Business Classes

6.3.1 Class A: Business controls

► **NOTE**: Class A is not explicitly referenced in the Compliance Matrix, because the feasibility of Class A as the primary method for ensuring compliance and auditability depends more on the type of organization and the way in which certain processes and controls are naturally implemented than on the nature of such controls. Nonetheless, all generic controls described in the Guidelines (controls that are applicable to all implementation classes) also apply to Class A.

Class A is all about transparency: it is particularly suitable for companies that have very transparent and easily auditable processes. Examples of companies that may consider relying on Class A for auditability include:

a) Companies that are so small or are so straightforward in the nature of their business and administrative processes (same products, customers, staff over long periods of time for example) that an auditor can quickly obtain assurances about the veracity of transactions.

b) Companies that by law have to meet heavy internal control requirements and that are regularly audited by both internal and external auditors. Examples include companies subject to US Sarbanes Oxley requirements or companies in certain heavily regulated industries.

Relying principally on internal controls for maintaining VAT auditability means that internal controls must be very well organized. In particular:

- General good security practices must be followed – see section 7.3.1 for more information.
- Particular attention must be paid to secure archiving of Invoices or of data allowing such Invoices to be correctly reproduced. Section 7.3.4 describes good practices for high-security archiving processes.
- Process and system documentation must be maintained using good practices in document management including version control systems with date references so as to enable auditors to understand which processes were in force within the corporate environment for all invoices during the storage period.

- Audit trails must be securely maintained of all Invoicing-relevant processing steps in the internal control process:
    - Where processes are manual, they must be well documented and traces of relevant process steps retained during the storage period.
    - Where processes are automated, relevant controls embedded in such automated business processes must be capable of being reproduced with the same result during the invoice storage period. Alternatively, it should be demonstrable by alternative means that the controls were working in the way intended.
    - In both above cases, trade documentation or data that Invoices are (manually or automatically) cross-checked against to attest to the integrity, authenticity and correctness of such Invoices must be retained.

Such classes of business solution may involve conversion between sending and processing an invoice following receipt. The mappings employed must be demonstrable to be correct.

6.3.2 Class B: controlled data exchanges

Business solutions relating to class B include, in addition to a controlled exchange, a level of automated syntax verification. Parties typically have a stable relationship and detailed agreement as to the modalities of their exchange process.

Class B implementations place the emphasis of controls for maintaining and proving integrity and authenticity of invoices on the exchange process between Supplier and Buyer. The following controls are generally required in Class B implementations:

- General good security practices are essential to the correct handling of invoices within the user systems – see section 7.3 for more information.
- Particular attention should be paid to secure archiving of Invoices or of data allowing such Invoices to be correctly reproduced. Section 7.3.4 describes good practices for high-security archiving processes.
- Structured data is used in such solutions and parties must agree beforehand on the Agreed Format and which processes and controls must be involved in the exchange. This requires an interchange agreement documenting at a minimum, which standards parties will use between them.
- Every leg of the process for sending or making available of the Invoice must be controlled through a combination of transport-level technologies and process-level controls.
- Both Supplier and Buyer (or third parties acting on their behalf) must typically have in place automated verification of message syntax. The Buyer must also have automated processes in place to identify messages from its Suppliers. Relevant controls embedded in such automated verification must be capable of being reproduced with the same result during the invoice storage period. This often means that specific steps must be taken to keep versions of software and systems used available with sufficient documentation to allow such evidencing.
- Process and system documentation should be maintained using good practices in document management including version control systems with date references so as to enable auditors to understand which processes were in force within the corporate environment for all Invoices during the storage period.

As described in section 6.8, for each control described in the Compliance Matrix to class B is indicated by a check in the appropriate column.

6.3.3 Class C: data-level controls

Class C implementations rely on the consistent use of Advanced Electronic Signatures or other (future) data-level techniques to prove integrity and authenticity from the moment of issue of an Invoice until the end of the storage period.

Because class C focuses on evidence of integrity and authenticity on the data level, the archiving process and technology does not need to provide these assurances for the invoice itself although sequence integrity is still needs to be maintained by the archive. Signing and signature validation can be performed locally with each trading partner or collapsed into a central point.

This form of electronic signature provides a technical means of protecting the authenticity and integrity, which can be directly bound to a Invoice. The signature may be used to verify the authenticity (if the signature identifies the invoice originator) and integrity of the invoice from the time of issuance, through sending and receipt, and in some cases for the life-time of storage. Some Member States may place explicit requirements regarding the use electronic signatures.

Guidance on the use of Advanced Electronic Signatures to provide data-level authenticity and integrity is given in section 7.2.2. Depending on the form of signature employed (see section 7.2.3) the signature may be used to a lesser or greater extent in protecting the authenticity in storage.

Other generic controls apply (see 7.3.1) to ensure that E-Invoices are correctly created and processed.

As described in section 6.8, for each control described in the Compliance Matrix to class C is indicated by a check in the appropriate column.

6.3.4 Class D: outsourced “safe-keeping”

Business solution class D typically revolves around a trusted outsourced relationship whereby the outsourcer operates highly trustworthy process and technological controls in a central secure environment – this third party therefore will engage in several process controls while the end user has to implement very few controls over and above Level 1 processes. The service could be provided by the Supplier, the Buyer or Service Providers.

Class D implementations rely on a trusted party that, under an outsourcing agreement, operates the entire life-cycle of an E-Invoice within a highly trustworthy environment. Invoices are stored within this environment and cannot be downloaded. Supplier, Buyer and their Tax Auditors can only view the E-Invoice through a graphical interface. Invoice data may be downloadable from the secure environment for downstream processing by the Buyer.

The Class D Service Provider, or the Supplier or Buyer providing Class D Services, must operate within an environment characterized by robust internal controls comparable to those described under Class A in Section 6.3.1 above. A Class D Service Provider must undergo regular recognized audits such as those mentioned in section 2, References, 17 and 35, by a trustworthy third party organization. Such audits would re-assure customers that the outsourced operations are totally under control. The Supplier or Buyer providing Class D Services may self certify compliance with internal controls or have third party certification, as agreed by the parties.

For class D, the archive is central to the concept (see section 7.3.4).

As described in section 6.8, for each control described in the Compliance Matrix to class D is indicated by a check in the appropriate column.

6.4 Extended Model Process

This process model extends that specified in sub-section 4.2. The extended process model that has been used to analyze different steps in the e-invoice life-cycle is shown below. It represents the different steps in the information flow from Supplier, on the left, to the Buyer on the right. Figure 2 represents the extended model without involving Service Providers; Figure 3 introduces the concept of Service Provider (or providers) into the model.

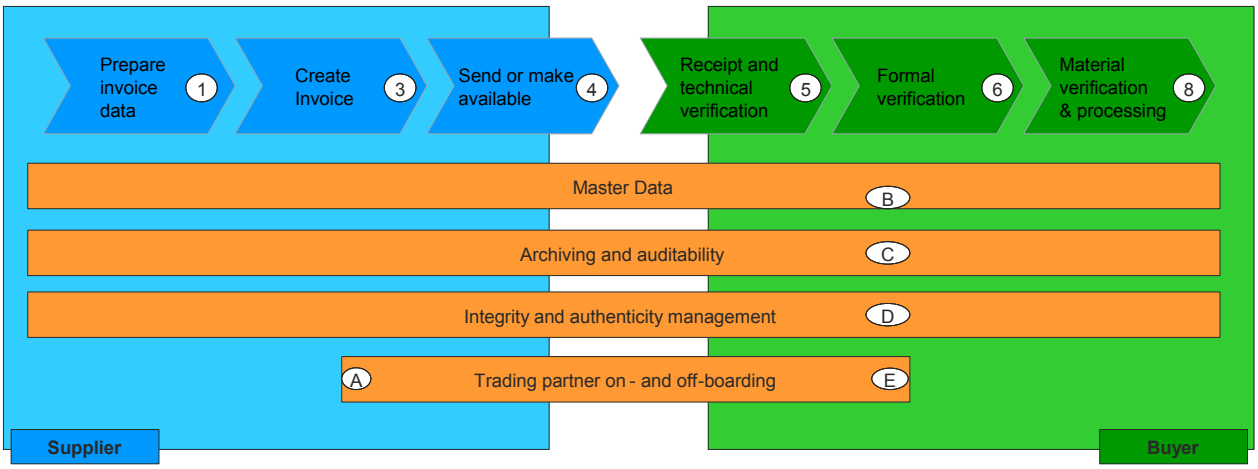


Figure 2 - Extended process Model without *Service Provider* involvement

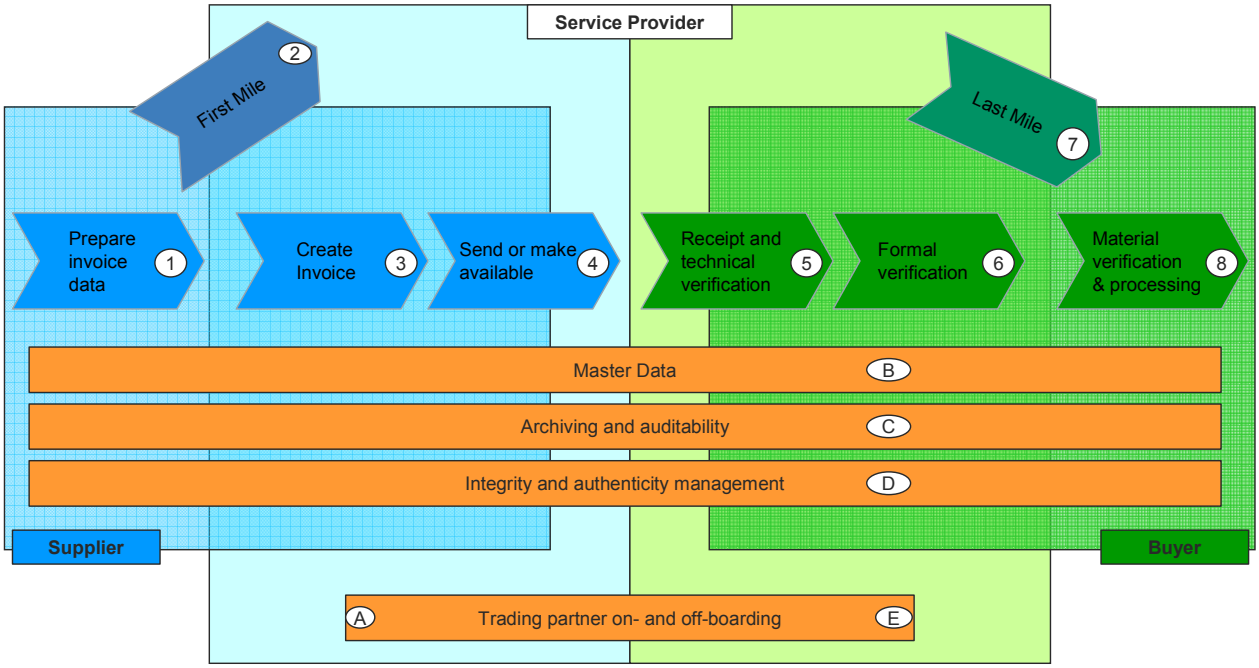


Figure 3 - Extended process Model with *Service Provider* involvement

In the case that one or both trading partners use Service Providers, then the flow passes through the 'first mile' between the Supplier and the Service Provider, and the 'last mile' between the Service Provider and the Buyer.

In the case of self-billing, the E-Invoice is issued by the Buyer (or his Service Provider) and flows in the reverse direction to the Supplier or via the Supplier's Service Provider. The following sub-sections provide an explanation of the steps in the above figures.

6.4.1 (On and Off) Boarding steps

Prior to exchanging E-Invoices, the trading partners have to go through the 'on-boarding' procedures that put in place the technical, procedural and legal basics of the E-Invoicing relationship. Similarly, specific "off-boarding" procedures must be ensured to wind down the relationship in good order. If one or more Service

Providers are involved, the on- and off-boarding process is extended into the relevant trading partner relationship with such Service Provider(s).

A. Trading partner on-boarding

On-boarding is the process of enabling a trading partner to interchange electronic invoices with another trading partner. This will include contracting, identification, connecting the trading partners to the technical infrastructure and applications used (this may include setting up web access or connectivity to the back-office system, format mapping, conversion, process re-engineering, testing, support, e-invoicing-specific contracting and/or training). Where one or more Service Providers act for the trading partners, the on-boarding process is aimed at setting up an end-to-end coherent structure and processes that enable appropriate auditability.

E. Trading partner off-boarding

Off-boarding is the process of terminating an E-Invoicing relationship. The parties terminating the relationship must ensure a winding-down of the relationship that preserves the trading partners' ability to provide the required auditability of their E-Invoices until the end of the storage period.

6.4.2 Processing steps

The processing steps in the exchange of the E-Invoice are expanded upon below.

1. Prepare invoice data

Based on source transaction data, the Supplier will prepare the invoice data required to issue an invoice in the Agreed Format or a format that can be converted into the Agreed Format.

The nature of this step depends on how automated the supply chain is. The Supplier provides invoice data via online entry forms or directly exported from back-office systems. Data captured manually has to be screened and checked to avoid errors occurring in subsequent processes or even later. In a back-office application, the same data will be obtained from data processed in other modules, e.g. order handling, shipping, etc. missing data or exceptions will be complemented after proper screening for correctness.

3. Creation of the E-Invoice

Starting with data prepared in step 1, the E-Invoices will be created in step 3 in the Agreed Format. Prior to creating the invoice, the Supplier must have performed all the controls required for ensuring that the E-Invoice is complete and accurate.

Creation of the E-Invoice is legally often followed by, or legally coincides with, the issue of the E-Invoice. See section 6.6 below for a more in-depth description of this legal concept.

4. Send or make E-Invoice available

This step consists of the exchange or depositing of the E-Invoice for collection by the receiving party. The Supplier (or in the case of self-billing the Buyer), or Service Provider will often start this process by initiating technical controls that must be checked by the Buyer (or in the case of self-billing the Supplier) or the Service Provider in order correctly to complete the technical receipt of the E-Invoice.

5. Receipt and technical verification of E-Invoices

In this step, the E-Invoice has entered into the control of the Buyer (or in the case of self-billing the Supplier), who will perform certain technical checks pertaining to e.g. the termination of secure transmission protocols, electronic signatures and/or – in automated systems - syntax checks and controls such as control counts, missing mandatory data (segments, data elements). This is defined at syntax level. Anomalies will generally be recorded and signalled to the Buyer (or in the case of self-billing the Supplier's) system controller. Only technically correct files/invoices will be passed to the next processing step. In case of a technical problem, the Supplier (or in the case of self-billing the Buyer) will be notified that there was an error detected during reception or processing of the E-Invoice and that it should be corrected and re-sent.

6. Formal verification of E-Invoices

Technically correct E-Invoice will be passed for formal verification, the extent of which depends on the capacity of the software and data available during this processing step; e.g. invoice date check, trading partner identification and addresses, availability of mandatory or conditionally required data, *vat* numbers, product and service codes,…

Only formally correct files/invoices will be passed to the next processing step. If a formal problem occurs the Supplier (or in the case of self-billing the Buyer) will be notified that the E-Invoice could not be accepted and a corrected E-Invoice should be sent.

8. Material verification and processing

In this step, further verification of the E-Invoice is carried out in the back office application, including checking and reconciling against all the necessary files available for invoice handling; e.g. Buyer order to the Supplier, goods receipt, price calculation, product file, contract or Supplier catalogue information, Supplier information, etc. differences identified in quantities, product specification, material or services, prices, conditions, payment terms, delivery terms, vat rates, etc. will have to be notified and resolved with the Supplier.

All E-Invoices in this step are processed. Only materially correct E-Invoices will be accepted for payment and further processing in the Buyer's application or in the case of self-billing the Supplier's application.

If an error is detected at this level, the Supplier or in the case of self-billing, the Buyer will be notified that the E-Invoice was not correct and that a credit note or other corrective document will be required to balance the accounting books such as the general ledger.

6.4.3 Service Provider-specific processes

2. First mile

In this step (applicable only to cases in which a *Service Provider* is involved), the invoice *data* will be communicated to a Service Provider to whom the function of issuing the Invoices and/or providing other services supporting E-Invoicing has been outsourced. The invoice data will typically be communicated through a secure communication channel.

7. Last mile

In this step (applicable only to cases in which a Service Provider is involved), the E-Invoice will be communicated by the last Service Provider involved in the processing of the E-Invoice to the Buyer's (or in the case of self-billing the Supplier's) in-house application for further processing. The E-Invoice will typically be communicated through a secure channel.

6.4.4 Supporting business processes

B. Master Data

Master data are data that are stable over longer periods of time such as the names, addresses, and identifications, e.g. *VAT* numbers, DUNS number, GS1 GLN numbers. For product or services, Master Data may include product names, descriptions, tax category, and identifications such as GS1 GTIN identifier.

When master data are stored separately from the E-Invoice data but relied on for completing or reproducing invoices in audit situations (this is allowed in some countries; see implementation classes A and B, sections 6.2 and 7.2), measures should be taken to ensure that the historically correct data are stored for each invoice to allow for such completion or reproduction.

C. Archiving and auditability

Both parties must store the E-Invoice for the storage period. The storage may be in-house or at a Service Provider. During the storage period, the competent tax administration has the right to audit stored Invoice. Invoice may (sometimes subject to additional requirements e.g. notification or authorization) be stored in another country. Some Member States may permit the storage of E-Invoices in a non-EU Member State, for example provided that they comply with data privacy laws. If

the E-Invoice is not stored within the Member State of the relevant trading partner, the latter as taxable person must ensure that the tax administration can access and audit the E-Invoice online within a reasonable time.

D. Integrity and authenticity management

This concerns the management of technology, policies, documentation and processes addressed to the assurance and long-term evidencing of integrity and authenticity of E-Invoice. Such assurances can be provided through two types of approach: using data-level methods whereby the long-term proof of integrity and authenticity remains technically verifiable as part of the audit of a stored E-Invoice; or using process-level controls whereby evidence is provided by referring to audit trails, documents, reproducible computer logic, reproducible conversions and/or third party audits.

6.5 Self-Billing: Issues and Controls

6.5.1 Self-billing

Self-billing is very common in certain sectors of industry where the Buyer is in a position to issue the invoice than the Supplier - for example:

- The payment of royalties following the sales of recorded music. Although the record distributor knows how many CDs were sold to a retailer, the retailer is able to initiate the process of settling the amount of royalty due to the artistes only when their record is sold.

  The supply of production materials direct to the production line, such as in the automotive industry; in these circumstances the manufacturer is able to issue the invoice on behalf of the Supplier, based on consumed quantities as part of the continuous production process.
  In the service industry, or other industries where purchases are not limited to discrete commodity units, self-billing may not be appropriate and should not be used absent consent of both parties.

6.5.2 Risks in VAT administration between self-billing partners

There should be strict adherence to agreed procedures between trading partners undertaking self-billing invoicing to avoid problems caused through lack of administrative controls. Some of the key risks regarding self-billing are the following:

- The Supplier takes no account of the self-billed E-Invoice and follows the normal process whereby the Supplier generates an E-Invoice and issues it to his Buyer. If this occurs, the Buyer will recover input tax VAT on his self billed E-Invoice, but may also recover input tax VAT on his Supplier's E-Invoice. There would be two sets of logic required here:
  - A process in the Buyer's system that did not permit automatic processing of an E-Invoice issued from a Supplier with whom a self-billing agreement exists, for a supply of a type covered by the self-billing agreement; and
  - A process in the Supplier's system which does not allow an E-Invoice to be issued to a Buyer with whom a self-billing agreement exists, for a supply of a type covered by the Self-Billing agreement.
- The Supplier receives his Buyer's self billed E-Invoice, but treats it as a purchase E-Invoice. The Buyer will have recovered input tax VAT when he issues his self billed E-Invoice, but the Supplier will both fail to account for the output tax VAT to balance the input tax VAT recovered by the Buyer, but will also recover an amount of input tax VAT to which he is not entitled. The logic required here would be either an automated or a procedural control which:
  - Prevents the VAT on an self billed E-Invoice received by a Supplier being treated as input tax VAT; and
  - Causes the VAT in the self billed E-Invoice to be accounted for as output tax.

In jurisdictions where each self-billed E-Invoice has to be explicitly accepted by the Supplier, it is possible to argue that these risks are much better mitigated than where such E-Invoice do not have to be explicitly accepted, but explicit acceptance is effectively a mandated procedural control and is much more burdensome than an effective system control. The electronic implementation of such explicit acceptance is likely to be equally burdensome. In other jurisdictions, the above risks are partially mitigated through an obligation for the trading partners to maintain a detailed agreement specifying the procedures to be followed. For example, it may be compulsory for the trading partners to agree on a specific time period within which the Supplier may reject the invoice issued by the Buyer on his behalf; non-rejection is then implicit acceptance. This mandatory agreement in such cases becomes a key piece of evidence of a process that the tax administration may audit for compliance with the contract terms.

6.6 The concept of an invoice in the legal context

6.6.1 Concept of an original invoice

Traditionally, in VAT law the Supplier and Buyer (the taxable persons) are liable to store the invoice exactly as sent or received; this unique instance of the invoice is often referred to as the “original” invoice. All other representations of the invoice, in whole or in part, are often called “invoice data”. While most laws do not explicitly define what constitutes an “original”, the concept of originality as currently used often refers to both the content and the format of the invoice. In the paper world, this means an invoice document that is identical in content and lay-out. This notion of originality encompassing the form of an invoice is related to the requirement for invoices to be rendered to the tax auditor in human-readable format: traditionally, a tax auditor can without any tools perform a prima facie comparison of two original instances of the invoice.

Currently, there are relatively few countries that use a definition of ‘original invoice’ as referring only to semantic content and not form or format. Such countries accept the concept of multiple datasets in different formats representing “original” invoices. The end result is that the invoices stored by the transacting parties are not comparable in terms of format but otherwise contain the same data set. Each transacting party maintains its own version of the original invoice that is readable by the trading party’s computer systems and the tax administrator may view the original invoices in each trading party’s systems. Conversion of original invoices is however always subject to each transacting party being able to produce an audit trail of all conversions of the data set comprising the invoice performed within its area of responsibility for the invoice as it finally stores. In addition or in the alternative, it is possible to compare the data set contained in the two original invoices to determine that only the format, and not the information, has been altered by the conversion.

For the countries in which the definition of an original invoice still has a form component, it remains important that each of the transacting parties can give the Tax Administration access to a dataset that is identical in both form and content. The format of the data set may not be automatically consumable by one or both Trading Partner’s systems but will represent the original data set in its original format prior to any conversion necessary to make it consumable by the trading party’s systems.

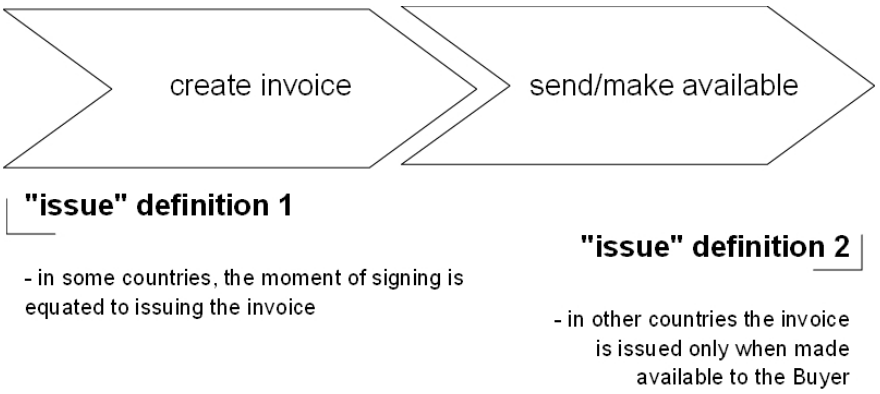
These Guidelines use the more neutral term Electronic Tax Invoice (E-Invoice) instead of original invoice. If this is not prohibited under applicable law, and subject to auditability being maintained in accordance with the good practices defined herein, a E-Invoice for purposes of these Guidelines can be converted (in terms of both form or content) without losing its status as a Invoice.

6.6.2 Moment of Issue of the E-Invoice

An E-Invoice begins its life cycle as a formal legal document when it is issued in the Agreed Format. Upon issue, the E-Invoice may no longer be disposed of or altered (other than in exceptional cases where Transformations are allowed, e.g. under class A, see 6.3.1); the E-Invoice from that moment onwards formally exists in VAT terms and both parties to the transaction are responsible for guaranteeing its integrity and authenticity until the end of the storage period.

In some countries, the E-Invoice is considered issued when explicit data-level methods have been applied for integrity and authenticity protection (when the E-Invoice is signed within an Advanced Electronic Signature). In such cases, the E-Invoice can be issued without having been sent or made available to the Buyer (Supplier in self-billing). In other countries, the E-Invoice is considered issued only when it has become available to the Buyer (Supplier in self-billing) or his Service Provider. The diagram below compares these contrasting situations in Member States.

Case 1 The E-Invoice is considered issued when a signature has been applied
Case 2 The E-Invoice is considered issued when it is made available to the Buyer.



6.6.3 Conversion of the E-Invoice

Conversion is essential for automatic data processing, since backend systems require different formats to extract invoice data from invoice messages. As long as some tax administrations interpret “original invoice” as “identical semantically and in syntax”, it is important to distinguish a conversion before or after the issuing of the original invoice.

- Before issuing of the E-Invoice:
  - conversion is possible based on the invoice data (at this time only invoice data exists);
  - for audit purposes it is recommended to store the invoice data before and after conversions, or at least to store the conversion logic (e.g. mapping tables) applied in order to preserve an end-to-end audit trail.
- After issuing of the E-Invoice:
  - conversion is possible only in regards to invoice data, but the E-Invoice must not be modified in any way:
  - the sender and receiver must store the E-Invoice and be able to provide this E-Invoice to a competent tax administration:
  - the converted invoice data needs to be treated as a “copy” (or “duplicate” – N.B. terms used may vary from country to country and depending on circumstances) but should always be distinguishable from the E-Invoice.

In both cases, the mapping to perform the conversion must not change the semantic meaning and should be reproducible. It is also required to provide both tax parties with access to the Invoice as explained above. Content conversion (e.g. using different code lists or units of measure), where permitted, requires Trading Partner to pay particular attention to the controls they put in place to avoid errors or misunderstandings. For example, a field or fields of data containing the information “10 Kilogram Cement Sack” may be transformed to “Cement Sack, 10.00 Kg” but the transformation must not interfere with the recipient’s ability to determine the correct number of kilos or that it is cement. Conversions that only change the format of the electronic invoice in accordance with agreed and reproducible maps are considered not to substantively alter the data contained in the electronic invoice.

Especially if multiple Service Providers are involved, it is currently common practice in many countries and industries to pass along multiple objects: the electronic Invoice, which is never converted, and electronic invoice data, which can be converted as required by e.g. the Buyer’s ERP system. This may require the trading partner to store the E-Invoice in one format for tax compliance purposes and invoice data in another format for commercial purposes.

The following must be considered in this regard:

a) The interchange agreement and/or any agreements with or among Service Providers should specify any conversion to be carried out and identify the party carrying out the conversion.

b) The integrity and authenticity of the information represented by the E-Invoice shall be verifiable across the end-to-end chain. Any transfer of data shall be protected as described in 7.3.8. Any process that performs conversion shall be assured as described in 7.3.1. Audit trails shall be kept of all mappings used, including information on any changes made and when applied, such the input and output invoice data can be compared to demonstrate that the information represented is the same as described in 7.3.7.

c) The agreements shall specify which party is responsible for archiving the invoice data in the Agreed Format and the automatic maps to or from Agreed Format in accordance with both applicable law and the contractual obligations among the trading partners and the Service Provider(s). The interchange agreement shall specify which party is responsible for performing each step in the end-to-end chain in an auditable fashion. The parties must agree on which Formats and Protocols may be transmitted and which will be the Agreed Format. To the extent permitted by applicable law, the parties may also agree to store their E-Invoice sent or received in their respective formats (i.e. the Supplier stores the invoice in the format it was in when it left the Supplier's computer or ERP system and the Buyer stores the invoice in the format it was consumed in by its computer of ERP system) for the specified time to allow for comparison between the stored E-Invoice to determine that the conversion did not alter the information represented in the E-Invoice.

6.7. The nature of Service Provider involvement

When a trading partner uses a Service Provider, this never implies outsourcing of any trading partner tax liabilities or responsibilities to the Service Provider. Outsourcing of E-Invoicing processes to a Service Provider can therefore never be an excuse for a trading partner's non-compliance towards the Tax Administration. The Service Provider's legal obligations are in most countries strictly contractual in nature; consequently, the obligations of Service Providers are merely derived from the trading partners' responsibilities. This is also how the Guidelines treat Service Provider responsibilities.

In exceptional cases, and where allowed under applicable legislation, a Service Provider that converts the E-Invoices must do so only in accordance with agreed maps that are reproducible and automatic. The mapping process must be auditable and audited. The maps may only change format and may not modify the recipient's ability to discern the correct amount and date of the invoice or other substantive data contained in the E-Invoice.

It should be noted, however, that this is different in countries that require a form of Service Provider approval or accreditation, as well as in countries where VAT law explicitly creates direct legal obligations for Service Providers: in such cases, a Service Provider may also be held directly accountable for the tax compliance of services delivered under or governed by such countries' laws.

6.8. How to use the Compliance Matrix

The content of the Compliance Matrix is not to be considered as exhaustive and although some of the original source material is from the Netherlands Tax and Customs Administration *Belastingdienst,* great care has been taken to ensure that content and recommendations are valid for most Member States and not specific to any individual Member State requirement.

Filters are provided in the Excel spreadsheet to help the user select his area of interest, e.g. Class B and self-billing, Service Provider for the Supplier and integrity and authenticity options. To get familiar with the guidelines it is in any case recommended to read the Compliance Matrix at least once from top to bottom.

Instructions on how to use the matrix are included with the Compliance Matrix file.

7 Further Technical Guidance

7.1 Introduction

Section 6 of this document and the Compliance Matrix identify requirements and possible corresponding controls for all aspects of E-Invoicing. Implementation examples reference standard solutions wherever available. In some cases, standard solutions exist but, because of the complexities of applying those solutions, it is not possible to provide succinct guidance on how the requirements may be implemented. This section expands on the implementation examples given in the Compliance Matrix giving further guidance on how the requirements and controls may be implemented.

7.2 Technical guidance specific to implementation classes

This Section 7.2 provides further guidance for rows in the Compliance Matrix relating to specific classes.

7.2.1 Class B: trusted exchange process

7.2.1.1 Model Agreements

Structured data must be used and parties must agree beforehand which processes and controls must be involved in the exchange. This requires an interchange agreement documenting at a minimum which standards parties will use between them. Commission Recommendation EDI 94 820 EC dated October 19th 1994 [34] relating to the legal aspects of electronic data interchange is the recommended basis for a model agreement under this class.

7.2.1.2 Securing Data

Every leg of the process for sending or making available of the E-Invoice must be controlled through a combination of transport-level technologies and process-level controls. In particular, controls must be in place in between physical or logical processing steps. Firewalls should be employed to ensure that trusted processes cannot be compromised through external attacks to transmission channels.

The mechanisms which may be employed to protect data during transmission are described in 7.3.8. Processes should be trustworthy using general good security practices as described in clause 7.3.1.

7.2.2 Class C: data-level methods (AdES)

Class C implementations rely on the consistent use of Advanced Electronic Signatures or other (future) data-level techniques to prove integrity and authenticity from the moment of issue of an E-Invoice until the end of the storage period.

7.2.2.1 Advanced Electronic Signatures

An Advanced Electronic Signature (AdES) as specified in the Electronic Signatures directive [19] is 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.

This form of electronic signature provides a technical means of protecting the authenticity and integrity which can be directly bound to an E-Invoice (see discussion on data-level method). The signature may be used to

verify the authenticity and integrity of the invoice from the time of issuance, through sending and receipt, and in some cases for the life-time of storage.

In Europe, three standard formats for advanced electronic signatures have been specified:

- CAdES (ETSI TS 101 733) [7] which builds on the use of binary formatted signatures as specified in Cryptographic Message Syntax (CMS - Internet RFC 3852 [26]), as profiled in TS 102 734[12].
- XAdES (ETSI TS 101 903) [8] which builds on the use of XML formatted signatures as specified in the XML Disg [33],as profiled in TS 102 904 [13].
- PDF Signatures as specified in ISO 32000 and profiled in ETSI TS 102 778 [15].

Although, the more widely implemented basic syntax for electronic signatures, XML DSig [33] and CMS [26], may be adopted for most countries.

The CAdES / XAdES standards specifies a number of different extended forms of signature referred to as "-T", "-C", "-X", "-XL", "-A". PDF Signatures already support an equivalent to the "-T" form using signature time-stamps. Work is ongoing in ETSI to specify forms of PDF Signatures equivalent to "-C", "-X", "-XL", "-A".

The signature may be applied by the Supplier as an organisation, by an individual representing the Supplier organisation, or a Service Provider with delegated authority. These different uses of signatures are discussed further in section 7.2.2.2 and 7.2.2.3

CAdES, XAdES and PDF signatures all depend on the use of Public Key Certificates (also referred to as certificates in this document). When signing a document, depending on the form of signature, information used to check the validity of the signature and its certificate is included within the signature. The different forms and their use when signing is explained in sections 7.2.2.4 and 7.2.2.6.

In order to achieve interoperability between the Supplier or other party signing the document and the Buyer or other party verifying the signature a number of aspects of the signature need to be agreed, for example through a signature policy. This is discussed in section 7.2.2.5.

The initial verification of a signature by the Buyer, or by a Service Provider on behalf of the Buyer, is described in 7.2.2.6. An important part of signature verification is the verification of the signer's Public Key Certificate. This may make use of certificate status and other information provided by the signer (as described in 7.2.2.4) where this is trusted, however in the general case this should be done using information collected by the verifier itself. Before verifying a signature the relying party may wait a grace period to be certain that up to date revocation information is available as discussed in 7.2.2.7.

One technique for ensuring the authenticity and integrity of E-Invoices in storage (see section 7.3.4) is to extend the E-Invoice signature with a time-stamp when the sender or recipient archives the E-Invoice as described in 7.2.2.8.

When verifying a certificate the relying party must trust the Certification Authority issuing the signer certificate. The management of certificate trust is discussed in section 7.3.3

Further guidance on the use of electronic signatures is given in CWA 15579 [5]. In particular, section 5.7.1 of CWA 15579 [5] recommends use of an extended key usage flag specifically for e-invoicing (“id-kp-eInvoicing”).

NOTE Equivalent forms to CAdES/XAdES -XL and -A for long term validation of PDF Signatures (PAdES) [15] is due to be published by ETSI Q3 2009

7.2.2.2 Usage of Signatures - Direct or Delegated Signatures

With electronic invoicing the emphasis of the Advanced Electronic Signature is to protect the authenticity and integrity of the E-Invoice rather than being an equivalent to a handwritten signature or other mark from the E-Invoice issuer.

Thus it is formally allowed in the Directive [1] and accepted market practice for the E-Invoice to be issued and signatures to be applied directly by the Supplier using a key under its own control or by a Service Provider on the Supplier's behalf. In the case of delegated or out-sourced issuance, the signature shall be applied with a

key and certificate identifying the Service Provider. It is further recommended (in the latter case) to indicate that the E-Invoice is issued by a third party Service Provider.
In the case of out-sourced signing on behalf of a Supplier, the Service Provider(s) shall ensure a proper audit trail showing how the identity of the Supplier (through proper authentication) is linked to the signing operation and the formally issued E-Invoice. This audit trail must start with a well-documented identification scheme as part of the Service Provider's Supplier on-boarding process.

7.2.2.3 Usage of Signatures - Personal or Organisation signatures

It is generally considered that the signature applied to an electronic E-Invoice is not the equivalent to a handwritten signature from an individual person.

Thus a signature should identify the organisation (company, governmental department or other form of organisation) that is signing the E-Invoice either directly or indirectly (see above). Where national legislation dictates that a signature is linked to an individual person then this should identify the person in the context of the responsible organisation.

7.2.2.4 Signing

When signing an E-Invoice, the signer's (public key) certificate should be included with the signature. This enables the verifier to check the signature using the appropriate certificate. This is a requirement of the basic forms of CAdES, XAdES and PAdES.

Note: In the case of the PDF signatures the signing certificate is not protected by the signature and so may be vulnerable to certain types of substitution attacks.

Ascertaining the time of signing is important for subsequent signature verification as the validity of certificates changes over time due to expiry and / or revocation. Thus it is recommended that signatures are time-stamped (using a time-stamp as specified in RFC 3161 [23]) on or shortly after the signing time. This can be applied either when creating the signature or immediately after by a Service Provider (in the case where the signature is created by the Supplier and then shortly after time-stamped by the Service Provider). This is provided by the CAdES-T and XAdES-T forms, and is an option for PDF Signatures.

Additional information that may be later used in verification of the signature, such as CA certificates, and revocation status (OCSP or CRL) information may be added to the signature as in the "-C", "-X", "-XL" forms of CAdES or XAdES.

If the party signing the document is also supporting the long term storage of E-Invoices the CAdES-A or XAdES-A form may be used to extend the authenticity and integrity of data over the storage period as described in 7.2.2.8. This "-A" form may be passed to the trading partner.

Further guidance on signatures for e-invoicing is given in CWA 14171 [4].

NOTE Equivalent forms to CAdES/XAdES -XL and -A for long term validation of PDF Signatures (PAdES) are due to be published by ETSI Q3 2009

7.2.2.5 Interoperable Signatures

In order that the signature created by the signer can be decoded and understood by the verifier there needs to be a common agreement on how the signature is to be applied to the data and how it can be verified.

This includes:

- How the certificate revocation status may be checked (e.g. whether using CRL or OCSP, where the revocation information may be obtained)..
- What time-stamps are to be employed (e.g. signature, archive).
- The relationship of signature to the data being signed (e.g. detached, enveloping, enveloped).
- Base standard used for signature (e.g. PDF / PAdES, CAdES, XAdES) & form (e.g. CAdES-A).
- Object being signed (e.g. message, invoice).

- Certificate format and profile.
- How to know if certificate (path) is trusted.

Much of this information may be specified in the form of a signature policy such as defined in RFC 3125 [22].

It is recommended that signature implementations are used that have successfully completed interoperability tests with a community of implementers of the same signature format.

7.2.2.6 Verification

On receipt of a signed E-Invoice the Buyer, or a Service Provider acting on behalf of the Buyer, should verify the signature. An important part of signature verification is the verification that the signer's (signing) certificate is valid at the time of signing. Unless there is other contextual information which can be trusted to indicate the signing time this should be as in the signature time-stamp (e.g. as from XAdES-T / CAdES-T).

Procedures for the verification of the validity of the signing certificate is specified in RFC 3280 [21] clause 6. This includes:

a) Verification that the certificate is issued by a Certification Authority directly, or indirectly via a valid chain of certificates, trusted by the verifier.

b) Verification that the signing time is in certificate validity period as indicated in the signing and CA certificates.

c) Verification that the signing and any CA certificates are not revoked using OCSP or CRLs.

If the signature is of the "-C", "-X", "-XL" or "-A" form the CA Certificate and revocation information provided or referenced in the signature may be used for verification. However, if available it is generally recommended that when initially verifying a signature the verifier obtains revocation status information from a source that it trusts.

When initially verifying a signature the verifier may augment the signature with the CA Certificate and revocation information used and apply a timestamp to create the "-C", "-X" or "-XL" form. If signatures are to be used for authenticity and integrity during the archive stage the "-A" form may be used as described in 7.2.2.8.

An audit record should be maintained of the verification of signatures.

Where a signature policy has been agreed between the parties the agreed policy rules should be applied.

Further guidance on signature verification can be found in CWA 14171 [4].

NOTE Equivalent forms to CAdES/XAdES -XL and -A for long term validation of PDF Signatures (PAdES) is due to be published by ETSI Q3 2009

7.2.2.7 Signature Grace Period

It is generally recommended to complete verification of a signature after what is called a “grace period” has elapsed allowing time to fetch the CRL/OCSP response applicable to the signing time. This grace period is the time taken for the certificate revocation information to propagate through the revocation process to relying parties. Without waiting, such a grace period there is a degree of uncertainty over whether the key was valid at the time of signing since it is possible that the user's certificate was revoked just before signing.

The need for a grace period can be avoided if CAs issuing certificates for e-invoicing take appropriate measures to apply such technological (e.g. OCSP [20]) and procedural (i.e. short revocation information publication cycles) measures as are required to reduce the grace period needed to a practicable minimum (ideally insignificant). Certain Service Providers or e-invoicing platforms may accept the business risk of compliance issues arising from non-respect of an applicable grace period.

CWA 14171 [4] specifies a signature validation process using a grace period.

7.2.2.8 Archived Signatures

One of the methods identified for protecting signed document over the storage period identified in 7.3.4 is to extend the signature using the CAdES/XAdES-A form.

The "-A" form signature can be created when the signed E-Invoice is first verified. Additional archive time-stamps may be necessary over the storage period if the document is to be stored longer than the lifetime of the time-stamp signature algorithm (see ETSI TS 102 176-1 [14] for guidance on the lifetime of signatures algorithms).

Use of such signatures ensures highly reliable verification of integrity and authenticity of stored E-Invoice. Therefore, there is less need for robust integrity and authenticity controls as part of the archive itself.

NOTE Equivalent forms to CAdES/XAdES -XL and -A for long term validation of PDF Signatures (PAdES) [15] is due to be published by ETSI Q3 2009

7.3 General Technical Guidance applicable across classes

7.3.1 General Good Security Practices

Taking into account the size and nature of the organisation as well as the basic approach to protection of E-Invoices (signature or process level), appropriate (general IT) controls should be implemented such as those set out in the following non-exhaustive list:

- Audit trails that demonstrate secure operation of all stages of the work flow including user applications, back office and external systems which enable E-Invoice to be transmitted (see also 7.3.7);

- The ability to prevent corruption during transmission and ensure timeliness;

- Controls to ensure completeness and accuracy of data.

- Logical access controls have to be in place to enforce business roles (e.g. mapping of defined user roles to user names and passwords, with permissions giving access to data and functionality appropriate to the role; and preventing access to data and functionality inappropriate to the role).

Use of recognised standards for auditing the security or general practices of the IT systems such as ISO 27001 [16] or AICPA Statement on Auditing Standards no 70 (SAS70) [17] provides a good basis for assuring the general practices of an organisation. The OECD Guidance on Tax Compliance for Business and Accounting Software (GTCBAS) [18] also provides guidance on good practices appropriate to business software.

It should be noted that a signature based e-invoicing process, which can always evidence E-Invoice integrity and authenticity, requires significant less in terms of audit trails, system documentation and formal third party audits to demonstrate authenticity at each stage in the e-invoicing process. Basic controls are still required to prevent unauthorised access, which may delete or make signed invoices invalid.

The signature based invoicing process can, based on the note above, be of special interest to SMEs where assurance of appropriate process based controls can be difficult.

7.3.2 Scanning of received Invoices

Some companies use scanning hardware, software or services to facilitate the processing of paper Invoices. Sometimes, optical character recognition techniques are used to convert the data on the paper Invoice into an electronically processable format. In other cases, the scanned images are used in an approval process using so-called workflow software. Nevertheless, scanned Invoices will often remain paper-based invoices from a legal perspective, which means that unless the law clearly states that the scanned copy of the Invoice may be electronically archived to replace the paper Invoice, companies using scanning systems must store the paper Invoice as received for tax evidence purposes.

7.3.3 Managing Certificate Trust

Many technical integrity and authenticity control techniques make use of public key techniques.

Where public key certificates (e.g. as defined in X.509 / RFC 3280 [21]) are used to support security such as in electronic signatures or secure communication channels (e.g. SSL / TLS [29]) for secure web access, or secure e-mail or AS2, they are the essential component of managing the trust between the trading parties. Establishing the trustworthiness of the Certification Authority (CA) which issues the certificate is essential to assuring the security protection provided by PKI techniques.

It is recommended that CAs are employed which use recognised good practices such as ETSI TS 102 042 [9], TS 101 456 [6] or AICPA/CICA Webtrust [35], and in the case of employing certificates to protect communications using SSL / TLS [29] also meeting the criteria defined by the CA Browser forum for Extended Validation certificates.

It is also recommended that authorities concerned with auditing compliance to VAT regulations directly, or by reference to a list maintained by an appropriate authority, provide a list of CAs recognised as meeting the needs for protecting the authenticity and integrity of E-Invoices. One means of issuing such a list of recognised CAs is to employ a Trust Status List as defined in TS 102 231 [10] (see Annex B for further details on ETSI trust status lists).

Ultimately, however, it is for a relying party (Buyer, Supplier, tax auditor or services provider) which verifies a signature or otherwise uses a certificate for security, to ensure that it maintains a list of "root" CAs which are trusted. A relying party must ensure that only those CAs, which are known to be trustworthy (through use of recognised good practice or by trust list information provided by a recognised authority), are held in its trust list. Procedures must be in place so that the trust list is updated to keep in line with those currently known to be trustworthy.

The CA issuing a signing certificate need not be directly trusted by the verifier. A chain of certificates may exist between the CA issuing the signing certificate and the trusted CA. There may exist a hierarchy of CAs with the verifier trusting the root and the issuing CA lower down in the hierarchy. Alternatively, there may be a "bridge" CA which provides a trusted mapping between the policy of the trusted CA and the issuing CA.

7.3.4 Archiving

E-Invoices are required to be held for a legally specified period for review by a tax auditor. The invoice must be stored in a way that prevents unauthorized access, deletion or theft, guarantees retrieval and readability and maintains the authenticity and integrity of the E-Invoice. A number of approaches are identified:

a) A "WORM" (write once read many) storage device such as a CD-ROM may be used to store E-Invoices. Any removable storage media should be labelled with a sequence number and date. CD-ROM devices may not be guaranteed to hold data for the full storage period, and hence it may be necessary to regularly make new copies of data held on such devices.

b) A trusted time-stamping service based on IETF RFC 3161 [23] (or equivalent) to time-stamp one or a set of E-Invoices may be used to protect the integrity of E-Invoices.

c) If a Service Provider is employed then the Service Provider may store E-Invoices on behalf of one or both trading parties. The Service Provider must apply appropriate controls to ensure the authenticity and integrity of E-Invoices.

d) If Advanced Electronic Signatures are employed, archive forms of the signature may be used (e.g. CADES-A or XAdES-A) to maintain the inherent authenticity and integrity of the signature over the storage period.

e) Access and retrieval via either web portal- based user interface including search index- based retrieval or direct links embedded in accounting data (e.g. hyperlink or web services) with security measure that prevent unauthorized access

A secure archive for electronic E-Invoice retention requires either “Write Once Read Many” (WORM) type hardware such as optical disk systems, software based technology or a well managed and third party audit secure database system with appropriate access control, integrity checks, audit trails and other security measures.

An additional alternative to WORM devices could be a system based on the use of cryptographic techniques.

A physical secure storage including backups separated by distance should be used.

If compression or encryption is used, the solution must support the ad-hoc decompression and/or decryption at any time of the storage period thus guarantying readability.

The best suited signature enveloper for archiving purposes are CAdES/XAdES-A as defined in ETSI TS 101 733 [7] and ETSI TS 101 903 [8] or the PAdES LTV profile [15]. These envelopes contain all elements required to verify a signature after the signer certificate expiration and possibly also after the CA certificate expiration. The envelope can be received as such in archive format or in any of the other formats (such as C/X AdES-BES or –T or –C etc) and then built in the Archive format. Since E-Invoices have to be stored by the sender and the receiver, using C/XAdES-A can be simpler if the same format is used for storage and transmission. For further details on long term signature required elements CWA 15579 §7.3 can be applied.

NOTE Equivalent forms to CAdES/XAdES -XL and -A for long term validation of PDF Signatures (PAdES) is due to be published by ETSI Q3 2009.

System documentation should record all the different elements that must be maintained e.g. digital certificates, receipt acknowledgements, invoice data, conversion rules (where a mapping Service Provider is utilized), any master data that is required to interpret invoice data, and the time period through which the data must be stored or retrieved. Data retention obligations should be clearly delineated between trading partners and Service Providers.

Service Provider documentation should also record how information stored with a third party Service Provider is made available if the third party ceases operation (Off-Boarding)

The above documentation should take into account tax and legal requirements as well as risk associated with keeping data longer than necessary. Archiving practices may also need to take account of the need to hold data relating to disputed invoices beyond the normal archival period.

7.3.5 Manual Web-based invoicing - authenticity and integrity concerns

Specific controls might be necessary in e-invoicing scenarios where a physical person manually handles the creation, sending or collection of E-Invoices through a web portal using tools such as a web-browser or similar client software.

The controls necessary for authenticating the web portal and the person in these scenarios depend heavily on the functionality available in the portal after logging in. For example, an invoicing portal that allows ad-hoc creation and sending of E-Invoices would require more stringent controls than a portal that only allows a purchase order to be turned into an E-Invoice (a so-called purchase order flip or PO-flip) without freedom to change data.

For portals that only allow purchase order flip, basic authentication of the web portal based on server-side SSL / TLS [29] and authentication of the individual based on username and password should be satisfactory. It should however be noted that such a web portal would still require a very high degree of security in the process relating to the purchase order upload.

For portals allowing more freedom in the process of creating or changing E-Invoices, additional measures should be considered. These measures should focus on increased user authentication based on client side certificates or tokens for two-factor authentication as well as increased web portal authentication using for example Extended Validation (EV) certificates. In addition users should be required to conform to an increased desktop security policy. Required desktop security measures should include:

- Virus protection software including timely updates.
- Firewall and optionally intrusion detection software.
- Use of modern browser, e-mail and operating system software, including the application of all security patches.
- Monitoring of log files from protection components.
- Running under a limited privilege user account (instead of a fully privileged administration account).

Security awareness and training is also critical and information to users should cover topics such as:

- Understanding common phishing techniques.
- How to check web portal identity based on SSL / TLS [29] server certificate authentication including use of Extended Validation certificates (see http://www.cabforum.org/).
- Instructions to never give away access credentials in situations other than the defined log on procedure.

While manual processes are permitted when agreed upon by mutual consent of the parties, the requirement to use manual processes should not be imposed on any trading partner by another trading partner.

7.3.6 Malicious Code in E-Invoice

E-Invoices when received can potentially contain malicious code which can:

- infect the E-Invoice processing system impacting on the overall operation of the invoicing processing system with potential disastrous consequences,
- cause the content of the E-Invoice to appear other than was in the original E-Invoice even though the E-Invoice passes the original integrity checks.

Malicious code includes not only viruses, worms and Trojan horses. Scripts passed within E-Invoices can be used to maliciously alter the content of E-Invoices. Clever use of formatting styles and special fonts can result in the information seen when viewing an E-Invoice to be different from that processed automatically.

Even if the source of an E-Invoice is authenticated and comes from a known trading partner, the recipient can be still subject to attack by this means. In spite of the security controls of the partner being considered to be adequate, unforeseen threats or lapses in security can result in malicious code being passed or introduced into E-Invoices. Thus, it is strongly recommended that controls are always in place to protect against malicious code.

A first level of protection can be achieved through use of general security and anti-virus controls.

A further level of protection can be achieved by placing restrictions on the content of the E-Invoice. Avoiding any use of scripts and rejecting any E-Invoice that includes active code and scripts is a good first step. Selecting the correct document format encoding can further significantly reduce vulnerabilities:

a) Use of editable formats with complex formatting and formula features such as office documents and spreadsheets should be avoided. It can be impossible to tell if any complex formula is not malicious. The ability to change the formatting data in editable documents makes them particularly vulnerable to abuse. Even if it is possible to “freeze” a Word file presentation ("shift+F9") the recipient cannot know whether this presentation was frozen before finalising the E-Invoice (e.g. before signing it)

b) Formats such as XML and PDF are much less susceptible to abuse. PDF/A is preferable to general PDF as this further restricts the use and requires all relevant format information, such as fonts, to be included with the documents.

c) Where style-sheets are used to convert XML to viewable formats, the source of such style sheets must be trusted. Style sheets should be held and accessed securely. Any third party providing style-sheets must be trustworthy. When auditing a system, consideration should be given to checking that any style sheets properly display randomly selected source data.

d) It should also be noted that graphical formats (e.g. BMP or TIFF) can also include HTML, which can result in different data being displayed depending on the context in which a file is viewed.

7.3.7 Audit trails

Audit logs holding audit trails are an important aspect of any auditable computer system. They provide evidence that the system is operating correctly and provide a means of tracing the source of a problem when things go astray.

Any errors detected during the operation should be logged. This includes authentication failures, errors in invoice data and any cross checks between invoice data and other data sources (e.g. orders). Any approvals made with regard to invoicing should also be recorded. If possible, audit logs should record positive occurrences of checks succeeding so that the correct operation of the system can be demonstrated. The audit logs should cover all the stages of handling an E-Invoice as described in the invoicing model (see section 6.4).

The level of detail required will depend on the class of e-invoicing business solution. For example, in the case of internal controls being the basis for auditability (class A) detailed information is required on all steps in the handling of E-Invoices. Whereas in cases where signatures are employed, less detail is required in the logs for handling the E-Invoice once it has been signed, but records of the signature verification are clearly vital.

Logs should be archived and protected against modification if possible to the same degree as E-Invoices (see.7.3.4).

7.3.8 Authenticity and Integrity of Transmission

Unless an E-Invoice is already protected by an electronic signature or other similar data-level security control, E-Invoice data must be transferred in a way that:

1) Protects the integrity of the data communicated,

2) Authenticates the source of the data.

Several types of solutions exist that provide the necessary protection. These commonly employ some form of cryptographic protection such as encryption or cryptographic check codes. Examples of such mechanisms include:

a) SSL / TLS with client passwords

The Transport Layer Security protocol (RFC 4346) is a variation of the Secure Socket Layer (SSL) protocol as commonly used across the Internet in with web browsers and other peer-to-peer interactive communications. These protocols always authenticate the server being accessed and protect the integrity of all the data exchanged. Additional measures are commonly necessary to authenticate the user accessing the service.

In a web based environment, use of simple identity and password mechanisms may be sufficient although care needs to be taken in operating in such a web based environment (see 7.3.5).

In a system to system integrated environment in which the parties elect to authenticate the client, dual SSL authentication can be used to validate both the server being accessed and the client initiating the HTTP connection.

b) AS1, AS2 and AS3

A set of security protocols have been defined specifically for securing business data (including invoices) interchange. These are commonly referred to as AS1, AS2 and AS3, where AS standards for applicability statement. AS1 (RFC 3335 [24]) is aimed at business interchanges using e-mail, AS2 (RFC 4130 [27]) is aimed at business interchanges using web (HTTP) protocols and AS3 (RFC 4823 [28]) is aimed at interchanges using file transfer protocols.

c) Secure E-Mail

General purpose email security protocols exist which may also be applied to invoicing. This includes S/MIME (RFC 3851 [25]) and the secure messaging service defined in ITU-T X.400 [36].

d) Registered E-Mail

Registered e-mail is a variation of secure e-mail that provides additional services to give proof of submission and delivery of the e-mail similar to the physical registered postal service. This has the advantage of providing further evidence that the E-Invoice has been successfully transmitted between the trading partners. A recent standard specification has been issued for Registered E-Mail (REM) in ETSI TS 102 640 [11].

e) Value Added Network

Where the provider of the transmission service establishes a network that is inherently secure (e.g. Value Added Network employing leased lines direct to each trading partner), further protection may be unnecessary. In such cases guarantees should be sought that integrity of E-Invoice is maintained and that correct routing between identified partners is assured.

f) Integrity measures, such as hash totals or reconciliation overviews

If the business process for handling E-Invoices is such that their authenticity and integrity is checked, then further mechanisms may be unnecessary. This can include of hash totals sent separately which can be reconciled with the received E-Invoices. Alternatively, business processes can incorporate a business response message that includes acceptance of the E-Invoice and a sufficient level of detail or summary of the E-Invoice to verify integrity of the received document.

g) Service Providers

Where Service Providers are used, each provider must validate the authenticity of inbound documents, maintain documented and auditable internal processes for routing or transformation of E-Invoices, and verify the security of the transmission of E-Invoices to the Buyer or next Service Provider in the process.

h) Use of encrypted/signed data fields within an unsigned document

Where data conversion or protocol mediation makes it impractical to encrypt and sign the complete electronic E-Invoice, trading partners may agree to sign just the invoice data that is mandatory under the applicable legislation within one or a limited set of data objects in the E-Invoice. The data in this field would remain unaltered even if the remainder of the document is transformed. The Buyer can realize the benefits of receiving digitally signed E-Invoice data which can also be used to validate the authenticity and integrity of the remainder of the transformed document.

i) OFTP/OFTP2

The Odette File Transfer Protocol (OFTP) and the more recent version OFTP2 (IETF RFC 5024) are widely used for secure business and CAD data exchange in the automotive industry and other industries. OFTP caters for partner identification via session ID and password protection. Used over ISDN or a VPN both authenticity and integrity of the transmission are ensured. A so-called end to end response provides an affirmative statement that the transmission had been successfully completed (i.e. a means of non-repudiation).
The OFTP2 protocol has security features such as SSL/TLS security (see paragraph a), file signing and encryption with digital certificates, usable on public internet without reducing integrity and proof of authenticity of the data exchange.

7.4 Dealing with incorrect or missing E-Invoices

Errors in Invoices can occur and rectification is required to arrive at a correct and balanced accounting between trading parties and with the VAT administrations, periodic reporting of VAT to be paid or recovered. The rectification transactions; credit notes and/or new Invoices, must be a clearly identifiable in the audit trail and any associated goods movement.

Tax regulations, accounting laws and Member State legislation often do not provide concrete examples and what is available may be open to interpretation. Some examples of situations are presented further in this section and some Tax Authorities do provide explanatory information on their websites.

In an automated environment errors can occur for several reasons:

- Basic data available in application systems on trading partners are incorrect or not maintained in a timely fashion leading to un-suspected errors; returned goods, new price lists and customer discount conditions, change in addresses, changes in VAT numbers, etc resulting in errors in a Invoice.
- Special conditions agreed at transaction level due to incidental promotions included in a purchase order but not reflected by the Supplier in the E-Invoice.
- Demands introduced manually in the E-Invoice by the Supplier that were not agreed with the Buyer.

7.4.1. Rejecting an E-Invoice, totally or partially

Independent of Member State regulation and accounting procedures, it is usually a requirement to reject an incorrect Invoice, totally or partially, and notify the issuer of the error in the Invoice, the Supplier in case of conventional invoicing and the Buyer in case of Self Billing. It is recommended that the Supplier be enabled to designate whether an incorrect or contested Invoice must be rejected in full or may be partially rejected with partial payment, but the trading partners must reach agreement on that election based on their particular circumstances. Allowing Suppliers to make such an election may have a significant impact on rate of adoption as many SME's may elect to allow partial rejection in order to receive partial payment prior to reconciling the Invoice and maximize their working capital. Larger Supplier enterprises operating ERP systems may prefer only full rejection of their Invoices in order to minimize the costs associated with reconciling a partial payment against the invoiced amount. Imposing a universal "reject in full" rule on all Suppliers might impose significant burdens on SMEs whose cash flow depends on receiving a partial payment of the uncontested amount, while imposing a "partial rejection" rule on all Suppliers may impose significant administrative cost and burden on larger Suppliers.

Some of the errors that can occur are mentioned below, including corrective procedures for some cases. The list is not exhaustive:

A) Rejecting Invoices

For paper E-Invoices, in some countries the Invoice must be returned to the issuer. For an E-Invoice, a rejection notification is sent to the issuer and the status of the invoice is changed to "rejected" on the E-Invoice administration log.

- Incorrect Purchase Order (PO) listed on the Invoice / The purchase order has been cancelled
- Invoice is not compliant with VAT requirements:
    - wrong content e.g. values like VAT IDs or future date
    - missing fields e.g. missing the reason for a reduced or 0% rated VAT (intra-EU trade with local law reference
- Depending on Buyer-Supplier contract a cancelation may be agreed for:
    - PO number not included on E-Invoice for PO vendors
    - Currency mismatch between Purchase Order and Invoice
    - Invoice amount is higher or outside of tolerance than the Purchase Order value
    - Invoice Quantity is higher or outside of tolerance than the Purchase Order Quantity
    - Mismatch of / outside of tolerance unit price compared to Purchase Order
- The Buyer should not modify any Invoice, including an incorrect or contested Invoice; after resolution of Buyer's objections, if necessary, a corrected E-Invoice should be resubmitted by the Supplier to the Buyer.

B) Request Credit Note

- Faulty goods returned or goods rejected by Buyer, credit note is used to correct the accounts receivable and inventory balance at the Buyer and Supplier side
- Product Wrongly Shipped – a "complete credit" should be used to correct the accounts receivable and inventory balance (assuming that the goods were received and invoice paid, if the goods were returned and invoice not paid, then the E-Invoice could be rejected)
- Discounts given after the E-Invoice is issued, these types of credit can refer to multiple Invoices, in that case instated of referencing the individual invoice the period or other references have to be used
- Purchase order exhausted - Credit note issued if goods are returned

Invoice can be processed but only after additional approval

- Delivery Charges exceeding tolerance limit
- Delivery charges incorporated on invoice, but not on PO or contract
- Purchase order exhausted – Invoice is paid if requestor wants to keep goods after PO is exhausted. Often, PO is amended to include additional delivery.

7.4.2. Invoice not received

Immaterial if it is a paper invoice or an Invoice, if an E-Invoice is not received by the trading partner for delivered goods or services, the E-Invoice receiver must request and obtain an invoice to proceed with their company accounting, this also holds true for self-billing where the Supplier must ensure to received the self billed Invoice.

On request of the party that should have received an E-Invoice, the E-Invoice issuer may make a copy of the E-Invoice already issued. Technical or process measures must be taken to ensure that such a copy E-Invoice can be clearly linked but distinguished from the Invoice. For example, the E-Invoice may include clear indication it is a ‘Copy’ or ‘Duplicate’ or equivalent appropriate term and the identifying reference to the E-Invoice that was not received.

Annex 1 E-Invoicing Compliance Guidelines Matrix

The Compliance Guidelines Matrix is downloadable from:

ftp://ftp.cen.eu/PUBLIC/CWAs/eInv2/Annex1_Compliance_Guidelines_Matrix_19102009.xls