CEN

WORKSHOP

AGREEMENT

CWA 16460

May 2012

ICS 35.240.60

English version

Good Practice: e-Invoicing Compliance Guidelines - The Commentary

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-CENELEC 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, Croatia, 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, Turkey 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 16460:2012 E

Contents

Foreword

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties on 2012-02-15, the constitution of which was supported by CEN following the public call for participation made on 2010-02-26.

A list of the individuals and organizations which supported the technical consensus represented by the CEN Workshop Agreement is available to purchasers from the CEN-CENELEC Management Centre. The following organizations endorsed this document:

- AITI, Italy
- CEGEDIM, France
- Dr. Otto Mueller Consulting, Switzerland
- FIR-DIG Consultants, Italy
- Hub2Hub, Italy
- ID Cyber-Identity Ltd, Switzerland
- InfoCert spa, Italy
- Legal Counsel, Stefan Engel-Flechsig, Germany
- OFS Portal LLC, USA
- Orange – France Telecom Group, France
- Sage France, France
- STS Group, Belgium
- Trustweaver, Sweden
- Voxel Group, Spain
- xft GmbH, Germany

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

The draft CWA was presented and discussed with industry representatives during two Open meetings, the first on September 22 and the other on December 12, 2011, both held in Brussels. The public comments period run from November 23, 2011 until January 23, 2012.

The final review/endorsement round for this CWA was started on 2012-04-04 and was successfully closed on 2012-04-16. The final text of this CWA was submitted to CEN for publication on 2012-04-18.

This CWA is part of a set of CWAs that has been prepared by Phase II and Phase III of CEN/WS e-Invoicing.

The overall target of Phase 3 is the “Integration of efforts in standardisation and developments” in the following areas:

1. Standards (e-invoicing modules for business software, methodology of software tools, functionalities and specifications for business software requirements)
2. Compliance (improvement of cooperation between companies and tax authorities, establishment of clear common understanding between companies and tax authorities in EU, accessibility of rules and regulation)
3. Implementation (best practice implementations with model agreements for electronic invoicing, model processes and SME focussed best practices)
4. Business Process (integration of electronic invoice in existing business processes).

This CWA covers the subject of project 2 and 4 listed above and is based on CWA 16047:2009, the original work of e-Invoicing Phase 2.

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.

The following CEN/WS eInvoicing III members have contributed to the work of this document:

Joost Kuipers	Leader	Netherlands Tax and Customs Administration *Belastingdienst*,
Christiaan van der Valk		TrustWeaver
Franco Ruggieri		FIR-DIG Consultants
Fabio Cavraro		Infocert
Isabelle Desmeytere		VAT Forum
Johan Borendal		TrustWeaver
Kevin Thornton		HM Revenue & Customs (HMRC)
Markus Gudmundsson	Technical Editor	Unimaze Software
Magali Kolnik		Sage France
Roger Nyberg		Ariba
Tony Nisbett		IBM/EDIFICE
William A. Le Sage		OFS Portal LLC

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN: Austria, Belgium, Bulgaria, Croatia, 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, Turkey and the United Kingdom.

Comments or suggestions from the users of the CEN Workshop Agreement are welcome and should be addressed to the CEN-CENELEC Management Centre.

1 Scope

1.1 General

The guidance set out in this CWA addresses electronic invoicing within the scope of VAT. In practice, this includes the majority of business-to-business sales/purchase transactions, but other types of transactions may also be involved. The regulatory background for the practices set out herein is the EU VAT Directive 2006/112/EC (1) as amended by Directive 2011/45/EU (2). Geographically, the practices set out herein are aimed at relevant invoices governed by at least one Member State's law transposing this Directive. The authors of this CWA document do not exclude that this CWA can be used to enhance or ensure compliance with similar requirements in other countries; however caution should be exercised in drawing parallels between EU rules and those of countries outside the EU.

Regulatory areas other than VAT are not specifically addressed in this CWA. The reader should remain cognisant of the fact that laws concerning the protection of personal data, corporate governance, customs, accounting and taxes other than VAT may impose different or additional requirements on electronic invoices.

The CEN Code of Practice (3) also published as part of this workshop (CWA 16463) provides a high level overview of legal requirements, while this guidance gives more detailed information on implementing E-Invoice processes.

1.2 Objectives

This CWA aims to inform and guide stakeholders in the setting up, operating and auditing of electronic invoicing processes and systems in accordance with requirements applicable under VAT law.

1.3 Target audience

The Guidelines are addressed to:

- Entities 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.

1.4 Guidelines as voluntary self-regulation

These 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.

These 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 with regards to technologies and processes companies may choose to adopt.

2 Introduction

2.1 Overall Summary

This section summarizes the key principles and recommended practices for the sending, receiving and storage of electronic invoices in the European Union with a view to maintaining a robust normative foundation on which both taxable persons and tax administrations can build their processes and coordinate their interactions in a cost- and time-effective manner.

An invoice must correctly reflect the actual supply of goods and/or services. This is achieved through business controls establishing a reliable audit trail linking invoices and supplies.

Those same business controls establishing reliable audit trails linking invoices and supplies may also meet the requirement of the authenticity of origin and integrity of content of the electronic invoice.

In some circumstances, the business controls used by a taxpayer may not be enough to demonstrate the authenticity of the origin and integrity of content of the electronic invoice[1].

The authenticity of the origin and integrity of content of the electronic invoice may also be demonstrated by other means, such as those mentioned in Article 233 (2).

2.2 Core Principles

Legislative compliance: Electronic invoicing solutions must comply with the relevant legislation. In the EU, the primary legislation is Directive 2006/112/EC (1) (as amended by 2010/45/EU (2)), specifically Articles 233 and 247. In essence; the authenticity of origin, the integrity of content, and legibility must be ensured for the life of an invoice and the use of an electronic invoice shall be subject to acceptance by the recipient. In practical terms this will mean that a business will have:

- An invoice which supports either an amount of VAT payable to or recoverable from a tax administration.
- Evidence to demonstrate authenticity of origin of the invoice.
- Evidence to demonstrate integrity of content of the invoice.
- Measures to ensure legibility of the invoice.

Technology neutrality: Use of particular technologies is not a precursor to adoption of electronic invoicing and no indication should be given that one technology is favoured over another. Trading parties have freedom of choice over current and future electronic invoicing solutions to meet their specific business needs consistently with the applicable legislative obligations.

Auditability: Businesses should be able to demonstrate and explain within a reasonable time their administrative and control capability to meet legal requirements. Businesses should maintain a legally compliant audit trail, including the underlying transaction data and any relevant supporting documentation and data, which must be accessible towards external auditors, both statutory and tax.

Proportionality: Businesses should not be required to implement control measures for audit and/or compliance purposes that are disproportionate to their individual circumstances. Circumstances that must be taken into account include, but should not be limited to, the size of a company, the nature of its business, the value and frequency of its transactions, its number of trading partners and the stability of its trading partner network.

2.3 Ensuring Authenticity & Integrity

"Authenticity of the origin" of an E-Invoice means the assurance of the identity of the supplier or the issuer of the invoice.

"Integrity of content" of an E-Invoice means that the content required according to Directive 2010/45/EU Article 233 (2) has not been altered.

---

1 Business controls should be appropriate to “the size, activity and type of the taxable person and should take account of the number and value of transactions as well as the number and type of suppliers and customers” [DG Tax Guidelines] (43).

In the EU, Directive 2010/45/EU (2) art. 233 states that "*Each taxable person shall determine the way to ensure the authenticity of the origin, the integrity of the content and the legibility of the invoice*". There are many way in which this can be achieved. The Directive gives three examples of approaches that can be used:

- Business controls which create a reliable audit trail between an invoice and a supply of goods or services.
- Electronic data interchange (EDI).
- Qualified electronic signature.

For reference purposes this and related documents categorise different approaches to ensuring authenticity and integrity by their inherent characteristics. Current categories are below (and more detailed description can be found elsewhere in this document):

- Class A - business controls which create a reliable audit trail between an invoice and a supply of goods or services.
- Class B – controls over data exchange process, i.e. EDI.
- Class C – data level control, i.e. advanced / qualified electronic signatures.
- Class D – sealed environments.

The following diagram illustrates the relative considerations for ensuring authenticity and integrity for each of these classes.

<table>
<tr><td colspan="4">Authenticity & Integrity Compliance</td></tr>
<tr><td>Class A
Business Controls</td><td>Class B
Transport Controls</td><td>Class C
Data Controls</td><td>Class D
Sealed Environment</td></tr>
<tr><td>Storage of Evidence to Demonstrate Authenticity & Integrity, e.g. historical audit trail proving the supply</td><td>Storage of Evidence to Demonstrate Authenticity & Integrity, e.g. historical EDI exchange & contract evidence</td><td>Storage of Evidence to Demonstrate Authenticity & Integrity, e.g. electronic signature and ability to verify</td><td>Storage of Evidence to Demonstrate Authenticity & Integrity, e.g. evidence of sealed-off environment</td></tr>
<tr><td>Additional Business Controls (as may be required) to Ensure Integrity</td><td rowspan="2">Controls to Ensure Authenticity & Integrity during storage</td><td rowspan="2">Electronic Signature Controls To Ensure Integrity</td><td rowspan="2">Environment Controls To Ensure Integrity</td></tr>
<tr><td>Additional Business Controls (as may be required) to Ensure Authenticity</td></tr>
<tr><td>Typical Business Invoicing Processes, Controls & Audit Trail</td><td>Controlled Exchange Controls To Ensure Authenticity & Integrity</td><td>Electronic Signature Controls To Ensure Authenticity</td><td>Environment Controls To Ensure Authenticity</td></tr>
</table>

An electronic invoicing solution does not need to fit entirely within one of the above classes to be compliant. For example, it would be perfectly reasonable for trading partners to agree to use class A for authenticity and class C for integrity. In such a case, applying the proportionality principle, a qualified electronic signature as defined in the Directive might be disproportionate and a 'lesser' electronic signature would be sufficient to ensure integrity. Likewise, the business controls would only need to be evaluated in respect to their contribution towards authenticity.

2.4 Ensuring Legibility

To be legible an invoice must be human-readable, which means an auditor (e.g. Tax Administration or accountant) is able to interpret the content of an E-Invoice.

An invoice must be legible, in particular for auditors including tax administrations. Businesses should maintain software that is capable of rendering an electronic invoice legible. Legibility is a precondition for acceptance by the recipient and auditability. Legibility of an electronic invoice can be achieved either because the file format was meant to enable human-readability in connection with desktop software, or through the application of viewer software in case of invoice formats meant for machine-to-machine communications.

3 Comprehensive Guidance

3.1 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 Compliance Matrix was originally developed from 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[2] 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 likely to be 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 Customer as well as self-billing) and provide detailed process guidance for a variety of implementation options, the use of various methods for ensuring integrity and authenticity and the storage 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 a more detailed view – for example: What are good practices for a Supplier in a self-billing process? What should Customers and Suppliers need to take into consideration when starting exchanging E-Invoices? Use of the Compliance Matrix and the Interactive User Interface is addressed in section 3.9 below and in the Introduction of the Matrix document.

The issues surrounding self-billing are presented in more detail in section 3.8.1, 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.

3.2 Process Model

The process model that has been used to analyse 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 Customer on the right.

This model is used as a tool for analysing 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.***

Figure 1 represents the process model without involving Service Providers; Figure 2 introduces the concept of Service Provider (or providers) into the model. The labelling on the figures is referenced in the Compliance Matrix and the Interactive User Interface.

[2] Decision No 1482/2007/EC of the European Parliament and of the Council of 11 December 2007 established a Community programme to improve the operation of taxation systems in the internal market (Fiscalis 2013)

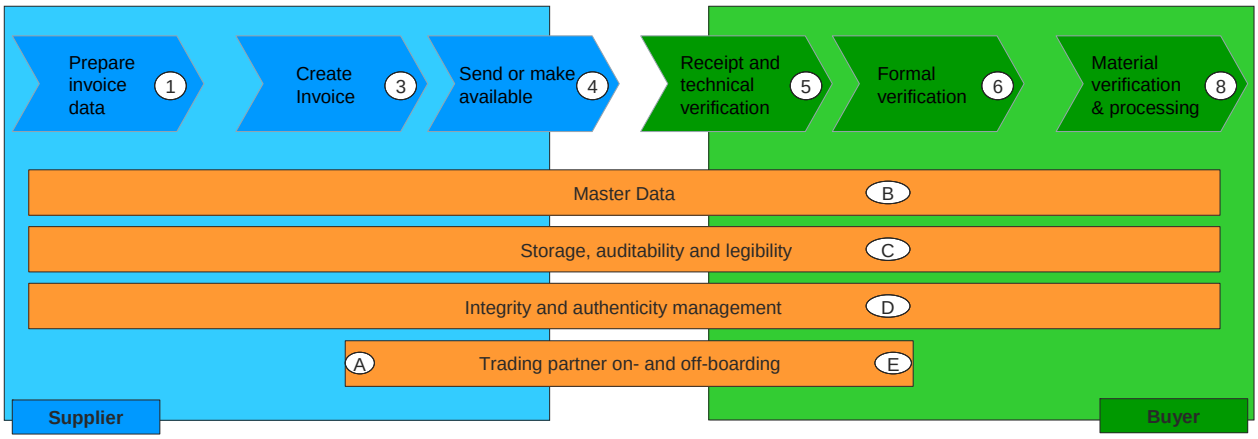


Figure 1 - Process Model

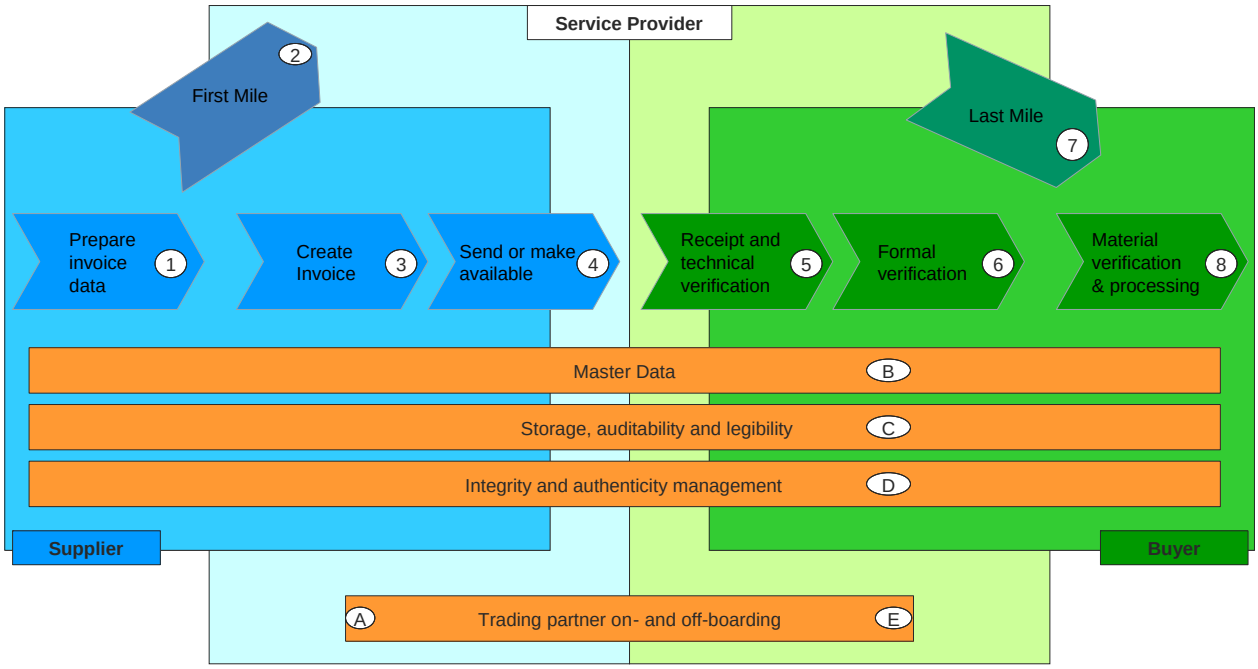


Figure 2 - Process Model with Service Provider involvement

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 Customer.

In the case of self-billing, the E-Invoice is issued by the Customer (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.

3.2.1 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:

i) When preparing the sales invoice.

a) Continuity and consistency between the information used in an invoice and its source (e.g. sales orders, delivery notes, contracts).

ii) When creating the sales invoice.

a) Ensure that the authenticity of the invoice will be verifiable by the customer
b) Ensure that the integrity of the invoice will be verifiable by the customer and supplier

iii) When sending invoices or making them available

a) Authenticity of the invoice remains verifiable upon receipt
b) Integrity of the invoice remains verifiable upon receipt

iv) When receiving an invoice and processing it

a) Continuity between all steps of the process concerned with handling a received invoice
b) Authenticity of the invoice is verified and maintained
c) Integrity of the invoice verified and maintained

v) When storing an invoice and during the storage period

a) Data continuity between invoice creation or receipt and its storage
b) Verifiable authenticity of the invoice ensured throughout storage period
c) Verifiable integrity of the invoice ensured throughout storage period
d) An invoice must be presentable in a legible form.

vi) Across the invoicing process

a) Invoices are handled in accordance with applicable law throughout every stage of their life cycle

3.2.2 (On and Off) Boarding steps

Prior to exchanging E-Invoices, the trading partners first have to agree on the legal basics, then on the specific types of electronic invoices to be exchanged; in particular they will have to agree on formats, on exchanging mechanisms and on methods to ensure Authenticity, Integrity and Legibility. This process called “on-boarding” may span from being very simple (e.g. just a click on a tick box) to very complex, including technical, procedural and legal basics of the E-Invoicing relationship. Similarly, specific “off-boarding” procedures should be ensured, to wind down the relationship in good order when it becomes necessary. If one or more Service Providers are involved, the on- and off-boarding processes are 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, and, where applicable 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. Among other things, this step is necessary to give the E-Invoice issuer reasonable confidence that the recipient will accept the E-Invoice, as envisaged by Directive 2006/112/EC art. 232 (1) as amended by Directive 2010/45/EU (2).

E. Trading partner off-boarding

Off-boarding is the process of terminating an E-Invoicing relationship. The parties terminating the relationship should ensure a winding-down of the relationship that preserves the trading partners’ ability to maintain the required authenticity, integrity, legibility and auditability of their E-Invoices until the end of the storage period. The complexity of the off-boarding process can span from practically nil to a complicated process, in particular if the off-boarding procedure involves a service provider.

3.2.3 Processing steps

The processing steps in the exchange of the E-Invoice are expanded upon below. Labelling is the same as is used in the Compliance Matrix the Interactive User Interface.

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 data 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, 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 should have performed all the controls required to ensure that the resulting E-Invoice will be complete and accurate.

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. This is commonly known as “issuing the E-invoice. The Supplier or its Service Provider will often start this process by initiating technical controls that should be checked by the Recipient or its Service Provider in order to correctly 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 Recipient, 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) defined at syntax level. Anomalies will generally be recorded and signalled to the Recipient’s system controller. Only technically correct files/invoices will be passed to the next processing step. In case of a technical problem, the Issuer 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, etc.

Only formally correct files/invoices will be passed to the next processing step. If a formal problem occurs the Issuer will be notified that the E-Invoice could not be accepted and a corrected E-Invoice should be sent.

7. 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. Customer 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 Recipient’s application.

If an error is detected at this level, the Issuer 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.

3.2.4 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 Recipient's in-house application for further processing. The E-Invoice will typically be communicated through a secure channel.

3.2.5 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 3.4 and 3.5), measures should be taken to ensure that the historically correct data are stored for each invoice to allow for such completion or reproduction.

C. Storage and auditability

Both parties must store the E-Invoice for the storage period. The storage may be either at a Trading Partner or at a Service Provider. During the storage period, a competent tax administration has the right to audit stored Invoices. Invoices 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, authenticity and legibility 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-Invoices. 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 and/or reproducible conversions.

Legibility is required to be maintained up to the end of the E-Invoice storage period. It cannot be ensured by the methods implemented to ensure Authenticity and Integrity.

The following issues should be taken into account:

1) Adoption of E-Invoice formats that are likely not to host malware able to change the document content and presentation;

2) Adoption of formats for which long term maintenance can be assured.

If either of the above are not met, it will be necessary to perform a format conversion that shall be implemented in a way to create a reliable audit trail.

3.3 Categorisation of Business Implementations

These Guidelines allow for the use of a wide choice of alternative controls to meet the Core Principles identified in section 2.2. Whilst a broad spectrum of business solutions supporting E-invoicing is possible

through the Guidelines, they can be broadly categorised into four classes to which the controls recommended in the Guidelines may be related.

The following categorisation assumes and builds on a minimum level of basic E-Invoicing processes. 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:

A) Class A is the “business controls that create a reliable audit trail between invoice and supply” as per Directive 2006/112/EC (1) Art. 233, as amended by 2010/45/EU (2);

B) Business solutions augmented by controlled data exchanges (e.g. EDI) to ensure the integrity and authenticity of E-Invoices between trading partners;

C) Business solutions augmented by data level controls (e.g. Qualified Electronic Signatures) to ensure the integrity and authenticity of E-Invoices throughout their full life-cycle;

D) Business solutions augmented by central "safe-keeping" of E-Invoices to ensure the integrity and authenticity of E-Invoices throughout their full life-cycle;

Further classes may be added as business practices are identified or evolve. Please note that the above classes are only defined to make the matrix and interface more accessible. In practice compliance methodologies could fall into multiple classes.

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 Customer uses a class A solution (exclusive reliance on process controls). It is nevertheless important that the manner in which the Invoices are exchanged is clearly agreed between the parties in order to avoid mismatches.

As described in section 3.9, for each control (requirement) described in the Matrix or Interactive User Interface, it is indicated whether it is applicable as a Class A business control, Class B Controlled data exchange, Class C data level control or Class D outsourced “safe-keeping”.

3.4 Class A: Business controls creating a reliable audit trail between invoice and supply

3.4.1 Definitions

(a) **Business Control:** The COSO[3] Model defines “business control” as:

a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

(b) **Audit Trail:** An audit trail[4] is:

a paper and/or electronic record that gives a step by step documented history of a transaction, which can validate or invalidate accounting entries. Components of an audit trail include: (i) source records, (ii) list of transactions processed and (iii) transaction identifiers so that reference can be made to the source of a transaction.

3.4.2 Introduction

An invoice must correctly reflect the actual supply of goods and/or services. This is achieved through business controls establishing a reliable audit trail linking invoices and supplies. Those same business controls may also meet the requirements of the authenticity of origin and integrity of content of the electronic

3 COSO: Committee of Sponsoring Organizations comprising American Accounting Association, American Institute of Certified Public Accountants, Financial Executives International, The Association for Accountants and Financial Professionals in Business, and The Institute of Internal Auditors.

4 This definition is an amalgamation from a number of sources.

invoice. This section examines practical examples, based on established business processes and controls, which fulfil these requirements. These business processes and controls are based on those already used for paper invoicing.

Legibility is treated separately within this CWA as the issue is common whatever mechanism is used to achieving authenticity and integrity.

3.4.3 Reliable Audit Trail

Directive 2010/45/EU references the use of reliable audit trails between invoice and supply as a means of also demonstrating invoice authenticity and integrity for electronic invoices. Examples of different types of audit trail that contribute to fulfilling this purpose include:

(i) The audit trail of documents produced by an ERP (Enterprise Resource Planning application software) or any application software that provided the type of business processing discussed therein, i.e. billing systems, procurement systems, financial systems, etc (henceforth the term ERP will be used to represent all these systems). It presumes the existence of cross-referencing between the audit trail documents.
(ii) An audit log of changes made to the ERP documents mentioned above during their life cycle.
(iii) An audit log of changes made to ERP master data that is reference during invoicing processing.
(iv) An audit log of activities performed by the ERP, such as the act of matching a purchase order with an invoice.

The purposes of these audit trails are to:

- Confirm that an invoice represents an actual supply.
- Provide independent verification of authenticity of an invoice and its representation in the ERP.
- Provide independent verification of integrity of content of an invoice and its representation in the ERP.

The practical application of these audit trails and what they need to contain will be examined in more detail later in this section.

For an audit trail to be reliable there are two main considerations:

(i) The data and documents contained within it. These need to be of sufficient detail to ensure that the audit trail is fit for purpose. In terms of this CWA a specific purpose is to ensure authenticity and integrity.
(ii) The quality of the data within the audit trail. This quality - can be achieved through any of the following means:
    - Reference to third party documents, e.g. bank statements.
    - Reference to second party documents, e.g. order or goods movement documents, contracts signed by both parties.
    - Internal controls creating independence between documents in the audit trail, e.g. segregation of duties or procedural controls such as purchase orders being created in advance of receipt of invoice

The applications of these techniques for ensuring audit trail reliability will vary depending on a business' individual circumstance and the systems and processes in use. A billing system reliant on master data to accurately produce invoices will need business controls to ensure that the standing/master data is correctly maintained. Whereas, for processes with less scope for business internal controls greater reliance will need to be placed on third and second party documents.

3.4.4 Typical business processes

Business controls and/or audit trails are a function of business processes and their contribution to E-Invoice authenticity & integrity should be considered within the context of the business process. Most business processes that result in the issue of an E-Invoice, or process an E-Invoice received, can be grouped into representative types that have shared characteristics from the perspective of invoice authenticity and integrity. These representative types, described below, are separated into sales and purchasing processes (self-billing is outside-the-scope of this section):

Sales processes

- Order-to-Cash (goods)
  - This represents the process that supports sales of inventoried goods, typically: sales order → goods dispatch note → sales invoice → payment receipt.
- Order-to-Cash (services)
  - This represents the process that supports billing of services supplied, typically: service contract → billing schedule → sales invoice → payment receipt.
- Invoice-to-Cash
  - This represents the process that supports billing of supplies not covered by the above examples, typically: invoice requisition → invoice → payment receipt. These are often supplies outside the usual supply chain.

Purchasing processes

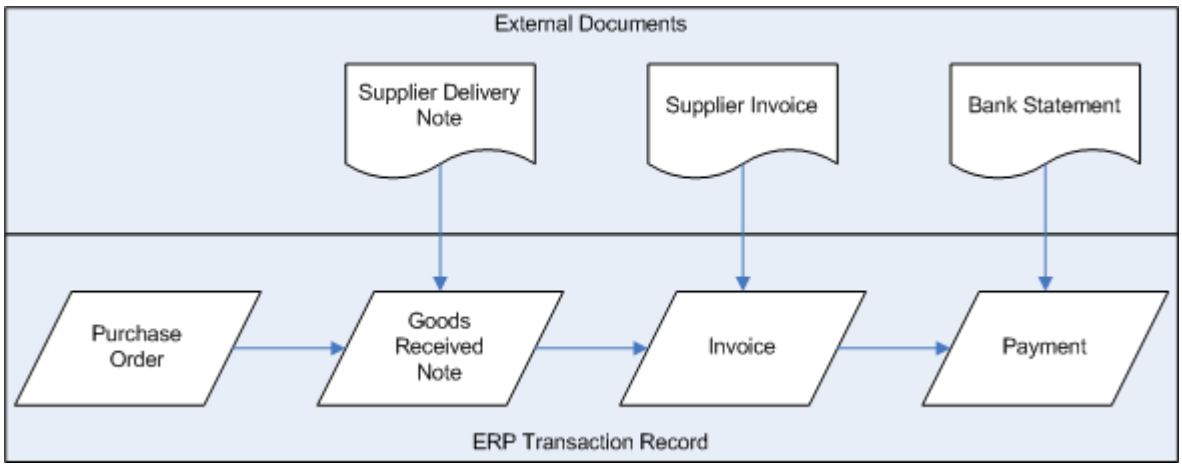
- Procure-to-Pay (3-way matching[5])
  - This represents the process that supports purchase of goods or services where the 3-way match control is implemented, typically: purchase order → goods received note/service received note → purchase invoice → payment.
- Procure-to-Pay (2-way matching[6])
  - This represents the process that supports purchase of goods or services where the 2-way match control is implemented, typically: purchase order → purchase invoice → payment.
- Invoice-to-Pay
  - This represents the process for procurement of supplies where neither 3-way nor 2-way matching is used, typically: purchase invoice → payment.

Each of these processes consists of a sequence of events, as described. The description uses generic terminology and the event may well be referred to differently within a particular organisation but the purpose will be equivalent. Table 11 provides a list of all events referred to with a description of the event's function as an aid to identifying equivalence. Also, an organisation may have additional events within their processes that can also contribute to demonstrating authenticity and integrity. Other equivalent alternative events may exist that do not leave an audit trail, for example verbal orders. In these cases particular attention should be paid to other trailing events in the process chain.

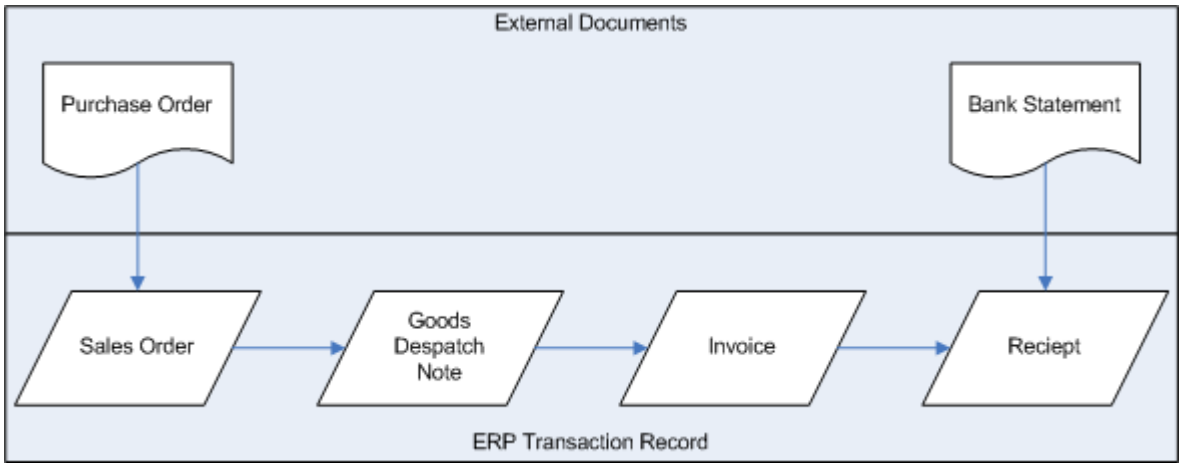
An electronic record of each of these events will usually be created in the ERP system. This record may directly contain values relating to the event, e.g. quantities, or reference master data to provide or derive content, e.g. pricing. It is this record of the sequence of events in the process that contributes to an audit trail. An audit trail will consist of documents outside the ERP and a transaction record within the ERP. For example, the audit trail for the 'procure-to-pay' cycle will often take the following form.

5 3-way matching refers to the control of comparing purchase order; goods received note and purchase invoices, or similar equivalent documents.

6 2-way matching refers to the control of comparing purchase order and purchase invoice, or similar equivalent documents.



The equivalent audit trail for an ‘order-to-cash’ cycle is.



Within the audit trail an invoice exists as an invoice in it own right and as a representation of the invoice’s content within the invoice record in the ERP system. The ERP invoice record will not only contain data derived from the invoice but also supplementary data created by the ERP. This supplementary data is independent of the invoice and can therefore be used within authenticity and integrity verification. However, those parts of the ERP invoice record that contain the VAT content of an invoice are derived directly from the invoice and are therefore not independent, thus they cannot be used for authenticity and integrity verification.

The audit trail for the invoice-to-cash and invoice-to-pay cycles is weaker than that for the other cycles and therefore authenticity and particularly integrity is more problematic to demonstrate. However, these cycles would typically indicate one-off/irregular trading and would therefore, because of the need to obtain the acceptance of the customer and other E-Invoicing start-up costs, be rather less attractive for E-Invoicing. Nonetheless, there may be scenarios where E-invoicing is required in invoice-to-cash and invoice-to-pay cycles. In these circumstances alternative controls, beyond the audit trail, may need to be used. Examples of these alternative controls are provided; see tables 1 through 11 in section 3.4.10.

Many purchasing, and some sales processes, will include an authorisation workflow. Although these may control the validity of the supply, they do not provide any additional audit trail component other than a record of it actually being done.

3.4.5 Authenticity of an electronic invoice

Although verification of authenticity is associated with something the invoice recipient needs to demonstrate, there is a responsibility on the invoice issuer to ensure that the invoice has sufficient attributes to support the recipient in their obligation. This will often be data beyond that required by the VAT Directive, for example, the customer may require inclusion of their purchase order number as an invoice attribute to support

integration into their audit trail. Such requirements should be established during the on-boarding process (see section 3.2.2).

3.4.6 Integrity of an electronic invoice

Directive 2010/45/EU (2) requires the integrity of certain specified invoice components to be maintained; those components that are required by virtue of Article 226. These invoice components can be divided into those that commonly occur on invoices and those that are circumstance specific. The common components are: Supplier (name, address & VAT ID); Customer (name, address & VAT ID); invoice date; date of supply; invoice number; quantity and nature of supply; taxable amount; vat rate; vat amount, and currency. Although currency is not specifically mentioned by Article 226 its requirement is implied to give a context to taxable and VAT amounts. Only these common components are addressed in this document. However, the principles discussed here could also be extended to the other circumstance specific components.

In examining E-Invoice integrity it is important to recognise that some invoice components have dependencies on others; for example, if there is sufficient integrity control over taxable amount and VAT rate it can be assumed that integrity of VAT amount is also sufficient

To demonstrate integrity of the above E-Invoice common components the baseline assumed in this document is that the value of the component is verifiable against at least one independent source, for example the gross value on an invoice would be verifiable against the equivalent payment value shown on a bank statement.

3.4.7 Achieving authenticity & integrity

Table 1 illustrates how different elements of sales process audit trail documents and master data may contribute to invoice authenticity and integrity. Table 6 is the equivalent of Table 1 for purchasing. A '✓' in the grid indicates that values held in that component of the audit trail may be used, either directly or indirectly, to derive that value on the invoice.

Although the processes described in Table 1 & Table 6 are typical, the exact detail of their content will vary depending on ERP system and business implementation and therefore the grid analysis is based on a number of assumptions. What these assumptions are will become clear in the next stage of analysis where authenticity and integrity for each of the cycles is examined in detail.

Organisations may have additional events within their business process which result in additional audit trail documents. The grids in figures 1 & 2 can be adapted to incorporate the additional audit trail documents and used to analyse the impact of them on demonstrating authenticity and integrity.

Business controls creating a reliable audit trail (as defined in section 3.4.3) are sufficient to establish authenticity and integrity. Businesses are free to use business controls creating a reliable audit trail to ensure authenticity and integrity. This document provides guidance on ensuring the selected business controls will create a reliable audit trail.

There may be occasions where the audit trail is not reliable and therefore insufficient to guarantee authenticity and integrity; for example when the data, documents or quality controls described in section 3.4.3 are deficient. When this occurs, other business controls can be utilised to fill the gaps. In areas where the audit trail alone is more likely to be insufficient, examples of these alternative business controls are provided within this document. These alternative business controls may not have the equivalent degree of reliability as an audit trail and should therefore be viewed as supplementing the audit trail rather than replacing it. Alternatively, businesses are free to use technological means, e.g. EDI or QES/AdES, for ensuring authenticity and integrity.

3.4.8 Achieving authenticity & integrity in sales process

Table 2, Table 3, & Table 4 provide a detailed analysis of how sales process audit trails and business controls contribute to authenticity and integrity for each of the previously described sales cycles. Not all audit trail components will be present in every scenario.

Table 5 provides illustrative types of business controls objectives that the system would need to meet to ensure the reliability of the audit trail. The business control objectives against an audit trail component only need to be met if reliance is being placed on that audit trail component in demonstrating authenticity and integrity. The controls required to meet these control objectives should be proportional to the business transaction being controlled. The business control objectives listed have been structured to be compatible

with other business control resources; for example, those published by the IT Governance Institute in their IT Control Objectives for Sarbanes-Oxley, 2nd Edition.

3.4.9 Achieving authenticity & integrity in purchase process

Table 7, Table 8, and Table 9 provide a detailed analysis of how purchase process audit trails and business controls contribute to authenticity and integrity for each of the previously mentioned purchase cycles. Table 10 provides the purchasing equivalent of Table 5 and the comments thereon equally apply to this item.

The document matching process in 3-way and 2-way matching is valuable in demonstrating authenticity and integrity and providing an audit trail between invoice and supply. The effectiveness of the matching process is dependent on appropriate tolerances, i.e. acceptable differences between values on the matched documents, being used within the matching process. Tolerances set disproportionately high for the type and value of supply will reduce the reliability of the matching process and impact on the suitability of the audit trail for verifying authenticity and integrity.

Although payment is included in the purchase process audit trail analysis, its contribution to authenticity and integrity is restricted. Payment and other post-invoice receipt events will reference values derived directly from the invoice. Unless the authenticity and integrity of the invoice has been ensured, post-invoice receipt events could be referencing inaccurate data. Payments and other post-invoice receipt events can only be used for ensuring authenticity and integrity if the authenticity and integrity of the invoice has previously been ensured. Without this, a payment can provide evidence that a supply has been received, but not necessarily the identity of the Supplier or value of the supply.

In the scenario where unplanned delivery cost and other similar unanticipated charges are included on an invoice the invoice will initially fail integrity checking. Additional processes would need to be used to verify these types of costs.

3.4.10 Storage

The authenticity and integrity of an invoice must be ensured throughout its life-cycle. This means that not only must the invoice be stored; any documentation that is referenced to ensure authenticity and integrity must also be stored in any form as required for an equivalent period. This documentation includes (but not exhaustively):

(1) Internal business records generated during the invoicing processes, i.e. contracts, sales/purchase order, goods receipt/dispatch notes..
(2) External documents received during the invoicing processes, i.e. purchase orders, goods dispatch notes, bank statements.
(3) Historic master data.
(4) Evidence of controls to ensure data quality.

3.4.11 Tables

Table 1 - Audit Trail Contribution to Integrity in Sales Processes

Sales Process Audit Trail & Master Data	Integrity												
	VAT ID Supplier	Supplier (Name + Address)	VAT ID Customer	Customer (Name + Address)	Invoice Date	Date of Supply	Invoice Number	Nature of Supply	Quantity	Taxable Amount	VAT Rate	VAT Amount	Currency
Order-to-Cash (goods)													
Sales Contract	✓	✓		✓				✓		✓			✓
Sales Order	✓	✓		✓				✓	✓	✓			✓
Goods Dispatch Note	✓	✓		✓		✓		✓	✓				
Invoice					✓								
Cash Recipt				✓			✓			✓		✓	✓
Customer Master Data			✓								✓		
Material (Supply) Master Data											✓		
Pricing Master Data										✓			
VAT Determination Data											✓		
Other business controls							✓					✓	
Order-to-Cash (services)													
Service contract	✓	✓		✓	✓			✓		✓			✓
Billing Schedule / Timesheets / etc	✓	✓		✓		✓		✓		✓			✓
Invoice					✓								
Cash Recipt				✓			✓			✓		✓	✓
Customer Master Data				✓									
Material (Supply) Master Data													
Pricing Master Data													
VAT Determination Data											✓		
Other business controls							✓						
Invoice-to-Cash													
Sales invoice requisition	✓	✓		✓				✓	✓	✓			✓
Invoice					✓								
Cash Recipt				✓			✓			✓		✓	✓
Customer Master Data													
Material (Supply) Master Data													
Pricing Master Data													
VAT Determination Data											✓		
Other business controls							✓						

Table 2 - Authenticity & Integrity in an Order-to-Cash (goods) Cycle

Authenticity / Integrity Invoice Component	Audit trail component	Audit trail component contribution to A&I
Authenticity	Invoice	Inclusion of attribute to facilitate referencing of supply in customer's ERP, e.g. customer's purchase order number.
VAT ID Supplier / Supplier Name & address	Sales contract	Company data in contract linked to ERP company master data.
	Sales order	Company data in order linked to ERP company master data.
	Goods Dispatch Note	Dispatch location linked to ERP company master data.
VAT ID Customer/ Customer Name & Address	Sales contract	Business records will contain a customer account reference providing a link back to ERP customer master data.
	Sales order	Business records will contain a customer account reference providing a link back to ERP customer master data.
	Goods Dispatch Note	Business records will contain a customer account reference providing a link back to ERP customer master data.
	Cash receipt	Receipts allocated to invoices will identify the payer.
	Customer master data	Maintains correlation between customer account/name/VAT ID (where required).
Invoice Date	Invoice	The posting date of the invoice record in the ERP will correlate with the invoice date.
Date of supply	Goods Dispatch Note	GDN date will correlate with date of supply on invoice.
Invoice number	Cash receipt	Remittance advice may reference invoice number for receipt allocation.
	Other business controls	Required control objective 'All invoices issued are recorded'. ERP system allocates invoice numbers within a controlled sequence.
Nature of supply	Sales contract	Will contain a record of what is to be supplied either as text or a material code referencing the material master data.
	Sales order	Will contain a record of what is to be supplied either as text or a material code referencing the material master data.
	Goods dispatch note	Will contain a record of what has been supplied either as text or a material code referencing the material master data.
Quantity	Sales order	Will contain a record of how much material has been requested.
	Goods dispatch note	Will contain a record of how much material has been supplied.
Taxable amount	Sales contract	Will quote the value of the supply.
	Sales order	Will quote the value of the supply. (This assumes that sales order pricing and billing pricing are the same. Some ERPs provide functionality for the order and billing pricing to be different as this is a requirement of certain industries)
	Cash receipt	Cash receipt value correlates with the sum of taxable & VAT amounts.
	Price list	Can be used to derive a value of the supply if not held against order. Also, may provide prices outside contract/order such as delivery charges.
VAT Rate	Customer Master Data	ERP will typically use data in each of these three areas to derived VAT rate.
	Material Master Data	
	VAT Determination Data	
VAT Amount	Cash receipt	Cash receipt value correlates with the sum of taxable & VAT amounts.
	Other business controls	The order-to-cash cycle provides sufficient integrity over taxable amount & VAT rate for integrity of VAT amount to be inferred.
Currency	Sales contract	Billing currency will be agreed within contract/order.
	Sales order	
	Cash receipt	Cash currency may provide an indication of invoice currency.

Table 3 - Authenticity & Integrity in an Order-to-Cash (services) Cycle

Authenticity / Integrity Invoice Component	Audit trail component	Audit trail component contribution to A&I
Authenticity	Invoice	Inclusion of attribute to facilitate referencing of supply in customer's ERP, e.g. customer's purchase order number.
VAT ID Supplier / Supplier Name & address	Service Contract	Company data in contract linked to ERP company master data.
	Billing Schedule	Company data in schedule linked to ERP company master data.
VAT ID Customer / Customer Name & Address	Service Contract	Business records will contain a customer account reference providing a link back to ERP customer master data.
	Billing Schedule	Business records will contain a customer account reference providing a link back to ERP customer master data.
	Cash Receipt	Receipts allocated to invoices will identify the payer.
	Customer Master Data	Maintains correlation between customer account/name/VAT ID (where required).
Invoice Date	Service Contract	Service contract may define a billing frequency
	Invoice	The posting date of the invoice record in the ERP will correlate with the invoice date.
Date of Supply	Timesheets	May provide record of what was done when.
Invoice Number	Cash Receipt	Remittance advice may reference invoice number for receipt allocation.
	Other Business Controls	Required control objective 'All invoices issued are recorded'. ERP system allocates invoice numbers within a controlled sequence.
Nature of Supply	Service Contract	Will contain a record of what is to be supplied.
	Billing Schedule	Will contain a record of what is to be supplied.
Quantity		
Taxable Amount	Service Contract	Will quote the value of the supply.
	Billing Schedule	Will quote the value of the supply.
	Cash Receipt	Cash receipt value correlates with the sum of taxable & VAT amounts.
VAT Rate		
VAT Amount	Cash Receipt	Cash receipt value correlates with the sum of taxable & VAT amounts.
Currency	Service Contract	Billing currency will be agreed within contract.
	Billing Schedule	Billing currency will be agreed within contract.
	Cash Receipt	Cash currency may provide an indication of invoice currency.

Table 4 - Authenticity & Integrity in an Invoice-to-Cash Cycle

Authenticity / Integrity Invoice Component	Audit trail component	Audit trail component contribution to A&I
Authenticity	Invoice	Inclusion of attribute to facilitate referencing of supply in customer's ERP, e.g. customer's purchase order number.
VAT ID Supplier / Supplier Name & address	Sales Invoice Requisition	
VAT ID Customer / Customer Name & Address	Sales Invoice Requisition	Will record the recipient of the supply (may not exist as a customer master record).
Invoice Date	Invoice	The posting date of the invoice record in the ERP will correlate with the invoice date.
Date of Supply		
Invoice Number	Cash Receipt	Remittance advice may reference invoice number for receipt allocation.
	Other Business Controls	Required control objective 'All invoices issued are recorded'. ERP system allocates invoice numbers within a controlled sequence.
Nature of Supply	Sales Invoice Requisition	Will contain a record of what has been supplied
Quantity	Sales Invoice Requisition	Will contain a record of what has been supplied
Taxable Amount	Sales Invoice Requisition	Will quote the value of the supply.
	Cash Receipt	Cash receipt value correlates with the sum of taxable & VAT amounts.
VAT Rate		
VAT Amount	Cash Receipt	Cash receipt value correlates with the sum of taxable & VAT amounts.
Currency	Sales Invoice Requisition	Will contain billing currency.
	Cash Receipt	Cash currency may provide an indication of invoice currency.

Table 5 - Illustrative Business Control Objectives for Sales Process Audit Trail

Audit Trail Component	Business Control Objectives
Sales Contract	
Service contract	
Sales Order	Orders and cancellations of orders are input accurately.
	Order records cannot be changed post goods dispatch/invoice.
Goods Dispatch Note	Shipments are recorded accurately.
	Shipments are recorded promptly and in the appropriate period.
	Inventory is reduced only when goods are shipped with approved customer orders.
	Goods Dispatch Note records cannot be changed post invoice.
Billing schedule	
Sales invoice requisition	Segregation of Duties between invoice requisition and invoice creation.
Invoice	Order entry data are transferred accurately to the invoicing activity.
	Invoices are generated using authorized terms and prices.
	Invoices are accurately calculated and recorded
	Invoices relate to valid shipments or services.
	All invoices are issued.
	All invoices issued are recorded.
	Invoices are recorded in the appropriate period.
Cash Receipt	Cash receipts are recorded in the period in which they are received.
	Cash receipts data are entered for processing accurately.
	Early settlement discounts are accurately calculated and recorded.
Customer Master Data	The customer information, such as name, address & VAT registration number, in master file is maintained.
	Only duly authorised changes are made to the customer name, address & VAT registration number in master file.
	All valid changes to customer name, address & VAT registration number in master file are input and processed.
	Changes to customer name, address & VAT registration number in master file are accurate.
	Changes to customer name, address & VAT registration number in master file are processed in a timely manner.
	Customer name, address & VAT registration number in master file data remain up to date.
	A record of changes made to customer name, address & VAT registration number in the master file data is maintained
	The VAT coding in customer master file is maintained.
	Only valid changes are made to VAT coding in the customer master file.
	All valid changes to VAT coding in the customer master file are input and processed.
	Changes to VAT coding in the customer master file are accurate.
	Changes to VAT coding in the customer master file are processed in a timely manner.
	VAT coding in Customer master file data remain up to date.
	A record of changes made to VAT coding in customer master file is maintained.
	The customer billing currency in master file is maintained.
	Only valid changes are made to the customer billing currency number in master file.
	All valid changes to the customer billing currency in master file are input and processed.

	Changes to the customer billing currency in master file are accurate.
	Changes to the customer billing currency in master file are processed in a timely manner.
	Customer billing currency in master file data remains up to date.
	A record of changes made to customer billing currency in master file data is maintained
Material Master Data	The VAT coding in material master file is maintained.
	Only valid changes are made to VAT coding in the material master file.
	All valid changes to VAT coding in the material master file are input and processed.
	Changes to VAT coding in the material master file are accurate.
	Changes to VAT coding in the material master file are promptly processed.
	VAT coding in the material master file data remains up to date.
	A record of changes made to VAT coding in material master file is maintained.
Pricing Master Data[7]	Price lists are maintained
	Only valid changes are made to price lists.
	All valid changes to price lists are input and processed.
	Changes to price lists are accurate.
	Changes to price lists are promptly processed.
	Price lists remain up to date.
	A record of changes to price lists is maintained.
VAT Determination Data	VAT Determination data is maintained
	Only valid changes are made to VAT determination data.
	All valid changes to VAT determination data are input and processed.
	Changes to VAT determination data are accurate.
	Changes to VAT determination data are promptly processed.
	A record of changes in VAT determination data is maintained.

[7] Pricing data may be stand-alone or a function of customer and/or material master data.

Table 6 - Audit Trail Contribution to Authenticity & Integrity in Purchasing Processes

Purchase Process Audit Trail & Master Data	Integrity													
	Authenticity	VAT ID Supplier	Supplier (Name + Address)	VAT ID Customer	Customer (Name + Address)	Invoice Date	Date of Supply	Invoice Number	Nature of Suppy	Quantity	Taxable Amount	VAT Rate	VAT Amount	Currency
Procure-to-Pay (3-way matching)														
Purchase contract	✓		✓	✓	✓				✓		✓			✓
Purchase order	✓		✓	✓	✓				✓	✓	✓			✓
Goods / service received note							✓		✓	✓				
Invoice						✓								
Payment	✓		✓					✓			✓		✓	✓
Vendor Master Data														
Material (Supply) Master Data														
Pricing Master Data														
Other business controls														
Procure-to-Pay (2-way matching)														
Purchase contract	✓		✓		✓				✓		✓			✓
Purchase order	✓		✓		✓				✓		✓			✓
Invoice						✓								
Payment	✓		✓					✓			✓		✓	✓
Vendor Master Data														
Material (Supply) Master Data														
Pricing Master Data														
Other business controls														
Invoice-to-Pay														
Purchase Contract	✓		✓		✓				✓		✓			✓
Invoice						✓								
Payment	✓		✓					✓			✓		✓	✓
Vendor Master Data														
Material (Supply) Master Data														
Pricing Master Data														
Other business controls												✓		

Table 7 - Authenticity & Integrity in a Procure-to-Pay (goods 3-way matching) Cycle

Authenticity / Integrity Invoice Component	Audit trail component	Audit trail component contribution to A&I
Authenticity	Purchase contract	Will identify the supplier for a particular supply.
	Purchase order	Will identify the supplier for a particular supply.
	Payment	Will identify the supplier for a particular supply.
VAT ID Supplier / Supplier Name & address	Purchase contract	Will identify the supplier for a particular supply.
	Purchase order	Business records will contain a supplier account reference providing a link back to ERP supplier master data.
	Payment	Payments allocated to invoices will identify the payee.
VAT ID Customer / Customer Name & Address	Purchase contract	Purchase contract will identify the purchasing company.
	Purchase order	Purchase order will identify the purchasing company.
Invoice Date	Invoice	There will be a correlation between invoice date and posting date of the invoice record in the ERP.
Date of Supply	Goods / service received note	Date of goods / service receipt will correlate with the date of supply.
Invoice Number	Payment	Payment remittance advice may reference invoice number.
Nature of Supply	Purchase contract	Will contain a record of what is to be supplied.
	Purchase order	Will contain a record of what is to be supplied.
	Goods / service received note	Will contain a record of what has been supplied.
Quantity	Purchase order	Will contain a record of quantity requested.
	Goods / service received note	Will contain a record of quantity delivered.
Taxable Amount	Purchase contract	Will quote the cost of a supply.
	Purchase order	Will quote the cost of a supply
	Payment	Payment correlates with the sum of taxable & VAT amounts.
VAT Rate		
VAT Amount	Payment	Payment correlates with the sum of taxable & VAT amounts.
Currency	Purchase contract	Billing currency will be agreed within contract.
	Purchase order	Billing currency will be specified within the order.
	Payment	Payment currency should provide an indication of invoice currency.

Table 8 - Authenticity & Integrity in a Procure-to-Pay (goods 2-way matching) Cycle

Authenticity / Integrity Invoice Component	Audit trail component	Audit trail component contribution to A&I
Authenticity	Purchase contract	Will identify the supplier for a particular supply.
	Purchase order	Will identify the supplier for a particular supply.
	Payment	Will identify the supplier for a particular supply.
VAT ID Supplier / Supplier Name & address	Purchase contract	Will identify the supplier for a particular supply.
	Purchase order	Business records will contain a supplier account reference providing a link back to ERP supplier master data.
	Payment	Payments allocated to invoices will identify the payee.
VAT ID Customer / Customer Name & Address	Purchase contract	Purchase contract will identify the purchasing company.
	Purchase order	Purchase order will identify the purchasing company.
Invoice Date	Invoice	There will be a correlation between invoice date and posting date of the invoice record in the ERP.
Date of Supply		
Invoice Number	Payment	Payment remittance advice may reference invoice number.
Nature of Supply	Purchase contract	Will contain a record of what is to be supplied.
	Purchase order	Will contain a record of what is to be supplied.
Quantity	Purchase order	Will contain a record of quantity requested.
Taxable Amount	Purchase contract	Will quote the cost of a supply.
	Purchase order	Will quote the cost of a supply.
	Payment	Payment correlates with the sum of taxable & VAT amounts.
VAT Rate		
VAT Amount	Payment	Payment correlates with the sum of taxable & VAT amounts.
Currency	Purchase contract	Billing currency will be agreed within contract.
	Purchase order	Billing currency will be specified within the order.
	Payment	Payment currency should provide an indication of invoice currency.

Table 9 - Authenticity & Integrity in an Invoice-to-Pay Cycle

Authenticity / Integrity Invoice Component	Audit trail component	Audit trail component contribution to A&I
Authenticity	Purchase contract	Will identify the supplier for a particular supply.
	Payment	Will identify the supplier for a particular supply.
VAT ID Supplier / Supplier Name & address	Purchase contract	Will identify the supplier for a particular supply.
	Payment	Payments allocated to invoices will identify the payee.
VAT ID Customer / Customer Name & Address	Purchase contract	Purchase contract will identify the purchasing company.
Invoice Date	Invoice	There will be a correlation between invoice date and posting date of the invoice record in the ERP.
Date of Supply		
Invoice Number	Payment	Payment remittance advice may reference invoice number.
Nature of Supply	Purchase contract	Will contain a record of what is to be supplied.
Quantity		
Taxable Amount	Purchase contract	Will quote the cost of a supply.
	Payment	Payment correlates with the sum of taxable & VAT amounts.
VAT Rate	Other business controls	The relationship between the customer & supplier may dictate that the VAT rate of the supplies between them is fixed, i.e. either high rate or lower rate.
VAT Amount	Payment	Payment correlates with the sum of taxable & VAT amounts.
Currency	Purchase contract	Billing currency will be agreed within contract.
	Payment	Payment currency should provide an indication of invoice currency.

Table 10 - Illustrative Business Control Objectives for Purchase Process Audit Trail

Audit Trail Component	Business Control Objectives
Purchase Contract	
Purchase Order	Purchase orders are accurately entered.
	Purchase orders are created prior to goods received note or invoice processing.
	Changes to orders post goods receipt/invoice are either blocked or recorded.
Goods Received Note	Raw materials/good for resale are received and accepted only if they have valid purchase orders.
	Raw materials/good for resale received are recorded accurately.
	Receipts of raw materials/good for resale are recorded promptly and in the appropriate period.
	Changes to Goods Receipt Note records post invoice are either blocked or recorded.
Invoice	Amounts posted to accounts payable represent goods or services received.
	Accounts payable amounts are accurately calculated and recorded.
	Amounts for goods or services received are recorded in the appropriate period.
	All invoices are received; they are accounted for only once
Payment	Disbursements are made only for goods and services received.
	Disbursements are distributed to the appropriate suppliers.
	Disbursements are accurately calculated and recorded.
Vendor Master Data	The vendor name, address & VAT registration number in master file is maintained.
	Only valid changes are made to the vendor name, address & VAT registration number in master file.
	All valid changes to vendor name, address & VAT registration number in master file are input and processed.
	Changes to vendor name, address & VAT registration number in master file are accurate.
	Changes to vendor name, address & VAT registration number in master file are processed in a timely manner.
	Vendor name, address & VAT registration number in master file data remain up to date.
	A record of changes made to vendor name, address & VAT registration number in the master file data is maintained
	The VAT coding in vendor master file is maintained.
	Only valid changes are made to VAT coding in the vendor master file.
	All valid changes to VAT coding in the vendor master file are input and processed.
	Changes to VAT coding in the vendor master file are accurate.
	Changes to VAT coding in the vendor master file are processed in a timely manner.
	VAT coding in Vendor master file data remain up to date.
	A record of changes made to VAT coding in customer master file is maintained.
Material Master Data	The VAT coding in material master file is maintained.
	Only valid changes are made to VAT coding in the material master file.
	All valid changes to VAT coding in the material master file are input and processed.
	Changes to VAT coding in the material master file are accurate.
	Changes to VAT coding in the material master file are promptly processed.
	VAT coding in the material master file data remains up to date.
	A record of changes made to VAT coding in the material master file is maintained
	Only valid changes are made to preferred supplier in the material master file.
	All valid changes to preferred supplier in the material master file are input and processed.
	Changes to preferred supplier in the material master file are accurate.
	Changes to preferred supplier in the material master file are promptly processed.
	Preferred supplier in the material master file data remain up to date.
	A record of changes made to preferred supplier in the material master file is maintained.

Pricing Master Data[8]	Purchasing price lists are maintained
	Only valid changes are made to purchasing price lists.
	All valid changes to purchasing price lists are input and processed.
	Changes to purchasing price lists are accurate.
	Changes to purchasing price lists are promptly processed.
	Purchasing price lists remain up to date.
	A record of changes made to purchasing price lists is maintained.

8 Pricing data may be stand-alone or a function of customer and/or material master data.

Table 11 - Glossary of Process Events and Master Data

Event / Master Data	Description
Billing schedule	Usually used for long-term service contracts. It will detail what is to be billed at specified points during the duration of the supply and how much is to be billed.
Customer master data	This represents all the data held by a supplier about its customers, usually referenced by a customer account number. The data held will typically include the customers name and address, delivery addresses and VAT registration number where required. There may also be data that impacts on pricing and VAT determination.
Cash receipt	The receipt of payment for a supply by the supplier, from the customer.
Goods dispatch note	This is a document that represents the physical movement of goods and will often accompany the goods in transit. The document will usually record the customer, delivery address and quantity and nature of supply.
Goods received note	This represents the event of recording the receipt of goods or acknowledgement that a service has been received. For goods it will typically be the instigator of the update of the stock inventory. The goods received note may be the purchasing party's view of the goods dispatch note issued by the supplier.
Material master data	This represents data about the supply. The term is usually associated with inventoried goods, although in some industries there may be an equivalent for fixed services, i.e. those that are repeated or quantified. Where the data relates to goods it may equally be held by the supplier or customer but where it relates to service it will usually only be held by the supplier. There may also be data that impacts on pricing and VAT determination.
Payment	The issue of payment for a supply by the customer to the supplier.
Pricing master data	This represents the data that is used to determine the selling (net) price for a supply. This type of data is essential for the supplier but customers may also have equivalent data in their systems for purchase price control.
Purchase order	This is a document produced by a customer to request a particular supply from a supplier – it is often transcribed by the supplier into a sales order. It will usually record details of the supply delivery address, quantity and nature of supply, and value of the supply.
Sales invoice requisition	A document that represents an instruction to create and issue a sales invoice and will typically contain the majority of information that is required for the invoice. These will normally only be used for irregular supplies outside the normal supply chain, e.g. sale of fixed assets.
Sales order	This is a document produced by a supplier as a record of an order received from a customer, often in the form of a purchase order. It will usually record details of the customer, delivery address, quantity and nature of supply, and value of the supply.
Sales / purchase contract	This represents a record of an agreement between the supplier and customer for a particular supply or supplies. It will usually provide details of what is to be supplied and the cost of the supply. Sales/purchase orders may be raised to represent the whole supply or components of it.
Sales / purchase invoice	The invoice for tax purposes from the perspective of the supplier & customer.
Service contract	This represents a record of an agreement between the supplier and customer for a particular supply or supplies of services. It will usually provide details of what is to be supplied and the cost of the supply. Sales/purchase orders may be raised to represent the whole supply or components of it. Alternatively, it may contain a billing schedule.
Supplier master data	This represent all the data held by a customer about its suppliers, usually referenced by a supplier account number. The data held will typically include the suppliers name and address, and VAT registration number. There may also be data that impacts on pricing and VAT determination.
VAT determination data	This represents the data that is used to determine the VAT rate and VAT amount for a supply. This type of data is crucial for the supplier but customers may also have equivalent data in their systems for purchase price control.

3.5 Class B: Controlled data exchanges

Business solutions relating to class B include, as part of a controlled exchange, a level of automated syntax verification. Parties typically have a stable relationship and a 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 Customer. 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 3.8.5 for more information.
- Particular attention should be paid to secure storage of Invoices and of any information which ensures the authenticity of the invoice, the integrity of its content and its legibility. Section 3.8.4 describes good practices for high-security archiving processes.
- Structured data is used in such solutions and parties have to agree beforehand on the agreed format and which processes and controls should 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 should be controlled through a combination of transport-level technologies and process-level controls.
- Both Supplier and Customer (or third parties acting on their behalf) should typically have in place automated verification of message syntax. The Customer should also have automated processes in place to identify messages from its Suppliers. Relevant controls embedded in such automated verification should 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.

3.5.1 Class B1: EDI

Directive 2010/45/EU (2) explicitly mentions EDI as an example of an implementation of class B. Here it is referred to as Class B1, a subclass of Class B.

3.5.1.1 Model Agreements

Structured data is used and parties must agree beforehand which processes and controls are 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 (4) dated October 19th 1994 relating to the legal aspects of electronic data interchange is the recommended basis for a model agreement under this class.

3.5.1.2 Securing Data

Every leg of the process for sending or making available of the E-Invoice is to be controlled through a combination of transport-level technologies and process-level controls. Similarly, measures suitable to prevent attacks to the data themselves must be in place. In particular, controls must be in place in between physical or logical processing steps. Suitable ICT security related measures, such as firewalls, IDS, encrypted channels (e.g. TLS-based) and malware detection and prevention solutions should be employed to ensure that trusted processes cannot be compromised through external attacks to processing applications and transmission channels.

Processes should be trustworthy using general good security practices as described in section 3.8.5. and the mechanisms which may be employed to protect data during transmission are described specifically in subsection 3.8.5.5.

3.5.2 Class Bn: Other controlled data exchanges

Although Directive 2010/45/EU (2) only explicitly mentions EDI as an example of an implementation of class B, other implementations exists and may prove as efficient methods to ensure authenticity, integrity and legibility.

As an example of such an implementation, the PEPPOL[9] project aims to enable cross-border electronic procurement, connecting communities through standards-based solutions.

In the PEPPOL transport infrastructure, data is secured in transport between service operators based on the START protocol with encryption using digital signatures issued by regional operators and PEPPOL provides a governance model where all service operators must abide to a common Interoperability Agreement before being part of the infrastructure.

3.6 Class C: Data-level controls

Class C implementations rely on a data object (“seal”) carried or associated with the invoice, which can ensure its authenticity and integrity throughout its lifetime.

Typically, in a Class C implementation, an E-Invoice is sealed when it is issued. The Customer receiving the invoice can subsequently verify the seal upon receipt. The creation and validation of Class C seals can be performed locally by each trading partner or collapsed into a central point. Any user, including tax administrations, can re-perform such verification at any time during storage. The sealed E-Invoice is stored by the trading partner(s) having chosen to use Class C as their strategy for complying with integrity and authenticity requirements. The Class C seal typically (i) encapsulates reliable identification information of the person that created the seal, thereby ensuring authenticity, and (ii) intrinsically allows the integrity of the sealed data to be technically verified at any moment in time, without reference to any other data external to the sealed object. When sufficient validity evidence is included in the seal, the storage process and technology do not need to provide further integrity and authenticity assurances for the specific invoice (invoicing sequence integrity is still needed to be maintained by the archive). Care must be taken to ensure that the seal does not become unreliable over time; this may occur when components of the above evidence have an expiration date. In this case the person responsible for storage shall adopt technical or organizational measures suitable to “extend” the seal validity.

Use of Class C makes any change of the sealed data detectable. This feature significantly limits options for the sealed E-Invoice to be converted to another format; various methods are in use or have been proposed to enable trading partners to use Class C while also allowing the buyer or intermediate service provider to automatically process a reliable unsealed representation of the E-Invoice in its workflow and/or accounting system. Examples of such Class C implementations include:

1. Extracting the E-Invoice data out from the sealed E-Invoice to feed them into the relevant processing (with or without prior format conversion), but maintaining the sealed E-Invoice for storage.

2. Implementations where one invoice, or any other type of document, is electronically sealed (e.g. by means of a signature) thus protecting its content (at least its mandatory content) and the same data (or at least a subset of them) is placed in a structure that can be freely processed and converted whilst remaining associated with the sealed (i.e. signed) E-Invoice which is stored for evidence purposes.[10]

Class C implementations enable compliance with requirements for integrity and authenticity of E-Invoices; they do not vouch for the consistency of an E-Invoice with underlying business processes.

---

9 Pan-European Public Procurement Online: The PEPPOL project is mutually funded by the European Commission and consortium members.

10 One method in this category, inspired by e-invoicing regulation and practices in other geographies where electronic signatures are used to embed a sealed object in an XML structure, has been called « single field encryption » (SFE). This allows the sealed object to be embedded in the document to be consumed and stored. Another possible way is using a PDF format strictly joined with an XML structure in a way that both formats align when one change is applied to one of them.

3.6.1 Class C1: Qualified electronic signatures

Directive 2006/112/EC (1), as amended by Directive 2010/45/EU (2), states in Art. 233(2) that Qualified Electronic Signatures[11] (QES) ensure the integrity and authenticity of E-Invoices. A QES is an enhanced version of an Advanced Electronic Signature (AdES), since it is supported by a qualified certificate and created by a secure signature-creation device. Qualified Electronic Signatures are recognised as legally valid across the European Union (see Directive 1999/93/EC (5)).

In some Member States, qualified certificates can legally be issued solely to a natural person (an individual). In such cases, a QES can only be created solely by such natural person. Many implementations of QES-based legal compliance therefore use the qualified certificate of an authorized company employee or executive.

For issuing signed E-Invoices it has become common practice to make use of automated signing processes protected with reliable security measures to ensure the signer's sole control on his/her signing key .

Ultimately a Qualified Electronic Signature depends on three elements:

1. Qualified Public Key Certificate – Generally speaking the "public key" used to verify a signature is held in a Public Key Certificate made available (generally it is included in the signature) for use in particular by the invoice recipient and auditor for verifying the signature. This certificate is issued by a trusted service provider called "Certification Authority". In the case of Qualified Electronic Signatures the supporting certificates are "Qualified" Public Key Certificates issued by Certification Authorities that meet requirements as in Directive 1999/93/EC and are supervised by the relevant EUMS, as per Directive 1999/93/EC art. 3(3). Qualified Certificates may be encoded to the specification ETSI TS 101 862 (6). Certification Authorities generally operate to the policy requirements specified in ETSI TS 101 456 (7). For an advanced electronic signature any certificate conforming to ISO/IEC 9594-8 (8) is generally considered acceptable.

2. Secure Signature Creation Device (SSCD) – An SSCD holds the necessary signing key and cryptographic functions to create the electronic signature. This may be an object like a smart card or USB token exclusively held by the signatory. Depending on the applicable legislation, the SSCD can also be a hardware security module (HSM) holding the signing key of many signatories. Each signatory can access remotely, in a secure manner, its own signature key and use it under its sole control. The security of the SSCD can be assured through conformance to a Common Criteria (ISO 15408 (9)) Protection Profile specified in CWA 14169 (10) shortly to be enhanced as EN 14169. For simple Advanced Electronic Signatures the signing key may not be stored in one SSCD, e.g. it can even be kept in a secured file held on a computer.

From these two items it stems that a QES provides E-Invoices with intrinsic means to ensure their authenticity of origin and integrity of content. Once these basic requirements are met, business controls implementation can focus on the fiscally related processes, addressing other relevant documents, such as orders, delivery notes, payment records, etc.

It must be clarified that the use of Qualified Certificates is not the only way to ensure the signer's identity. This can be equally achieved if non-QC certificates are issued by Certification Authorities that abide by suitable policies and practices and if such abidance is supervised by a trusted entity, e.g. a governmental body.

The third element follows.

3. Signature Formats – Once created, any Advanced Electronic Signature, including QES, is held throughout its lifetime as a data object joined, or associated, with the invoice data. The format of signed invoices must be maintained throughout the lifetime of the invoice for the signature to be verifiable. Thus, if the invoice is converted (see section 3.8.7), a copy of the originally encoded E-Invoice should be kept alongside the converted version for verification by the auditor.

---

11 Art. 233(2): "Other than by way of the type of business controls described in paragraph 1, the following are examples of technologies that ensure the authenticity of the origin and the integrity of the content of an electronic invoice: (a) an advanced electronic signature within the meaning of point (2) of Article 2 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (*), based on a qualified certificate and created by a secure signature creation device, within the meaning of points (6) and (10) of Article 2 of Directive 1999/93/EC

Depending on the invoice encoding used, one of three signature encodings are generally employed referred to as CAdES, XAdES and PAdES. CAdES uses binary encoding techniques, XAdES uses XML encoding and PAdES uses PDF encoding. As explained above, a QES is an AdES enhancement, therefore the same encoding applies to Qualified Signatures.

3.6.2 Class C2: Advanced digital signatures

Advanced Electronic Signatures can also be used, provided that they are securely and reliably implemented so as to ensure the required authenticity and integrity. Among the characteristics of an Advanced Electronic Signature as defined in Directive 1999/93/EC, Art. 2 (5), requirements (b) and (d) state respectively: "*(b) it is capable of identifying the signatory*" 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*".

In practice: non-QC certificates can be reliable if issued by Certification Authorities that abide by suitable policies and practices and if such abidance is supervised by a trusted entity, e.g. a governmental body. Similarly, an AdES does not need to be created using a Secure Signature Creation Device (SSCD), but its creation can still be reliable if other measures are implemented that ensure sole control of the certificate holder (i.e. "signatory") over the private key.

3.6.3 Class Cn: Other data level controls

Currently there are no other known implementations of class C beyond QES and AdES. Additional Class C methods may emerge over time.

3.7 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 Customer or a Service Provider.

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 removed. Suppliers, Customers 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 Customer.

The Class D Service Provider, or the Supplier or Customer providing Class D Services, must operate within an environment characterized by robust internal controls comparable to those described under Class A in section 3.4 above. A Class D Service Provider should undergo regular recognized audits based on procedures such as the International Standard on Assurance Engagement (ISAE 3402 (11)), the successor of SAS 70 (12), by a trustworthy third party organization. Such audits would re-assure customers that the outsourced operations are totally under control. The Supplier or Customer 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 3.8.4). If a single storage is managed by one of the two trading partners, instead of a third party (a service provider), the other party is entirely delegating the responsibility of keeping the invoice single copy to its counterparty. There is a theoretical risk of tampering with that single copy. Delegating parties are therefore advised to carefully evaluate all possible risks before entering into such an agreement.

Usually in E-invoicing implementations there will be two instances of an invoice stored; that stored by the issuer, and that stored by the recipient. Under Class D implementations it is possible that there is only one instance of an invoice, which represents both that issued by the issuer and that received by the recipient. In such circumstances, in order to ensure availability of the invoice to both parties, disaster recovery plans enacted by the single storage might envisage security measures possibly even more rigid than those implemented when each party independently stores its own copy of the invoice. The "buyer portal", widely used today, is an example of this case where only one party could take care of storing invoices for itself and on behalf of its trading partner.

3.7.1 Manual Web-based invoicing - authenticity and integrity concerns

Extra controls will be necessary in E-invoicing scenarios where the creation, sending or collection of E-Invoices is manually handled through a web portal using tools such as a web-browser or similar client software.

3.7.1.1 Service Provider Controls

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.

Differing classes of access should be provided to portal applications. Read-only access may be granted to auditors or service desk personnel, neither of whom should be able to create amend or delete any E-Invoices.

For portals that only allow purchase order flip, basic authentication of the web portal based on server-side SSL / TLS (8) 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 general and in particular 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 at least two-factor authentication as well as increased web portal authentication using for example Extended Validation (EV) certificates.

A portal application should make clear distinction between invoices which are rejected because of technical reason or because of business reasons. These rejections or failures may occur at any time between initial data entry and delivery to the Customer. A regular reconciliation report, or an automatic process, should be constructed so that Supplier and Customer are able to check that manual portal output reconciles completely with their internal systems.

3.7.1.2 User Controls

The data used to enter an invoice into a portal or to create a PO flip, will have been extracted in some way from a supplier’s internal accounting/invoicing system. A careful comparison, preferably by more than one pair of eyes, should be made to make sure that the original invoice data is faithfully represented in the portal. Although the E-Invoice output from the portal will be the legal invoice, it is likely that supplier tax reporting will be based on the internal application which produced the invoice data.

Portal users should be required to conform to an increased desktop security policy through an agreement with the operator. Required desktop security measures should include:

- Up-to date malware protection software.
- 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 (13) 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.

3.8 Issues affecting all classes

This section addresses a number of issues that may arise in the context of invoicing or e-invoicing regardless of the class used for meeting the legal requirements for ensuring integrity and authenticity. In some cases, however, the way in which such matters are approached or resolved by trading partners may depend on the legal compliance strategy. It should also be noted that a number of the issues that are briefly described in this section are the subject of specific legal requirements in EU Member States; this CWA does not purport to provide guidance on meeting such requirements.

3.8.1 Self-billing

Self-billing is where the Customer issues the invoice rather than the Supplier.

3.8.1.1 Risks in managing VAT 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 specifically related to self-billed electronic invoices are:

- 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 Customer. If this occurs, the Customer 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 Customer'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 Customer with whom a self-billing agreement exists, for a supply of a type covered by the Self-Billing agreement.
- The Supplier receives his Customer's self-billed E-Invoice, but treats it as a purchase E-Invoice. The Customer 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 Customer, 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 every single 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 Customer 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.

3.8.2 Scanning of received Invoices

Companies can use scanning techniques to facilitate the processing and/or storing of received paper Invoices. There are two common processes:

Scanning for processing. Scanned images and optical character recognition techniques are used to scan the data on the paper Invoice into an electronically processable format. If the paper Invoice is stored, the authenticity, integrity and legibility requirements remain with the paper Invoice. In the case where the paper invoice is not kept, the following paragraph applies.

Scanning for storage. Where paper invoices are scanned to electronic form (and the paper invoice discarded) for storage purposes there should be a demonstrable internal control mechanism in place to ensure integrity and compensate the loss of authenticity measures of the invoice. EU VAT Directives provide that it is possible to copy a paper invoice to an electronic format for storage purposes; Member States may opt out of this rule by stipulating that the paper invoice cannot be replaced by an electronic equivalent.

3.8.3 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 or other authorities. 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.

Where allowed under applicable legislation, a Service Provider that converts the E-Invoices should do so only in accordance with agreed mapping that is reproducible. The mapping process should be auditable. The conversion can 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.

3.8.4 Storage

E-Invoices and associated evidence to ensure authenticity and integrity must be stored, at least, for the period specified by the applicable Tax Administration [12]. E-Invoices and evidence supporting authenticity and integrity must be stored in a way that prevents unauthorized access, modification, deletion, and theft. Also, in a way that ensures retrieval, legibility and integrity of the information..

Reliable preservation of data can only be achieved if suitable organisational, archival, technical, security measures are implemented. These measures are defined in a number of standards and specifications, some of them related specifically to archival matters, others to security. There is a common belief that it may be sufficient to rely just on media types without implementing other organisational and security measures: this is misleading and dangerous because without all of the above mentioned measures, the preserved information can be lost or tampered with, intentionally or unintentionally. In the following paragraphs a high level description of a few of the archival related topics and security related measures are provided. For a more thorough analysis, the reader may refer to other publications, some of which are indicated in specifically focused bibliography clauses added to each paragraph. The business should ensure that the necessary controls are in place even if the storage is outsourced to a third party.

3.8.4.1 Archival related aspects

The final goal of the archival related aspects is to assure that any archived piece of information can be retrieved at any subsequent time that may be indefinite or limited depending on a number of factors. In particular in the E-Invoices case the archived items preservation time is defined by the applicable legislation, but it may extend even beyond where legal proceedings occur or additional organizational requirements are in place.

Among the main archival related issues to take into account, it is to be ensured that key index data are:

1. Extracted from every archived information,
2. Arranged and managed in a way to make any subsequent information retrieval possible,

and that the archived pieces of information are:

3. Properly kept in storage for all the preservation time,
4. Timely made available to authorised requesters.

---

12 It is to be taken into account that the legally required storage period may be lengthened in case of legal proceedings of any kind.

These items must be properly addressed from the initial stage of the document preparation (items 1 and 2 in particular) through the entire information life cycle. Just as an example of the archival matter scope, it is sufficient to mention a few of the main topics indicated in ISO 14721 (14):

- Ingest of digital data sources to the archive;
- Delivery of digital sources from the archive;
- Submission of digital metadata, about digital or physical data sources, to the archive;
- Identification of digital sources within the archive;
- Search and retrieval of metadata information about digital and physical data sources;
- Migration of information across media and formats.

For further information, these standards may be referred to ISO 14721 (14), ISO 15489 (15), ISO 14641 (16) (under development) and ISO 30300 (17) (under development).

3.8.4.2 Storage security measures

Storage security spans from strictly ICT security related measures through organisational matters, such as financial stability, abidance by the applicable legislation, contractual aspects, organisation independence, just to name a few.

As specified above, the main goal of an information preservation service is to ensure the integrity of the preserved information at least for the entire storage period.

To achieve this purpose, a solution is proposed by the currently existing technical specifications; Advanced Electronic Signatures supported with certificates issued by Certification Authorities whose operations are certified and monitored by independent trusted entities, like Governmental Bodies. These signatures can be issued either directly by the Information Preservation Service Provider (IPSP, the storing organisation) or by independent trusted entities like Time Stamping Authorities. In the latter case, Time Stamp Tokens (TST) would be issued, compliant with standards or Public Available Specifications like RFC 3161 (18) and its successors.

To this purpose in many EUMS, where signatures are applied by the IPSP it is often required to support these signatures with Qualified Certificates that are issued by CAs supervised under the Government responsibility. Where they, instead, are applied in the shape of Time Stamp Tokens, the issuing TSA is often required to be independently supervised and monitored, at times by governmental bodies.

The above signature (be it directly issued by the IPSP or by one TSA) is not requested to be applied to each single preserved item, but to binary objects cryptographically derived from logical batches of the preserved objects and built in a way to ensure that tampering with any of the preserved documents can be subsequently identified. Specifications on how to derive such binary object from the preserved information are often country developed. For example in Germany it is addressed in the BSI TR 03125, in Italy in the UNI 11386:2010 specification.

In any case, where an IPSP is employed, such Service Provider that stores, in our case “E-Invoices”, on behalf of one or both trading parties, must enact appropriate controls to ensure the E-Invoices’ integrity at least during the preservation time.

International, regional or national specifications exist that address these controls and the related objectives.

Among the International standards the ISO/IEC 27000 family addresses “Information technology — Security techniques”, in particular ISO/IEC 27001 (19) that deals with “Information security management systems” and ISO/IEC 27002 (20) providing a “Code of practice for information security management”. Other components of this ISO/IEC family are also to be taken into account though. It is to be remarked that the ISO/IEC 27000 family is not specific to Information Preservation, therefore its provisions need to be “customised” to such an environment.

In the EU, such customisation has been carried out by ETSI[13], first with the ETSI TS 102 573 (21), that specifies policy requirements, and later in the ETSI TS 101 533-01 (22) and TR 101 533-02 (23)[14] that

[13] European Telecommunications Standards Institute

provide detailed practices requirements. These ETSI deliverables further elaborate the ISO/IEC 27000 family (20; 19), customising and integrating its provisions to the Information Preservation peculiarities.

Among the National Specifications it is worth mentioning the above cited German BSI TR 03125.

3.8.5 General Good Security Practices

3.8.5.1 IT General Controls (ITGC) & IT Application Controls

Business controls in an IT context are usually categorised into IT General Controls (ITGC) and IT Application Controls.

ITGC represent the foundation of the IT control structure. They help ensure the reliability of data generated by IT systems and support the assertion that systems operate as intended and that output is reliable. ITGC usually include the following types of controls: control environment, change management procedures, source code/document version control procedures, software development life cycle standards, logical access policies, standards and processes, incident management policies and procedures, problem management policies and procedures, technical support policies and procedures, hardware/software configuration, installation, testing, management standards, policies and procedures, disaster recovery/backup and recovery procedures, and physical security.

IT Application Controls are designed to ensure the complete and accurate processing of data, from input through output. These controls vary based on the business purpose of the specific application, and can include automatic, manual and user controls. These controls may also help ensure the privacy and security of data transmitted between applications. Categories of IT application controls may include: completeness checks, validity checks, matching, identification, authentication, authorization, and input controls.

IT General Controls are a prerequisite to reliable IT Application Controls and both are essential to accurate operation of electronic invoicing systems. The General & Application Controls should always be appropriate to the IT environment in question. Use of recognised standards for auditing the security or general practices of the IT systems such as ISO 27001 (19) or International Standard on Assurance Engagement ISAE 3402 (11) provides a good basis for assuring the general practices of an organisation. The OECD Guidance on Tax Compliance for Business and Accounting Software (GASBAS) (24) also provides guidance on good practices appropriate to business software.

3.8.5.2 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 process model (see section 3.2).

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.

3.8.5.3 Advanced/Qualified Electronic Signatures – Specific Awareness

Users of Advanced Electronic Signatures, as well as of Qualified Electronic Signatures, should be aware of a number of requirements to be complied with in order to reliably issue and manage signed documents. A short description of these requirements is presented in this paragraph to help users obtain the necessary information from the relevant sources: Government, Certification Authorities awarding them Public Key Certificates, even Qualified, Time Stamping Authorities, Signature Creation/Verification Application

---

14 ETSI TS 101 533-1 provides an exhaustive set of measures to implement and manage the ICT Security of an Information Preservation Service Provider. Its sister document ETSI TS 101 533-2 provides recommendations on how to audit such IPSP.

Providers, Secure Signature Creation Device Providers, hosts of Hardware Security Modules suitable to allow signatories to remotely issue signatures, etc.

A Qualified Electronic Signature is an Advanced Electronic Signature based on a Qualified Certificate and issued by means of a Secure Signature Creation Device.

Qualified Certificates are issued, in compliance with technical specification ETSI[15] TS 101 862 (6) that is based on standard ISO/IEC 9594-8 (8), by Certification Authorities operating under their relevant Government's supervision as required by Directive 1999/93/EC (5), art. 3(3),

Secure Signature Creation Devices are presented in subsequent item C; Advanced Electronic Signatures formats are presented in item F.

A. Electronic Signatures legal validity
Foremost, Qualified and Advanced Electronic Signatures legal validity depends on the applicable legislation; therefore users should be aware of the requirements imposed by legislation they have to abide by.

B. Qualified legal recognition across the EU internal borders
If a Qualified Certificate supporting a Qualified Electronic Signature is issued in a EUMS different from the signature verifier's one, the latter is to ascertain if the issuing Certification Authority was legally recognized as a valid Qualified Certificates issuer when it issued the specific certificate and when the signature was generated. The mechanism to be used in EU to this purpose is specified in Commission Decision 2009/767/EC (25) and subsequent corrigenda and amendments, based on ETSI TS 102 231 (26).

C. Secure Signature Creation Devices
Secure Signature Creation Devices are hardware signature devices, like smart cards, USB tokens, etc., certified against Common Criteria Protection Profiles defined in CEN Workshop Agreement – CWA 14169, shortly to become EN 14169.

D. Certificate revocation
When one signing key is recognized as having been misused or no longer under the signatory's sole control, i.e. it has been compromised, the associated Public Key Certificate is revoked by the issuing Certification Authority – CA. This revocation status is usually made known by inserting the identifier of the certificate at issue in a "Certificate Revocation List" – CRL – the relevant CA issues in compliance with standard ISO/IEC 9594-8 (8). Signature verifiers should access such CRLs to ascertain if the certificate involved has been revoked and when it was revoked.. Alternatively, verifiers can access a suitable OCSP Responder, where available, complying with RFC 2560 (27). Some authorities that issue certificate revocation information remove references to revoked certificates when they expire. In this case it is necessary to obtain information on the certificate status (i.e. if it was revoked or not) before it expires, and store it along with the E-Invoice.

E. Need for a trusted time reference
The validity of Electronic Signatures, Advanced or Qualified, primarily depends on the validity, at time of signature issue, of all supporting certificates, from the signers' upwards. Therefore it is of paramount importance to associate signatures to a trusted time reference applied soon after they have been generated, to allow ascertain in the future if the signature was generated when the certificates at issue were all valid. The commonly used time reference is a Time Stamp Token as specified in ETSI TS 101 861 (28) that, in turn, is based on RFC 3161 (18) and its subsequent amendments and replacements.

F. Electronic Signature formats
The basic need for interoperability among different signature users (issuers and verifiers) would be met if common signature formats are used. Depending on the object type to be signed, different signature formats are available, issued and maintained by ETSI:

- CAdES (ETSI TS 101 733 (29)) which builds on the use of binary formatted signatures as specified in Cryptographic Message Syntax (CMS - Internet RFC 3852 (30)), as profiled in TS 102 734 (31).

[15] ETSI – European Telecommunications Standards Institute – is one of the three European Standardisation Organisations formally recognised by the European Commission with a number of Directives starting from 83/189/EEC.

- XAdES (ETSI TS 101 903 (32)) which builds on the use of XML formatted signatures as specified in the XML-DSig (33), as profiled in TS 102 904 (34).
- PAdES Signatures (sometimes referred to as PDF signatures) as specified in ISO 32000 and profiled in ETSI TS 102 778 (35).

G. Signatures applied by automated E-invoicing processes
Often E-Invoices are issued with an automated E-invoicing process. In case the process security measures are compromised, attackers may succeed in submitting fake documents to the signing process. To assure that, should this occur, these documents can be recognized as fake in subsequent verifications, measures should be implemented as specified in CEN Workshop Agreement CWA 15579 (36).

H. Signature Policy
In some environments it is either required or customary to include into a signature the applicable "Signature Policy", that specifies the rules under which the signature was generated and under which it is expected to be verified. More on this can be found in ETSI TS 101 733 (29).

3.8.5.4 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 from the early stages of the E-Invoice creation process 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 malicious or not. 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 stylesheets are used to make the XML content understandable by human beings, 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.

It should also be noted that graphical formats (e.g. BMP or TIFF), as well as other formats like DOC and PDF (except PDF/A) can also include HTML instructions, which can result in different data being displayed depending on the application used to visualize a file, that can be triggered by just altering the filename extension (e.g. from ".tif" to ".html").

3.8.5.5 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:

a) Protects the integrity of the data communicated
b) 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 5246 (13)) 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 carefully chosen and managed identity and password based mechanisms may be sufficient although care needs to be taken in operating in such a web based environment (see section 3.7.1).

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 interchange including invoices. These are commonly referred to as AS1, AS2 and AS3, where AS standards for applicability statement. AS1 (RFC 3335 (37)) is aimed at business interchanges using e-mail, AS2 (RFC 4130 (38)) is aimed at business interchanges using web (HTTP) protocols and AS3 (RFC 4823 (39)) is aimed at interchanges using file transfer protocols.

c) Registered E-Mail

Registered e-mail is a secured e-mail having the following features:

1) The sender's REM service provider produces evidence of what was sent from what REM address, at what time and day, to what REM address;

2) The recipient's REM service provider produces evidence of what was delivered to what REM address, at what time and day, incoming from what REM address;

3) All REM "messages" (i.e. the REM message itself, the above mentioned pieces of evidence, as well as other ancillary messages) are recommended[16] to be signed with at least an AdES by the respective issuing REM provider.

When feature no. 3) is implemented. one E-Invoice sent via REM is endowed with evidence of Integrity, since the sent "payload" (in this case an E-Invoice) is included in a REM message that is signed by the sender's REM Provider. Additionally, the other above mentioned features provide both parties, involved in an E-Invoice exchange, with evidence of when the shipment and its delivery occurred.

Authenticity of the sender is also achieved, although with different degrees, depending on the REM mailbox owner identification mechanism adopted by REM providers. In fact, this authenticity may span among the following levels.

a) "*Authenticity of the sending mailbox*" – The mailbox is assigned by the REM provider without ascertaining the requester's identity;

[16] It is to be reminded that the implementation of one "RECOMMENDED" feature can be discarded only after having carefully evaluated al consequences of not implementing it, therefore it is not just a simple option.

b) "*Authenticity of the organisation responsible for the sending mailbox*" – The mailbox is assigned by the REM provider to an organisation upon identification of its representing officer that takes over the requesting organisation the responsibility of the specific REM mailbox management;

c) "*Authenticity of the specific individual who is assigned one specific REM mailbox*" – The mailbox is assigned by the REM provider to one specific individual whose identity is verified, at contract time, either directly or through proxy.

In order to meet the Directive 2010/45/EU (2) requirements as described in art. 233[17] and art. 247[18] it will be necessary to store, alongside the E-Invoice, the entire REM message that carries it, including the related pieces of evidence.

Registered E-Mail specifications have been issued, and are maintained, by ETSI in ETSI TS 102 640 (40).

d) 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.

e) 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 securely 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.

f) 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 Customer or next Service Provider in the process.

g) 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, where allowed by the applicable legislation, 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 Customer 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.

h) OFTP/OFTP2 - The Odette File Transfer Protocol (OFTP) and the more recent version OFTP2 (IETF RFC 5024 (41)) 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.

3.8.6 Error Management

Errors in Invoices can occur and rectification is required to arrive at correct and balanced accounting between trading parties and with the VAT administrations, periodic reporting of VAT to be paid or recovered.

---

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

18 "… Additionally, in the case of invoices stored by electronic means, the Member State may require that the data guaranteeing the authenticity of the origin of the invoices and the integrity of their content, as provided for in Article 233, also be stored by electronic means."

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 later 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 unexpected 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 his E-Invoice.
- Demands introduced manually in the E-Invoice by the Supplier that were not agreed with the Customer.

3.8.6.1 Rejecting an E-Invoice

Art. 232 of Directive 2006/112/EC (1), as amended by 2010/45/EU (2), states: “The use of an electronic invoice shall be subject to acceptance by the recipient”. The acceptation mentioned in this article only reflects the technical requirements or the customer's ability to ensure the authenticity, integrity and legibility that might need to be agreed to receive electronic invoices and which do not exist for paper invoices. This may include any written acceptance, whether formal or not, or by tacit agreement through, for instance, the processing or payment of the received invoice.

However, trading partners should distinguish between not accepting invoices due to technical reasons and due to business reasons.

Where an agreement is made between business partners when exchanging electronic invoices, it should preferably mention that the fact an E-Invoice was accepted for technical reasons does not automatically mean the invoice has been accepted for business purposes.

In the case where an invoice was not accepted for technical reasons, it is automatically not accepted for business reasons either, since no invoice has been received.

In the case where an invoice has been accepted for technical reasons, but there is a dispute about the invoice, then the invoice can still be rejected for business reasons. The dispute will in principle lead to the issuance of an amending invoice or a credit note.

The following list contains examples of business reasons for the rejection of invoices:

- 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 Customer-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 Customer should not modify any Invoice, including an incorrect or contested Invoice.

Depending on the technical solution used for exchanging electronic invoices, the technical reasons for which invoices are rejected are diverse (e.g. mailbox closed down, syntax error, etc.).

3.8.6.2 Invoice retransmitted

E-Invoices should normally only be re-transmitted because for technical reasons the originally issued invoice was not received by the intended recipient. Before re-transmitting, the invoice issuer should verify non-receipt with the recipient. There should be a documented process for verifying non-receipt and evidence of the verification should be stored in a way to link it back to the relevant invoice.

Invoice recipients should have controls in place to prevent processing of more than one instance of a particular invoice.

3.8.7 Format conversion of the E-Invoice

Format conversion may be necessary for automatic data processing in backend systems. It may also be necessary to convert the content for example changing codes for products, supplier or customer in descriptions. As long as some tax administrations interpret “invoice” as “identical semantically and in syntax” to what was issued, it is important to distinguish a conversion before or after the issuing of the original invoice.

- Before issuing the E-Invoice
    - Conversion is possible on the invoice data (at this time only invoice data exists)
    - It is recommended to preserve an end-to-end audit trail

After having issued the E-Invoice

In all cases

- It may be good practice to maintain an audit trail of the conversions enacted
- The Supplier needs to store the invoice as issued and the Customer needs to store the invoice as received. Storing can be done by their respective service providers. Integrity and authenticity is made verifiable in accordance with the implementation:

Class A	The independent authenticity and integrity verifications processes performed by the Customer and Supplier will ensure conversion has been accurately performed.
Class B	The EDI exchange agreement will detail the conversions that will be applied to the invoice. The conversions must not change the intrinsic means of the invoice content. The evidence should be sufficient to demonstrate that authenticity and integrity has been maintained.
Class C	There should be a clear agreement between the trading partners and any intervening service providers detailing what conversions are to be performed, who performs them, and how signatures are to be applied to the converted invoices. An audit trail of the signature chain should be maintained.

    - Format and/or content conversion may occur at sender and/or recipient;
    - The converted invoice should always be distinguishable from the received E-Invoice.

In both cases the conversion must not change the E-Invoice semantics and should be reproducible. It is also required to provide tax authorities an access to the Invoice[19]. Content conversion requires Trading Partners to pay particular attention to the controls they put in place to avoid errors or misunderstandings.

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, as well as if any data extraction will be passed along separately.

b) The integrity and authenticity of the information represented by the E-Invoice shall be verifiable across the end-to-end chain. Any process that performs conversion shall be assured as described in section 3.8.5 and specifically any transfer of data should be protected as described in its subsection 3.8.5.5. Audit trails shall be kept of all mappings used, including information on any changes made and when applied, so that the input and output invoice data can be compared to demonstrate that the information represented is the same as described in section 3.8.5.2.

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.

3.9 How to use the Compliance Matrix and Interactive User Interface

Requirements, associated risks, examples and resolutions are compiled into content which is accessible in two different ways, through the Compliance Matrix and the Interactive User Interface.

The content 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.

The Compliance Matrix is in the form of an Excel spreadsheet. Filters are provided to help users select their 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.

The Interactive User Interface is in the form of a web page. Likewise, filters are provided to help users select their area of interest. In addition to the attributes selectable in the Compliance Matrix, context categories are available to further help narrowing down requirements applicable to every situation.

Instructions on how to use the matrix are included with the Compliance Matrix file and the Interactive User Interface.

The content of the Compliance Matrix and the Interactive User Interface constitutes a reasonable set of “Best Practices”. It is therefore left to the reader to make sure that the content is: a) consistent with the applicable legislation and b) exhaustively addresses all the aspects of such legislation.

---

19 Directive 2006/112/EC, art. 249: “*For control purposes, where a taxable person stores, by electronic means guaranteeing online access to the data concerned, invoices which he issues or receives, the competent authorities of the Member State in which he is established and, where the VAT is due in another Member State, the competent authorities of that Member State, shall have the right to access, download and use those invoices.*”

4 References

The following non-exhaustive list of examples of normative documents, contains provisions which, through reference in this text, constitute provisions of this CWA. For dated references, subsequent amendments to, or revisions to 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.

NOTE ETSI will replace some of the documents referenced below with new ones in 2012 and with a new numbering scheme. Please be aware of this when looking for new versions of standards referenced below.

1. **European Council.** *Council Directive 2006/112/EC on Common System of Value Added Tax.* November 28, 2006.

2. —. *Council Directive 2010/45/EU amending Directive 2006/112/EC.* July 28, 2010.

3. **CEN.** CWA 16463, Code of Practice for Electronic Invoicing in the European Union. 2012.

4. **European Commision.** Commission Recommendation 94/820/EC relating to the legal aspects of electronic data interchange. [Online] 19 October 1994. [Cited: 25 September 2011.] *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31994H0820:en:HTML*

5. **European Council.** Council Directive 1993/93/EC on a Community framework for electronic signatures. [Online] 13 December 1999. *http://portal.etsi.org/esi/Documents/e-sign-directive.pdf*

6. **European Telecommunications Standards Institute.** ETSI TS 101 862: Qualified certificate profile. [Online] v1.3.2, June 2004. [Cited: 22 9 2011.] *http://www.etsi.org/deliver/etsi_ts/101800_101899/101862/01.03.02_60/ts_101862v010302p.pdf*

7. —. ETSI TS 101 456: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates. [Online] v1.4.3, May 2007. *http://www.etsi.org/deliver/etsi_ts/101400_101499/101456/01.04.03_60/ts_101456v010403p.pdf*

8. **International Organization for Standardization.** ISO/IEC 9594-8: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. [Online] 2005. [Cited: 25 September 2011.] *http://www.iso.org/iso/catalogue_detail.htm?csnumber=34551*

9. —. ISO/IEC 15408 (multipart): Information technology - Security techniques - Evaluation criteria for IT security. [Online] 2009.

10. **CEN.** CWA 14169: Secure signature-creation devices “EAL 4+”. [Online] March 2004. [Cited: 25 September 2011.] *ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14169-00-2004-Mar.pdf*

11. **International Federation of Accountants.** ISAE 3402: International Standard on Assurance Engagement. [Online] June 2011. [Cited: 25 September 2011.] *http://www.ifac.org/sites/default/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf*

12. **AICPA SAS 70.** Statement on Auditing Standards No.70, Service Organizations. AICPA SAS 70.

13. **Internet Engineering Task Force.** IETF RFC 5246: The Transport Layer Security (TLS) Protocol. [Online] v1.2, August 2008. [Cited: 25 September 2011.] *http://tools.ietf.org/html/rfc5246*

14. **International Organization for Standardization.** ISO 14721: Space data and information transfer systems - Open archival information system - Reference model.

15. —. ISO 15489 (multipart): Information and documentation - Records management.

16. —. ISO 14641 (multipart): Electronic archiving Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation.

17. —. ISO 30300: Information and documentation - Management system for records.

18. **Internet Engineering Task Force.** IETF RFC 3161: Internet X.509 Public Key Infrastructure, Time-Stamp Protocol (TSP). [Online] [Cited: 22 September 2011.] *http://www.ietf.org/rfc/rfc3161.txt*

19. **International Organization for Standardization.** ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements.

20. —. ISO/IEC 27002: Information technology - Security techniqiues - Code of practice for information security management.

21. **European Telecommunications Standards Institute.** ETSI TS 102 573: Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data for digital accounting. [Online] v1.1.1, July 2007. [Cited: 22 September 2011.]
http://www.etsi.org/deliver/etsi_ts/102500_102599/102573/01.01.01_60/ts_102573v010101p.pdf

22. —. ETSI TS 101 533-01: Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security - Part 1: Requirements for Implementation and Management. [Online] v1.1.1, June 2008. [Cited: 26 September 2011.]
http://www.etsi.org/deliver/etsi_ts/102500_102599/102533/01.01.01_60/ts_102533v010101p.pdf

23. —. ETSI TR 101 533-02: Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security Part 2: Guidelines for Assessors. [Online] May 2011. [Cited: 26 September 2011.]
http://www.anorc.it/documenti/ETSI%20101%20533-2.pdf

24. **OECD: Centre for Tax Policy and Administration.** Guidance and Specifications for Tax Compliance of Business and Accounting Software. [Online] April 2010. [Cited: 25 September 2011.]
http://www.oecd.org/dataoecd/42/33/45045404.pdf

25. **European Commision.** Commission Decision 2009/767/EC setting out measures facilitating the use of procedures by electronic means through the ‘points of single contact’ under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market. [Online] 16 October 2009. [Cited: 25 September 2011.] *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:EN:PDF*

26. **European Telecommunications Standards Institute.** ETSI TS 102 231: Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information. [Online] v3.1.2, December 2009. [Cited: 26 September 2011.]
http://www.etsi.org/deliver/etsi_ts/102200_102299/102231/03.01.02_60/ts_102231v030102p.pdf

27. **Internet Engineering Task Force.** IETF RFC 2560: X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP. [Online] June 1999. [Cited: 22 September 2011.]
http://www.ietf.org/rfc/rfc2560.txt

28. **European Telecommunications Standards Institute.** ETSI TS 101 861: Time stamping profile. [Online] March 2002. [Cited: 22 September 2011.] *http://docbox.etsi.org/EC_Files/EC_Files/ts_101861v010201p.pdf*

29. —. ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES). [Online] January 2011. [Cited: September 22, 2011.]
http://www.cryptopro.ru/sites/default/files/products/tsp/ts_101733v010803p.pdf

30. **Internet Engineering Task Force.** IETF RFC 3852: Cryptographic Message Syntax (CMS). [Online] July 2004. [Cited: 22 September 2011.] *http://www.ietf.org/rfc/rfc3852.txt*

31. **European Telecommunications Standards Institute.** ETSI TS 102 734: Electronic Signatures and Infrastructures; Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES). [Online] v1.1.1, February 2007. [Cited: 22 September 2011.]
http://www.etsi.org/deliver/etsi_ts/102700_102799/102734/01.01.01_60/ts_102734v010101p.pdf

32. —. ETSI TS 101 903: XML Advanced Electronic Signature. [Online] v1.4.1, June 2009. [Cited: 22 September 2011.] *http://uri.etsi.org/01903/v1.4.1/ts_101903v010401p.pdf*

33. **W3C.** W3C Recommendation: XML Signature Syntax and Processing. [Online] June 2008. [Cited: 25 September 2011.] http://www.w3.org/TR/xmldsig-core/.

34. **European Telecommunications Standards Institute.** ETSI TS 102 904: Electronic Signatures and Infrastructures; Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES). [Online] v1.1.1, February 2007. [Cited: 22 September 2011.]
http://www.etsi.org/deliver/etsi_ts/102900_102999/102904/01.01.01_60/ts_102904v010101p.pdf

35. —. ETSI TS 102 778 (multipart): Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles.

36. **CEN.** CWA 15579: E-invoices and digital signatures. [Online] July 2006. [Cited: 25 September 2011.] *ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eInvoicing/CWA15579-00-2006-Jul.pdf*

37. **Internet Engineering Task Force.** IETF RFC 3335: MIME-based Secure Peer-to-Peer Business Data Interchange over the Internet (AS1). [Online] September 2002. [Cited: 25 September 2011.] *http://tools.ietf.org/html/rfc3335*

38. —. IETF RFC 4130: MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2). [Online] July 2005. [Cited: 25 September 2011.] *http://tools.ietf.org/html/rfc4130*

39. —. IETF RFC 4823: FTP Transport for Secure Peer-to-Peer Business Data Interchange over the Internet, Applicability Statement 3 (AS3). [Online] April 2007. [Cited: 25 September 2011.] *http://tools.ietf.org/html/rfc4823*

40. **European Telecommunications Standards Institute.** ETSI TS 102 640 (multipart): Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies. [Online] October 2008. [Cited: 25 September 2011.] *http://www.e-imza.com.tr/dokuman/ts_10264001v010101p.pdf*

41. **Internet Engineering Task Force.** IETF RFC 5024: ODETTE File Transfer Protocol 2. [Online] November 2007. [Cited: 25 September 2011.] *http://tools.ietf.org/html/rfc5024*

42. **International Organization for Standardization.** ISO 32000-1: Document management - Portable document format - Part 1: PDF 1.7. 2008.

43. **European Commision.** xxxxx: TAXUD Guidelines on eletronic invoicing (NOT FINAL TITLE, to be published). [Online]

44. **European Commission Expert Group on e-invoicing.** Final Report of the Expert Group on e-Invoicing. [Online] November 2009. [Cited: September 25, 2011.] *http://ec.europa.eu/internal_market/consultations/docs/2009/e-invoicing/report_en.pdf*

45. **European Telecommunications Standards Institute.** ETSI TS 102 778-1: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES. [Online] v1.1.1, July 2009. [Cited: 22 September 2011.] *http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf*

46. —. ETSI TS 102 778-2: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1. [Online] July 2009. [Cited: 27 September 2011.] *http://www.etsi.org/deliver/etsi_ts/102700_102799/10277802/01.02.01_60/ts_10277802v010201p.pdf*

47. —. ETSI TS 102 778-4: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile. [Online] December 2009. [Cited: 27 September 2011.] *http://www.etsi.org/deliver/etsi_ts/102700_102799/10277804/01.01.02_60/ts_10277804v010102p.pdf*

48. —. ETSI TS 102 778-5: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures. [Online] December 2009. [Cited: 27 September 2011.] *http://www.etsi.org/deliver/etsi_ts/102700_102799/10277805/01.01.02_60/ts_10277805v010102p.pdf*

49. —. ETSI TS 102 778-3: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles. [Online] July 2010. [Cited: 27 September 2011.] *http://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.02.01_60/ts_10277803v010201p.pdf*

5 Definitions and abbreviations

5.1 Abbreviations

AdES	Advanced Electronic Signature
AICPA	The American Institute of Certified Public Accountants
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 (29))
CICA	Canadian Institute of Chartered Accountants
CMS	Cryptographic Message Syntax (see RFC 3852 (30))
DUNS	D-U-N-S® Number (Data Universal Numbering System),
EDI	Electronic Data Interchange
ETSI	European Telecommunications Standards Institute
ITS	Intrusion Detection System
OCSP	Online Certificate Status Protocol (RFC 2560 (27))
PAdES	PDF Advanced Electronic Signature (see TS 102 778 (35))
PDF	Portable Document Format (see ISO 32000 (42))
QC	Qualified Certificate
QES	Qualified Electronic Signature
REM	Registered mail
RFC	Request for Comment http://www.rfc-editor.org/rfc.html
SME	Small and Medium Enterprise
SSCD	Secure Signature Creation Device
SSL / TLS	Secure Socket Layer / Transport Layer Security (see RFC 5246 (13))
TSA	Time-Stamping Authority
TS	(ETSI) Technical Specification
XAdES	XML Advanced Electronic Signature (see TS 101 733 (29))

5.2 Definitions

The CEN Code of Practice Glossary of Terms (3) defines a consistent terminology and a definition of roles and responsibilities of distinct actors of the e-invoicing process, to be adopted by trading parties, service providers and public authorities. The terms defined therein and adopted in the Compliance Guidelines are (further explanation in footnotes):

- 3-Corner Model
- 4-Corner Model (or Multi Corner Model[20])
- Advanced Electronic Signature (AdES)
- Buyer
- Conversion
- E-Invoicing Service Provider or Service Provider[21]
- Electronic Data Interchange (EDI)[22]
- Electronic Invoice
- Electronic Signature
- Format[23]
- Invoice Data
- Invoice Header Data
- Invoice Line Data
- Issuing an E-Invoice in name and on behalf of the Supplier
- Issuer of an Invoice
- Secure Signature-creation Device
- Self-Billing[24]
- Supplier
- Storage Period of an Electronic Invoice
- Trading Parties (aka Trading Partners)
- VAT or Value-Added Tax

In addition, the following terms have the following meanings in these compliance guidelines (the Guidelines). (Where necessary, in the definitions above and below, substitute “Supplier” with “Customer in the case of self-billing”):

a) **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.

b) **Archiving**; The business process and associated information system(s) enabling users to Store, for as long as is required by applicable law, E-Invoices, associated documents and/or audit trails and subsequently retrieve and consult or process them for specific business or regulatory compliance purposes.

c) **Audit of an E-Invoice or associated business processes**: The process of inspection of the content 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 or others, such as a chartered accountant or an internal audit

---

20 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.

21 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.

22 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 (at least 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 (24), 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 which may include forms EDI accessed via a web browser (see section 3.7.1).

23 According to the preset syntax and/or schema such as UN/EDIFACT, UNCEFACT, xCBL, cXML or PIDX.

24 See further section 3.8.1.

committee to ascertain the compliance of that E-Invoice and the underlying sales / purchase transactions with applicable law.

d) **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. Also see definition relevant to the discussion in section on Class A Business Controls.

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

f) **Authenticity of an E-Invoice:** "Authenticity of the origin" of an E-Invoice means the assurance of the identity of the supplier or the issuer of the invoice.

g) **Business control**: See the definition of Internal Control below. Also see definition relevant to the discussion in section on Class A Business Controls.

h) **E-Invoice life cycle**: A process comprising (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 Customer; and (3) storage of the electronic invoice during the storage period by or on behalf the Supplier and the Customer.

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

j) **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.

k) Integrity of an E-Invoice: "Integrity of content" of an E-Invoice means that the content required according to Directive 2010/45/EU Article 233 (2) has not been altered.

l) **Internal Control**: A process, affected by an organization's people and information technology (IT) systems, designed to help the organization accomplish specific goals or objectives. The EU Directive refers to Internal Controls as Business Controls.

m) **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.

n) **Legibility of an E-Invoice**: To be legible an invoice must be human-readable, which means an auditor (e.g. Tax Administration or accountant) is able to interpret the content of an E-Invoice.

o) **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.

p) **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.

q) **Qualified Certificate:** A certificate which meets the requirements laid down in Annex I of Directive 1999/93/EC and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II of the same Directive.

r) Qualified Electronic Signature: Advanced electronic signature based on a qualified certificate and created by a secure signature creation device.

s) **Public Key Certificate (certificate)**: The public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it. (ISO/IEC 9594-8:2005)

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

u) **Spoofing**: An attacking technique used to gain unauthorized access to computers, applications, etc. whereby the intruder masquerades as a different entity, e.g. indicating that a message is coming from a trusted host.

v) **Storage:** The keeping (retention) of information for future reference.

w) **UN-Layout Key (UNLK)**: United Nations Layout for Trade documents, including the invoice. UN Recommendation 1 and Recommendation 6; ISO 6422 (20).

x) **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.

Annex 1: E-Invoicing Compliance Guidelines Matrix

Most of the Risks, Requirements, Controls and Reference Examples specified in the following Compliance Guidelines Matrix have been tailored for E-invoices, but in some cases they may also apply to paper invoicing, making up a valuable tool also in the latter case. It is left up to the readers to assess whether each of them applies to their paper invoicing environment.

The Compliance Guidelines Matrix is downloadable from: *ftp://ftp.cen.eu/PUBLIC/CWAs/eInv2/Annex1_Compliance_Guidelines_Matrix_19102009.xls* and is accesible from the E-Invoice Gateway http://www.e-invoice-gateway.net/. The same information can be accessed via the Interactive User Interface on that same web site. See Annex 2 for more information.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
All	**(Supplier and Buyer Side)**									
All	0 - Generic	x	x	x	x	0100	General risks on IT systems	Support general commercial good security practices	Implement recognised standards based on good practices for the security, continuity and integrity of the business system. These practices should be applied and audited in line with the requirements of recognised good practices so as to provide a robust control framework. See sections 4.8.5.1 and 4.8.5.2.	Taking into account the size and nature of the organisation, appropriate (general IT) controls should be implemented. Examples of such controls can be found in recognised standards such as ISO/IEC 27001
All	0 - Generic		x	x	x	0200	Service provider has responsibilities to both the supplier and the buyer, with potential for conflicts of interest.	The responsibilities of each party must be clearly delineated.	The processes implementing the supplier and buyer requirements should be clearly separable with separate audit records, separate archives, separate management control parameters and operated under separate management roles. Separation should be procedural and can also be physical or logical.	Clearly document on whose behalf functions are implemented
All	0 - Generic		x		x	0300	The process and procedures applied cannot be audited as they are undocumented	Documentation of processes and procedures should be in place.	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 E-Invoices during the storage period.	

25 The order can be adjusted

26 The examples listed are non-exhaustive and provided only to illustrate the kind of measures envisaged as being used.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
All	A - Trading partner onboarding		x	x	x	A100	Trading partners use the E-Invoicing system without prior identification and clearance.	The trading partners must ensure proper trading partner identification and clearance.	Trading partners must accept and know each other. Identification and clearance can be performed through e.g. trade registers and/or commercially available supporting data.	DUNS lookup, trade register or Chamber of Commerce etc. checks - these processes can be performed by a service provider for the trading partners
All	A - Trading partner onboarding	x	x	x	x	A200	E-Invoices are sent to a trading partner that does not accept them.	The decision to send and accept E-Invoices is auditable.	Rules in agreement (e.g. general terms and conditions)	
All	A - Trading partner onboarding		x	x	x	A300	Trading partners are given access to the e-invoicing system without a sufficient contract regulating rights and responsibilities, including as regards taxes, data use and confidentiality, responsibility for service providers and change management, of both trading partners, and change management, of both parties.	The trading partner should ensure that other trading partners sign a comprehensive and enforceable agreement before providing access to the trading partner's system. There must be an explicit agreement if tax relevant parts are outsourced to service providers.	There should be a process to make sure that there is an agreement as a result of the onboarding phase.	[Model agreements for this purpose should be developed]
All	A - Trading partner onboarding		x	x	x	A400	Trading partners are given access to the e-invoicing system without sufficient training of key staff.	The trading partners/service providers should ensure that the trading partner in question is trained to perform the required system activities, including processes for error and exception handling.	The trading partner/service provider should make documentation or other appropriate learning tools available that allow the trading partner to effectively train relevant staff. A minimum skill level should be verifiably obtained by key staff.	Online documentation and tool tips, multi-lingual support, clearly mark user IDs to indicate and separate test and production accounts (that no test account message can be sent to production accounts).
All	A - Trading partner onboarding		x	x	x	A500	Inconsistent application of security of information exchange between parties leaving vulnerabilities.	Security mechanisms employed across parties involved with exchange of E-Invoice shall address identified risks in a coherent manner.	Parties involved in exchanging E-Invoices should agree on security mechanisms or controls applied to address identified threats to the exchange of information.	
All	A - Trading partner onboarding		x	x	x	A600	Trading partners are given access to the e-Invoicing system without successful testing the communication based on pre-agreed criteria.	The proper technical functioning of the trading partner's access to the e-Invoicing system should be ensured prior to production.	The trading partners/service providers test plans and test results should be agreed by both parties.	Online testing and tight controls; separated testing and production accounts; self service facilities to create test E-Invoices.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
All	A - Trading partner onboarding		x			A700	EDI E-Invoices are issued to buyers without an interchange agreement.	An interchange agreement is required if EDI E-Invoices are sent and received, otherwise the E-Invoice is not valid (VAT law).	Address this risk in the procedure for initiating sending EDI E-Invoices. See section 4.5.1.	Model-agreement
All	A - Trading partner onboarding				x	A800	Trading partners use different EDI-structures	The proper technical functioning of the trading partner's EDI-structures should be ensured prior to production.	The trading partner's test plans and test results shall be agreed.	Online testers and tight controls; separated testing and production accounts; self service facilities to create test E-Invoices.
S	**Supplier Side**									
S	1 - Prepare invoice data	x	x	x	x	1100	Invoice data is not prepared for a supply requiring an invoice	It must be ensured that an E-Invoice is raised for all supplies for which there is an obligation to issue an E-Invoice for VAT purposes.	Application audits and internal control actions. Audit trail from supply to invoiced supply.	System shows invoice balance per Purchase Order + supplier's ERP (Enterprise Resource Planning) system control. Reports of unfulfilled orders and un-invoiced deliveries
S	1 - Prepare invoice data	x	x	x	x	1200	Supply is E-Invoiced but not reported in general ledger/VAT declaration	Audit trail from supply to reported revenue enabled by segregation of duties between preparing the E-Invoice and the receiving of the payment.	Segregation of duties should fit with the size of the company. Logical access controls should map to an appropriate segregation of duties, which is evidenced by the end-to-end audit trail.	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.
S	1 - Prepare invoice data	x	x	x	x	1300	Unauthorized persons can add, alter or delete invoice data.	The supplier must take steps to prevent unauthorised changes to the content of the E-Invoice.	Segregation of duties should fit with the size of the company. Logical access controls should map to an appropriate segregation of duties, which is evidenced by the end-to-end audit trail.	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.
S	1 - Prepare invoice data	x	x	x	x	1400	The invoice data do not contain all mandatory information	The invoice data must contain at least the data prescribed by the applicable law.	Controls are used to check required data before E-Invoice creation (e-Signing as the last step of creation if the trading partners use Class C controls) + constraints are used for conditional fields to ensure that the E-Invoice shows all mandatory data. The completion of data fields must be ensured in the application.	Online and [XML/EDI] syntax controls validate required data; conditional fields like buyer VAT ID are validated based on range and format checking, including validation algorithms where appropriate.
S	1 - Prepare invoice data	x	x	x	x	1500	The invoice data are not prepared on time	The issue of an E-Invoice must be within the time prescribed by applicable law.	Application audits and internal control actions. Audit trail from service to invoice turnover.	

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
S	1 - Prepare invoice data	x	x	x	x	1600	The person accountable for preparing the dataset cannot be identified after the event	A person must be accountable for each E-Invoice (whether prepared manually or automatically)	Audit trail identifying the accountable person.	Keeping an audit log of access and activity in the application or DBMS (Data Base Management System), including the identity of the user (or process). Keep record of accountable persons
S	1 - Prepare invoice data	x	x	x	x	1700	Changes to invoice data, resulting in a break in the audit trail between the source transaction data and the invoice data.	The invoice data must at all times be consistent with the source transaction data.	The technical design of the application should ensure this; the data flow must be clear.	In the ERP (Enterprise Resource Planning) system, the quotation, order, delivery, E-Invoice or other business documents are cross referenced to each other.
S	1 - Prepare invoice data **Prepare corrective invoice data**	x	x	x	x	1800	A corrective invoice data set (including credit note) without reference to an original invoice is prepared.	The corrective E-Invoice data set includes a reference to identify the original E-Invoice data set. It should be possible to identify corrective E-Invoices.	Application controls and internal control actions. It is advised to at least have reference to the original E-Invoice number.	E.g. by means of reference of original E-Invoice number and original E-Invoice date. Separate series of E-Invoice numbers for corrective E-Invoices. Audit trail.
S	2 - First mile	x	x	x	x	2100	The invoice data transferred by the supplier to the service provider can be altered or added to during the transmission.	Ensure authenticity and integrity of invoice data whilst being sent.	The invoice data shall be transferred in a way that : a) Protects the integrity of the data communicated, b) Authenticates the source of the data. See section 4.8.5.5.	i) Transport Layer Security (RFC 4346) with passwords. ii) Business Data Interchange over the Internet Applicability Statement 1, 2, 3 with signatures (RFC3335, RFC 4130, RFC 4823) iii) Secure network service provided by Value Add Network service provider. iv) Secure messaging services such as ITU-T X.400 or S/MIME (RFC 3851) . v) Integrity measures, such as hash totals or reconciliation overviews vi) Registered email such as defined in TS 102 640

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
S	D - Integrity and authenticity management			x		D100	Invoice signer does not carry out obligations regarding security of keys and certificates. Private (signing) key is not held in a manner which ensures sole control	The invoice signer must ensure sole control of the private key and comply with its obligations regarding security and reporting of potential compromises.	The invoice signer shall comply with its obligations regarding security of the private keys and reporting potential compromises. In addition, the signature shall be created using mechanisms commensurate with identified risk relating to fraud to assure protection of keys.	All trading partners that may be recipients of invoices should be informed of any suspected compromise of the signing key employed, and a) a cryptographic device conforming to an internationally recognised standard that assures sole control over the private key (e.g. FIPS 140-2 level at least 2 or 3 , Common criteria EAL at least 4) or b) Software keys held on a system that is held in an environment which is protected such that the key is under sole control of the business entity issuing the invoicing.
S	D - Integrity and authenticity management **Certificate management (CA Issued)**			x		D200	Certificate used for AdES on E-Invoices is issued by a CA (Certification Authority) which does not properly manage its operations.	The CA must operate under good practice for PKI (Public Key Infrastructure) systems	The signature shall be supported by certificates issued by a certification authority operating to recognised good practices. The certificate should include the identity of the legal entity applying the signature. See section 4.6.2.	Examples of recognized good practices: ETSI TS 102 042, TS 101 456 or AICPA/CICA Webtrust.
S	D - Integrity and authenticity management **Certificate management (CA Issued)**		x		x	D300	Certificate used to protect invoice data exchanges is issued by a CA which does not properly manage its operations.	CA issuing any certificates used to protect data exchange must operate under good practice for PKI systems	Data shall be protected by certificates issued by a certification authority operating to recognised good practices. See section 4.6.2.	Examples of recognized good practices: ETSI TS 102 042, TS 101 456 or AICPA/CICA Webtrust, Extended Validity certificates (for SSL / TLS certificates) as defined by the CA/Browser Forum.
S	D - Integrity and authenticity management **Certificate management (self-signed)**			x		D400	Certificate created fraudulently by someone impersonating the identity of the signer	Before using the self-signed certificate, it must be authenticated to all trading partners as coming from a trusted source. The use of self-signed certificates is not accepted in all EU Member States.	The private key associated with a self-signed certificate should be tied to a proof of identity that has been obtained in the onboarding process at a level comparable to recognised good practices for CA's (Certification Authority). Certificates shall be previously exchanged between parties in a way that authenticates the identity of the source.	Examples of recognized good practices for CA's: ETSI TS 102 042, TS 101 456 or AICPA/CICA Webtrust.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
S	3 - Create E-Invoice		x	x	x	3050	E-Invoice contains executable code; the integrity of the E-Invoice can no longer be guaranteed.	Ensure E-Invoice does not contain executable code.	The creator of the E-Invoice shall take steps to ensure that there is no executable code in the E-Invoice. The contract with trading partner should state that no executable code will be part of an E-Invoice. See section 4.8.5.4.	Disable any use of macros within the E-Invoice. Scan E-Invoice for virus and other malicious codes. Do not use document formats capable of carrying hidden code and macros.
S	3 - Create E-Invoice	x	x	x	x	3100	An E-Invoice is created more than once.	It must be ensured that an E-Invoice can only be created once.	The workflow must ensure that E-Invoices are created once, whether electronically or on paper.	
S	3 - Create E-Invoice	x	x	x	x	3150	Not all E-Invoices issued in name and on behalf of the supplier are reported in General Ledger by the supplier	Method to verify the issued E-Invoices	In contract and internal control measures. Reports of issued E-Invoices to the supplier.	
S	3 - Create E-Invoice **E-Invoice created by service provider**	x	x	x	x	3200	Service provider adds invoice data that does not originate from the prepared invoice data by the supplier (outside of an agreed enrichment service).	Service provider shall not add invoice data (outside of an agreed enrichment service)	Measures must be in place to prevent and detect any creation of E-Invoices that were not prepared or agreed by the supplier. The contract between service provider and supplier must prevent it. Logical access control at the service providers system. Logical access controls should map to an appropriate segregation of duties, which is evidenced by the end-to-end audit trail.	Audit reports and/or access to service provider-stored E-Invoices to make sure that only E-Invoices have been issued that originate from the prepared E-Invoice data by the supplier.
S	3 - Create E-Invoice **E-Invoice created by service provider**	x	x	x	x	3250	The E-Invoice as created by the service provider does not contain all agreed upon data.	The E-Invoice as created by the service provider must contain all agreed upon data.	Control conversion process, audit trail, rules in contract.	Substantive tests of a number of E-Invoices
S	3 - Create E-Invoice **E-Invoice created by service provider**	x	x	x	x	3300	The service provider does not create all E-Invoices	The service provider must create all of the E-Invoices provided by the supplier.	Control conversion process, audit trail, rules in contract.	Generate totals to audit complete issue of E-Invoices.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
S	3 - Create E-Invoice **E-Invoice created by service provider**	x	x	x	x	3350	The service provider adds data to the E-Invoice or modifies it, the supplier does not have this information.	The supplier is still responsible for the accuracy and completeness of the content of the E-Invoices. The supplier must (be able to) access all data of his E-Invoices.	Control conversion process, audit trail, rules in contract. The supplier should always have access to the issued E-Invoices. Conversion Process should be performed in accordance with agreed mapping processes that are tested and auditable and which alter only the Format of the E-Invoice and do not modify the recipient's ability to discern all mandatory information.	Substantive tests of a number of E-Invoices
S	3 - Create E-Invoice	x		x		3400	Signature is not created.	The E-Invoice is provided with an advanced electronic signature to protect its integrity and authenticity.	The application should ensure that signatures are applied. The signature shall be created in accordance to an internationally recognised standard signature format. Verify signature on a number of E-Invoices. See section 4.8.5.3.	- CAdES-T s defined in ETSI TS 101 733 & profiled in TS 102 734 - XAdES T as defined in ETSI TS 101 903 & profiled in TS 102 904 - PDF Signature as specified in ISO 32000 and profiled in ETSI TS 102 788
S	3 - Create E-Invoice	x		x		3450	Signature is created with an invalid or expired certificate	The E-Invoice must be provided with an advanced electronic signature with a valid certificate.	In order for the supplier to provide easy evidence of CA-issued certificate validity at the time of signing, the signing party should timely validate the signature to ensure that the information required to re-verify the signature is readily available. See section 4.8.5.3.	See process step archiving and auditability for (sub-process) AdES. Modern applications and standards will handle this automatically.
S	3 - Create E-Invoice			x		3500	Not all mandatory E-Invoice data are signed.	All mandatory data according to applicable law must be signed.	The application must ensure that all mandatory E-Invoice data is signed.	
S	3 - Create E-Invoice		x			3550	Structure of the E-Invoice differs from the structure of the E-Invoice as agreed in the current interchange agreement	Structure of the E-Invoice must comply with the structure of the E-Invoice as agreed in the current interchange agreement.	A correct validation mechanism should be maintained in order to automatically validate the structure against the interchange agreement. See also the requirements for testing in the onboarding process step (A) in section 4.2 in Commentary report, figures 1 & 2.	
S	3 - Create E-Invoice		x			3600	The integrity and authenticity of a summary document might not be guaranteed. Regardless of its form; paper or electronic	To the extent that a summary document is used for evidencing completeness, the integrity and authenticity of the summary document (paper report) must be guaranteed.	Measures should ensure integrity and authenticity of summary documents. See section 4.8.5.3.	Advanced Electronic Signature applied to summary documents. Summary document printed on the suppliers stationary.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
S	3 - Create E-Invoice **E-Invoice created by service provider**	x	x	x	x	3650	An E-Invoice is created by both the supplier and the service provider (not according to agreement)	It must be ensured that an E-Invoice can only be created by the designated issuer in the contract. It must be clear between the parties who issues an E-Invoice.	The controls should ensure that E-Invoices are created/issued only once.	
S	4 - Send or make available	x	x	x	x	4050	Created E-Invoices are not sent or made available on time.	The supplier must ensure that E-Invoices are sent or made available, timely according to applicable law	Action of internal control, included in application or agreement with service provider, if appropriate.	
S	4 - Send or make available	x	x	x	x	4100	Dispute over whether an E-Invoice has been sent/made available.	E-Invoices have to be sent/made available (general).	Maintain audit records of sending / retrieving E-Invoices.	The sending or retrieval of the E-Invoice, and any associated acknowledgement, will be recorded. Preferably make use, where available, of systems that produce trusted evidence of sending and, where applicable, of delivery.
S	4 - Send or make available	x	x	x	x	4120	Dispute over whether an E-Invoice has been sent via E-mail.	E-Invoices have to be sent (e-mail).	Maintain audit records of sending / retrieving E-Invoices.	When using e-mail, ETSI TS 102 640 is a multi-part Technical Specification laying down provisions for a Registered E-Mail (REM) mechanism suitable to provide the said evidences for sent E-Invoices.
S	4 - Send or make available		x			4150	Authenticity is based on an invalid or expired certificate.	When a certificate is used to protect the transport of an unsigned E-Invoice, the certificate must be valid.	Internal control of certificate validity. See section 4.8.5.3.	See process step archiving and auditability for (sub-process) AdES. Modern applications and standards will handle this automatically.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
S	4 - Send or make available	x	x			4200	False invoice data is sent by party masquerading as supplier or modified during transport	Authenticity and integrity of the E-Invoice must be guaranteed within the EDI-process	The invoice data shall be transferred in a way that: a) Protects the integrity of the data communicated, b) Authenticates the source of the data. See section 4.8.5.5.	i) Transport Layer Security (RFC 4346) with passwords. ii) Business Data Interchange over the Internet Applicability Statement 1, 2, 3 with signatures (RFC3335, RFC 4130, RFC 4823) iii) Secure network service provided by Value Add Network service provider. iv) Secure messaging services such as ITU-T X.400 or S/MIME (RFC 3851). v) Integrity measures, such as hash totals or reconciliation overviews vi) Registered email such as defined in TS 102 640
S	4 - Send or make available		x		x	4250	The buyer is unaware of an E-Invoice being made available.	There must be an understanding between trading partners when an E-Invoice is sent or is made available.	Send notifications; It is good practice to address this risk in the application; record when and to whom the notifications were sent. Rules in contract.	If email is used for the notification, request delivery receipt by email from recipient.
S	4 - Send or make available				x	4300	Presented E-Invoices are not reviewed by buyer	In order to correctly perform the receipt process, the buyer must review the E-Invoices.	It is good practice to have a clear understanding with the buyer that it is his responsibility to review the E-Invoice. Log access to the E-Invoice.	Within the web environment the audit trail of viewing the E-Invoices can be made visible. Alert in the application if the E-Invoice is not accessed within a specific time period.
S	4 - Send or make available				x	4350	E-Invoices are presented twice with the result that the buyer may claim the VAT twice, whereas the supplier only reports the VAT once.	E-Invoices may only be presented once and must be uniquely identifiable. E-Invoices should normally only be re-transmitted because for techincal reasons the originnally issued invoice was not received by the recipient.	The workflow should ensure that E-Invoices are presented once and that the transaction is processed correctly. Presented E-Invoices must therefore be uniquely identifiable, e.g. from the document name and unique number in a way to facilitate prevention of the same invoice from being processed multiple times by the recipient. Before re-transmitting an invoice, the invoice issuer should verify non-receipt by the recipient. There should be a documented process for verify non-receipt and evidence of the verification should be stored in a way to link it back to the relevant invoice.	
S	4 - Send or make available				x	4400	Not all E-Invoices are presented. Special attention for corrective E-Invoices.	All E-Invoices must be presented. Special attention for corrective E-Invoices.	Application audits and internal control actions.	

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
S	4 - Send or make available				x	4450	The wrong web server is consulted (spoofing)	The server on which the E-Invoices are accessible must authenticate itself verifiably towards the buyer	A mechanism shall be in place to authenticate the web server. See also requirements for Integrity and authenticity management (Process step D in section 4.2, figures 1 & 2). See also section 4.8.5.5.	Authentication by SSL/TLS with a sufficiently strong server certificate. The server on which E-Invoices are held must be made available by buyer with a link in an email (legal requirement in some Member States). Use of extended validation certificates as defined by CA Browser forum is recommended.
S	4 - Send or make available				x	4500	The E-Invoice is modified whilst being held on web server	The E-Invoice cannot be changed in authorised manner whilst on web server.	Web system operates under recognised good practices for security of web servers and controls access to E-Invoice.	
S	4 - Send or make available **E-Invoice created by service provider**		x	x	x	4550	It is not clear who issues the E-Invoice	It must be ensured that a E-Invoice can only be issued by the designated issuer in the contract. It must be clear between the parties who issues an E-Invoice.	Rules in the contract between the trading partner and service provider, should clarify the issuer the E-Invoices. The E-Invoice can contain a statement that it was issued by a third party in name and on behalf of the supplier (this is mandatory in some Member States).	
S	4 - Send or make available	x	x	x	x	4600	Invoice data used for processing is different from original E-Invoice	Conversion is required for automatic data processing in back-end systems, but the original E-Invoice needs to be kept from which the converted E-Invoice can be audited.	Control conversion process, audit trail, mapping rules in contract. The supplier and buyer should always have access to the original E-Invoices. See sections 4.8.4, 4.8.5.1, 4.8.5.2 and 4.8.5.5.	1) Use mappings which are well documented, version controlled and tested. 2) Represent the original E-Invoice as a single, signed field string (with delimiters) within the converted invoice. The converted invoice data can be automatically checked against the original invoice data.
S	4 - Send or make available	x	x	x	x	4650	Converted E-Invoice is sent, but original E-Invoice is not available to supplier and/or buyer / not treated as the original – in case of an audit, different E-Invoices are presented as the original from each party.	Conversion is required for automatic data processing in back-end systems, but the original E-Invoice must be made available and considered as the original E-Invoice by all parties	Action of internal control, included in application or agreement with service provider, if appropriate. See sections 4.8.4, 4.8.5.1, 4.8.5.2 and 4.8.5.5..	Comparison of daily counts for original versus converted E-Invoices Representing the original E-Invoice as a single, signed field string (with delimiters) within the converted E-Invoice avoids the situation of having separate E-Invoice message (original and converted)
All	**(Supplier and Buyer**									

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
	Side)									
All	D - Integrity and authenticity management **This process step applies to any exchange of data between parties of the E-Invoice transport chain**	x	x		x	D500	The invoice data or E-Invoice transferred between chain participants can be altered or added to during the transmission	Ensure authenticity and integrity of data whilst being sent.	The data shall be transferred in a way that : a) Protects the integrity of the data communicated, b) Authenticates the source of the data. See section 4.8.5.5.	i) Transport Layer Security (RFC 4346) with passwords. ii) Business Data Interchange over the Internet Applicability Statement 1, 2, 3 with signatures (RFC3335, RFC 4130, RFC 4823) iii) Secure network service provided by Value Add Network service provider. iv) Secure messaging services such as ITU-T X.400 or S/MIME (RFC 3851) . v) Integrity measures, such as hash totals or reconciliation overviews vi) Registered email such as defined in TS 102 640 vii) If AdES was applied integrity can be validated at recipient
All	C - Archiving and auditability			x		C100	It is not possible to verify that the certificate was valid at the time of signing or receipt of the E-Invoice	Advanced electronic signatures must remain verifiable during the storage period.	When issuing an E-Invoice the signature used should be verified (see above process step Create E-Invoice; step 3 in section 4.2, figures 1 & 2.) and all the information necessary to re-verify the validity of the signature at or around the signing time shall be readily available. See also section 4.8.4.	- recording certificates and revocation information - CAdES-C, CAdES-A or CAdES-X in ETSI TS 101 733 & profiled in TS 102 734 - XAdES-C, XAdES-A or XAdES-X as defined in ETSI TS 101 903 & profiled in TS 102 904 Note: Equivalent forms to CAdES/XAdES -C to -A for long term validation of PDF Signatures (PAdES) has been published by ETSI as multi-part specification ETSI TS 102 778.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
All	C - Archiving and auditability			x		C150	It is not possible to verify the integrity of the E-Invoice	Advanced electronic signatures must remain verifiable during the storage period.	The integrity of the signed E-Invoice, including information used to re-verify the signature (see above process step Create E-Invoice; 3 in section 4.2, figures 1 & 2.), shall be maintained beyond the lifetime of the signature algorithm and certificates. See also section 4.8.4.	1) Applying archive timestamp to signature as in CAdES-A as defined in ETSI TS 101 733 & profiled in TS 102 734 2) Applying archive timestamp to signature as in XAdES-A as defined in ETSI TS 101 903 & profiled in TS 102 904 3) Employing WORM devices within an auditable archive process. 4) Using third party service trusted to archive data (e.g. notary) 5) Employing archive system which maintains the integrity of data Note: Equivalent forms to CAdES/XAdES -XL and -A for long term validation of PDF Signatures (PAdES) has been published by ETSI as multi-part specification ETSI TS 102 778.
All	C - Archiving and auditability	x	x	x	x	C200	E-Invoices are not archived for statutory archiving period	The issued and received E-Invoices must be archived for the statutory archiving period under the applicable law(s). Data guaranteeing authenticity and integrity must also be stored.	This needs to be addressed in fit for purpose archiving procedures.	
All	C - Archiving and auditability	x	x	x	x	C250	The E-Invoices are not available within a reasonable period	At the request of a tax inspector, the E-Invoice must be made available promptly over the full mandatory storage period.	Inquiry can be executed within a reasonable period of time. Archival must be implemented in a way suitable to ensure that during the archival period: a) the archived E-Invoices are always available, i.e. they are not arbitrarily or accidentally destroyed; b) it is possible to identify and fetch one specific E-Invoice/E-Invoices set through keywords within a period suitable to meet the Tax Authority requirements, consistently with the applicable legislation.	Online access can be used and provides prompt access.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
All	C - Archiving and auditability	x	x		x	C300	Archived E-Invoices can be modified or removed within the agreed archiving period	The authenticity and integrity of the content of the E-Invoices stored must be guaranteed throughout the storage period.	The E-Invoice and audit records regarding handling of the E-Invoice, including information on authentication checks carried out, shall be protected by mechanisms that assure the integrity of data throughout the storage period. See sections 4.8.5.2 and 4.8.4.	- the use of WORM (Write Once Read Many) type devices - secure archive
All	C - Archiving and auditability	x				C350	Stored E-Invoices are not readable (by humans or by machine) due to degradation in the media	The E-Invoice archiving service provider must set up a proper Information Security Management System addressing media management	The archiving service provider must comply with Information Security Management Systems provisions, e.g. based on the ISO/IEC 27001/27002 addressing also the risk of media degradation. In particular a Business Continuity (or at least a Disaster Recovery) Plan shall be in force.	ISO/IEC 27001/27002, ETSI TS 102 573 and ETSI TS 101 533-01/TR 101 533-02
All	C - Archiving and auditability	x	x	x	x	C400	Stored E-Invoices are not readable (by humans or by machine) because their format is no longer processable with the available software and/or hardware	The E-Invoice archive system must ensure the stored documents are readable	When archived E-Invoices are not in a properly maintained standard format, the archiving service provider should comply with archival and Information Security Management Systems provisions by means of format conversion, where allowed, suitable to preserve the stored information semantics, or by keeping the software and/or hardware necessary to read the original information format	Two possible countermeasures: 1) Adopt for E-Invoices a properly maintained standard format. 2) Implement measures specified in Records Management related standards, such as ISO 15489, or related to information preservation security, such as ISO/IEC 27001/27002, ETSI TS 101 533-01/TR 101 533-02
All	C - Archiving and auditability	x				C470	E-Invoices archiving system can be affected by security incidents causing destruction of stored E-Invoices	The E-Invoices archiving system shall have in place an Information Security Management Systems envisaging a reliable Business Continuity Plan or at least Disaster Recovery Management.	The E-Invoices archiving system must comply with Information Security Management Systems provisions e.g. based on the ISO/IEC 27001/27002. In particular a Business Continuity (or at least a Disaster Recovery) Plan shall be in force	ISO/IEC 27001/27002, ETSI TS 101 533-01/TR 101 533-02
All	C - Archiving and auditability	x				C530	E-Invoices are deleted from the archive before the expiration of the applicable retention period or any extension thereof (e.g. ongoing litigation)	Storage time needs to be extended to match the applicable retention period or any extension thereof (e.g. ongoing litigation)	Routines must be in place to prevent deletion.	

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
All	C - Archiving and auditability	x				C600	Unauthorized access to archive	Archives for each taxable person should be separated, at least logically, in order to meet the necessary confidentiality needs, Applicable country legislation may add to this a legal requirement	Where physical separation of data is not implemented for each taxable person, at least such data must be accessible separately upon specific authentication.	
All	C - Archiving and auditability	x				C630	E-Invoices are not stored in a legally permitted country	E-Invoices cannot be stored physically in a specific country/region not accepted by the applicable legislations/rules (tax and account/commercial laws apply)	The archive service provider shall document the logics that, in compliance with the applicable legislation, govern the storage location and shall trace the E-Invoice transfer from and to specific Countries	Adopt (automated) from/to matrix based logic to trigger the archival in specific countries
All	C - Archiving and auditability	x				C670	Invoice cannot be retrieved due to inadequate management of index fields and of multiple places and providers of storage.	Minimum search/retrieval parameters must be supported, at least as per the applicable legislation, addressing, where necessary, also the storage distribution among multiple locations and service providers	Metadata and search indexes shall be managed according to existing storage standards and in compliance with the applicable legislation. The search index should support at least these keys: Invoice ID, Invoice Date, issue/ recipient name, Tax ID, VAT ID and, where necessary, shall keep track of different storage locations and service providers	ISO 14721 (OAIS), ISO 15489, ISO 23081, ISO 14641 (to be issued by 2011) (German BSI 03125)
All	C - Archiving and auditability	x				C700	If E-Invoices are stored at multiple storage service providers' retrieval can be unfeasible	The information owner must be able to access its own E-Invoice regardless of the number of storage service providers.	If all E-Invoices are not stored at the same storage service provider, suitable controls should be in place ensuring the information owner will be able to timely access any invoice at any time.	
All	C - Archiving and auditability		x	x	x	C730	E-Invoice may not be legible throughout the entire archiving period	Any authorised person shall be able to read the E-Invoice any time it is necessary.	Measures must be implemented to ensure that the E-Invoice can be legible throughout the entire archiving period.	
All	C - Archiving and auditability	x	x	x	x	C770	The legible form differs from the machine readable one	It must be demonstrable for the entire storage period that the invoice content in human legible form matches the machine readable form data.	It shall be demonstrable that the mapping between human legible and machine readable forms is correct.	If a style sheet is used, the correctness of its logic can be verifiable. Alternatively, there shall be a third party report asserting that at time of creation of the human readable form it was consistent with the machine readable form.
All	C - Archiving and auditability	x	x	x	x	C800	E-Invoices cannot be correctly reproduced because they make reference to external objects which are no longer available	All information necessary to allow invoices to be correctly interpreted must remain available for audit purposes	All mandatory invoice content must be archived, including external information, where applicable.	Either each invoice has all its relevant data self-contained, or relevant external information must be available.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
All	C - Archiving and auditability	x	x	x	x	C900	Audit trail is not correctly maintained	Adequate audit trail must be available throughout the storage period	Retain the audit trail, as appropriate to the "class". See section 4.8.5.2.	Retain key process information such as mappings, date recordings, logs etc. In addition, retain documents like Purchase Orders, Dispatch Advise. ETSI TS 101 533-1 and TR 101 533-2 provide indications on how to implement, manage and assess Information Preservation Systems ICT Security.
B	**Buyer Side**									
B	5 - Receipt and technical verification		x	x	x	5050	The buyer's environment is not available for receiving E-Invoices.	The technical availability for receiving E-Invoices must be ensured. The accurate, complete and prompt receipt of E-Invoices must be adequately ensured.	See also process steps Generic (0) and On-boarding (A) in section 4.2 in Commentary report, figures 1 & 2.. Procedure or application check on the completeness of the received E-Invoices and credit notes.	
B	5 - Receipt and technical verification	x	x	x	x	5100	E-Invoices are received multiple times	Multiple receipts of E-Invoices must be detected. Multiple E-Invoices must be removed and eliminated from further processing.	Application checks to detect E-Invoices received multiple times and exclude them from further processing after thorough analysis of the cause.	
B	5 - Receipt and technical verification		x	x	x	5150	E-Invoices are rejected for technical reasons	E-Invoice must be technically correct before being further processed. The rejected E-Invoices must be separately identifiable.	Thorough agreements about the technical standards of the E-Invoices should be present and adequately tested. Mechanism for promptly detecting technical inaccuracy and reporting to the sender by some form of notification (e.g. XML response or email). Processing of the received E-Invoice must be stopped. The sender should send the correct E-Invoice again or issue a credit note and a corrective E-Invoice.	
B	5 - Receipt and technical verification	x	x	x	x	5200	The buyer or the service provider on his behalf does not receive all E-Invoices (including credit notes)	The buyer or the service provider on his behalf must receive all E-Invoices sent.	There shall be proper procedures in place to ensure that all E-Invoices are properly received. Register all incoming E-Invoices	Handshake or confirmation of received E-Invoices where possible.
B	5 - Receipt and technical verification		x	x	x	5300	E-Invoice contains executable code.	Ensure E-Invoice does not contain executable code	The recipient shall verify that there is no executable code in the E-Invoice. The contract with the trading partner should state that no executable code will be part of an E-Invoice. See section 4.8.5.4.	Disable any use of macros in invoice encoding; Scan E-Invoice for virus and other malicious codes.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
B	5 - Receipt and technical verification		x	x	x	5350	The moment of formal receipt is unclear.	Measures of authenticity and integrity in transport should be in place until the moment of formal receipt. From the moment of formal receipt of the E-Invoice, integrity and authenticity must be ensured by preventing changes to the original E-Invoice.	Rules in contract	- ETSI TS 102 640 (REM) provides evidence also of the moment of delivery - AS2 provides for time-stamped Message Delivery (MDNs) upon receipt of messages
B	5 - Receipt and technical verification			x		5400	E-Invoice has no (or invalid) signature and/or issuer cannot be identified	The authenticity and integrity of the E-Invoice must be ensured by means of an advanced electronic signature. The authentication mechanism (at the buyer) must ensure the clear identification of the issuer.	Procedure or check in the application. Ensure that E-Invoice or e-mail is provided with an advanced digital signature. Otherwise reject E-Invoice. See section 4.8.5.3	
B	5 - Receipt and technical verification			x		5450	Uncertainty over the time which the signature was verified and hence possible ambiguity over the status of the certificate.	Record time that the advanced electronic signature is verified. (Different EU-member states have different rules.)	Have assurance that the correct time is recorded of the verification. See section 4.8.5.3.	If the signature does not already include a time-stamp or trusted time-mark then a trusted time-mark or time-stamp can be applied. (e.g. as specified in long term forms of CAdES, XAdES or PAdES)
B	5 - Receipt and technical verification			x		5500	Uncertainty over the rules applied in verifying a signature.	The process/software applied to verify the advanced electronic signature should be identifiable and reliable.	Records should be maintained of the process/software employed in validating the signature (for software including version and patches). See section 4.8.5.3.	Signature policy identifier as in EPES forms of CAdES, XAdES and PAdES may be Included
B	5 - Receipt and technical verification		x			5550	E-Invoice cannot be processed by the application.	E-Invoice must comply with the (technical) requirements of the current interchange agreement	E-Invoices are tested during Process step A Trading partner Onboarding in section 4.2 in Commentary report, figures 1 & 2. Any error should be reported to the sender by some form of notification (e.g. XML response or email)	Requirements may relate for example to the protection, registration of the E-Invoices in a register, mandatory fields, acceptability of an EDI report as evidence e.g. See Recommendation 94/820/EC

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
B	5 - Receipt and technical verification	x	x		x	5600	The content or format of the original E-Invoice is changed during transfer	It must be possible to detect whether issued E-Invoices are modified during transfer	Within the process of the buyer, there should be a verification/check that the agreed secure mechanisms are applied. See section 4.8.5.	i) Transport Layer Security (RFC 4346) with passwords. ii) Business Data Interchange over the Internet Applicability Statement 1, 2, 3 with signatures (RFC3335, RFC 4130, RFC 4823) iii) Secure network service provided by Value Add Network service provider. iv) Secure messaging services such as ITU-T X.400 or S/MIME (RFC 3851) . v) Integrity measures, such as hash totals or reconciliation overviews vi) Registered email such as defined in TS 102 640 For EDI this can also be protected using summary statements
B	5 - Receipt and technical verification **Conversion of E-Invoice-data**	x	x	x	x	5650	The E-Invoice is converted and treated as a new instance of the E-Invoice.	There can only be one E-Invoice and an audit trail must be maintained between it and any sets of invoice data derived from it.	Archive the original E-Invoice and the audit trail. See sections 4.8.4 and 4.8.5.2.	
B	5 - Receipt and technical verification **Conversion of E-Invoice-data**	x	x	x	x	5700	The invoice data is converted incompletely or incorrectly.	Conversion of invoice data must not modify the original E-Invoice content. Authenticity and integrity measures should remain verifiable.	Detailed process steps and mapping have to be defined and traced in an audit trail. See sections 4.8.5.2 and 4.4.3.	
B	5 - Receipt and technical verification **Conversion of E-Invoice-data**	x	x	x	x	5750	New data is added to the invoice data	Only data already available in or from the E-Invoice must be converted to the system of the buyer.	Archive the original E-Invoice. Make sure conversion is correct and complete. Audit trail. It is possible to add internal business data to the E-Invoice; this will not compromise the existing mandatory data. See section 4.8.5.2.	Substantive test of a number of E-Invoices

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
B	5 - Receipt and technical verification	x			x	5800	E-Invoices cannot be accessed e.g. supplier/presenter environment is not available for checking presented invoices	E-Invoices must be accessible	Agreements and general conditions of supply. Post-contract conditions, see also process step Off-boarding E in section 4.2 in Commentary report, figures 1 & 2.	
B	5 - Receipt and technical verification				x	5850	E-Invoice is not (promptly) accessed after receiving a notification in case of Web access	All notifications must lead to accessing the E-Invoice	Procedures and guidelines.	Online solution to offer audit trail of access
B	5 - Receipt and technical verification	x			x	5900	It is not possible to verify who made the E-Invoice available.	On-line E-Invoices may only be consulted on websites whose identity and authenticity can be verified.	Check in application/web browser. See sections 4.8.5.5 and 4.7.1.	Authentication by SSL/TLS with a sufficiently strong server certificate. Use of Extended Validation certificate as defined by CAB Forum is recommended.
B	D - Integrity and authenticity management **Certificate management (Self signed)**			x		D600	The self-signed certificate required to verify an advanced electronic signature is not trustworthy.	Signature verification must use only self-signed certificates authenticated as coming from known and trusted trading partners. (The use of self-signed certificates is not accepted in all EU Member States.)	The self-signed certificate should be tied to a proof of identity that has been obtained in the onboarding process at a level comparable to recognised good practices for CAs .CAs. Certificates shall be previously exchanged between parties in a way that authenticates the identity of the source.	Good practices for CA's may include ETSI TS 102 042, TS 101 456 or AICPA/CICA Webtrust
B	D - Integrity and authenticity management **Certificate management (CA Issued)**			x		D700	The CA Certification Authority certificate required to verify signature is not trusted.	Signature verification must use certificates issued by a CA which does properly manage its operations.	Only certificates from a certification authority operating to recognised good practices shall be configured into the signature verification system. See section 4.8.5.3.	Good practices for CA's may include ETSI TS 102 042, TS 101 456 or AICPA/CICA Webtrust.
B	D - Integrity and authenticity management **Certificate management (Self signed)**			x		D800	The revocation status of the signing certificate is unknown.	Signature verification must check the status of certificates. (The use of self-signed certificates is not accepted in all EU Member States.)	There should be a contractual commitment from the signer to notify the buyer in case of key compromise or other reasons to consider the certificate to be invalid.	

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
B	D - Integrity and authenticity management **Certificate management (CA Issued)**			x		D900	The revocation status of the signing certificate is unknown.	Signature verification must check the status of certificates.	The signature verification software should check the status of the signing certificate. See section 4.8.5.3.	Check validity period and Certificate Revocation Lists (as defined in ISO/IEC 9594-8 and IETF RFC 5280) or an OCSP server (IETF RFC 2560)
B	D - Integrity and authenticity management **Certificate management (Self signed)**			x		D950	Certificate used to protect an E-Invoice data exchanges is not from the self-signed issuer	Data exchanges must be protected using certificates from trusted certificate issuer. (The use of self-signed certificates is not accepted in all EU Member States.)	Data shall be protected by certificates issued by a trusted supplier operating to practices comparable to recognised good practices for CAs. Certificates shall be previously exchanged between parties in a way that authenticates the identity of the source.	CA good practices include e.g. ETSI TS 102 042, TS 101 456 or AICPA/CICA Webtrust, Extended Validity certificates as defined by the CA/Browser Forum.
B	B - Master Data	x	x			B500	The E-Invoices are not correctly and fully reproducible due to historically incorrect retention of master data including parameters, code-tables and calculation rules.	It must be possible to reproduce the correct E-Invoice including referenced data	Retain history of master data versions	
B	6 - Formal verification	x	x	x	x	6100	Electronic E-Invoice does not contain all mandatory data or addressed to the wrong legal person.	E-Invoice must comply with the country specific mandatory data.	The application must ensure that the E-Invoice contains all mandatory data according to the VAT Law before the E-Invoice can be processed.	
B	6 - Formal Verification	x		x		6200	E-Invoice may be modified or another party may be masquerading as the issuer.	The authentication of origin and integrity of the E-Invoice must be verified by verifying the advanced electronic signature.	The validity of the AdES signature shall be checked and the results should be recorded including verification time and information (e.g. CRLs or OCSP and certificates) used to verify the signature. See section 4.8.5.3.	If possible, the verifier should wait for a grace period before confirming signatures are valid, to ensure that revocations have been reported. However, where this is not practical due to the automated business process, there should be an agreement between the E-Invoice issuer and the recipient that potential compromises to the signing key are reported immediately the recipient.

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
B	6 - Formal Verification			x		6300	E-Invoice has a signature that does not protect all mandatory data.	Integrity of all mandatory data shall be protected by advanced electronic signature. The buyer shall verify this.	Procedure or application check.	
B	6 - Formal verification		x			6400	E-Invoice may be modified or another party may be masquerading as the supplier	The authentication of origin of the E-Invoice must be verified by verifying the channel through which the E-Invoice is received.	The authenticated identity of the E-Invoice issuer, and any integrity check codes, shall be checked and the results should be recorded including the time of authentication.	
B	6 - Formal Verification		x			6500	Buyer accepts E-Invoice from a supplier without interchange agreement	The E-Invoice must come from a supplier with whom there is an interchange agreement	Application check; is the supplier known as an EDI biller. Procedure for entering and modifying fixed data. See also Process step On-boarding A	
B	6 - Formal verification				x	6600	E-Invoice may be modified or another party may be masquerading as the issuer.	The authentication of origin of the E-Invoice must be verified by verifying the channel through which the web server is accessed	Web system operates under recognised good practices for security of web servers and controls access to E-Invoices. The E-Invoice shall be sent through a secure channel which: a) Protects the integrity of the E-Invoice up to the buyer or the buyer's service provider. b) Authenticates the E-Invoice issuer to the buyer or the buyer's service provider. This can be either: o Authentication information confirmed by a trusted third party (e.g. certificate issued by recognised CA or identity authenticated by a VAN). The third party should be accredited or certified against a recognised standard. o Authentication information securely linked to an interchange agreement. (E.g. self-certified keys physically exchanged alongside the interchange agreement.) See section 4.8.5.5.	i) Transport Layer Security (RFC 4346) with passwords. ii) Business Data Interchange over the Internet Applicability Statement 1, 2, 3 with signatures (RFC3335, RFC 4130, RFC 4823) iii) Secure network service provided by Value Add Network service provider. iv) Secure messaging services such as ITU-T X.400 or S/MIME (RFC 3851). v) Integrity measures, such as hash totals or reconciliation overviews vi) Registered email such as defined in TS 102 640
B	6 - Formal verification	x	x	x	x	6700	Delayed E-Invoice payments	The recipient of an electronic E-Invoice should be allowed to accept or reject the document at either the document level or the line item level, as agreed upon by the trading partners.	They buyer and supplier may agree whether to accept partial payment of E-Invoices, or to allow/disallow the short payment of E-Invoices. The various cash flow, working capital requirements and collection processes of different size suppliers should not be dictated by the buyer's system There may be differences with how local legislation deals with this requirement.	

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
B	7 - Last mile	x	x	x	x	7500	The invoice data transferred to the buyer by the service provider can be altered or added during the transmission.	Ensure authenticity and integrity of invoice data whilst being sent.	The invoice data shall be transferred in a way that : a) Protects the integrity of the data communicated, b) Authenticates the source of the data. See section 4.8.5.5.	i) Transport Layer Security (RFC 4346) with passwords. ii) Business Data Interchange over the Internet Applicability Statement 1, 2, 3 with signatures (RFC3335, RFC 4130, RFC 4823) iii) Secure network service provided by Value Add Network service provider. iv) Secure messaging services such as ITU-T X.400 or S/MIME (RFC 3851) . v) Integrity measures, such as hash totals or reconciliation overviews vi) Registered email such as defined in TS 102 640
B	8 - Material verification and processing	x	x	x	x	8300	E-Invoices occur twice	Each E-Invoice shall only be booked once	(Application) Controls to detect duplicated E-Invoices and prevent them from being processed	
B	8 - Material verification and processing	x	x	x	x	8400	E-Invoices are not checked timely for content and processed	The consistency of each transaction and the content must be checked within an appropriate time on receipt for processing.	(Application) Controls and reconciliation with e.g. orders, goods receipt.	
B	8 - Material verification and processing	x	x	x	x	8500	Incorrect or fraudulent E-Invoice is processed	Only process E-Invoices that correspond to business expectation	The E-Invoice content can be validated against buyer's in-house accounts payable master data - in case of substantial differences do not further process and run an approval workflow. Application checks and procedures for modifying master data of the supplier.	
B	8 - Material verification and processing	x	x	x	x	8600	The person accountable for processing the E-Invoice cannot be identified	The accountable person needs to be identifiable	All internal control records relating to the receipt, audit and processing of the E-Invoices must be retained.	
All	**(Supplier and Buyer Side)**									

Who	Process step[25]	Business implementation classes A-D				KEY	WHY (RISK)	WHAT (REQUIREMENTS)	HOW (CONTROLS)	Reference Examples.[26]
		A	B	C	D					
All	E - Trading partner off-boarding	x	x	x	x	E300	Transactions and stored E-Invoices are lost, duplicated, or processed without sufficient controls. Required system or process auditability becomes legally unavailable; audit trails and descriptive documents can no longer be accessed by competent authorities.	The trading partners must ensure that termination does not impact tax control and auditability. Authenticity and integrity must remain verifiable during the storage period	Trading partners should agree on minimum procedures for an appropriate transition should there be a need to move E-Invoices from one environment to another during their life cycle. Equally, trading partners should ensure that critical audit trail and documentary evidence of past storage processes is retained, irrespective of E-Invoices/invoice processes having been moved, for the remainder of the mandatory storage period of E-Invoices under applicable law.	These issues should be regulated in an explicit agreement between the trading partners, and between each trading partner and their service provider(s), concluded prior to starting the e-invoicing process.
All	E - Trading partner off-boarding	X			x	E700	The buyer cannot access the 'original' presented E-Invoice.	If the physical connection is not available due to contract termination, the E-Invoices must still be available for the entire retention period. This must include authenticity and integrity characteristics.	Should be agreed in a contract, see also process step Archiving an auditability C in section 4.2 in Commentary report, figures 1 & 2.	

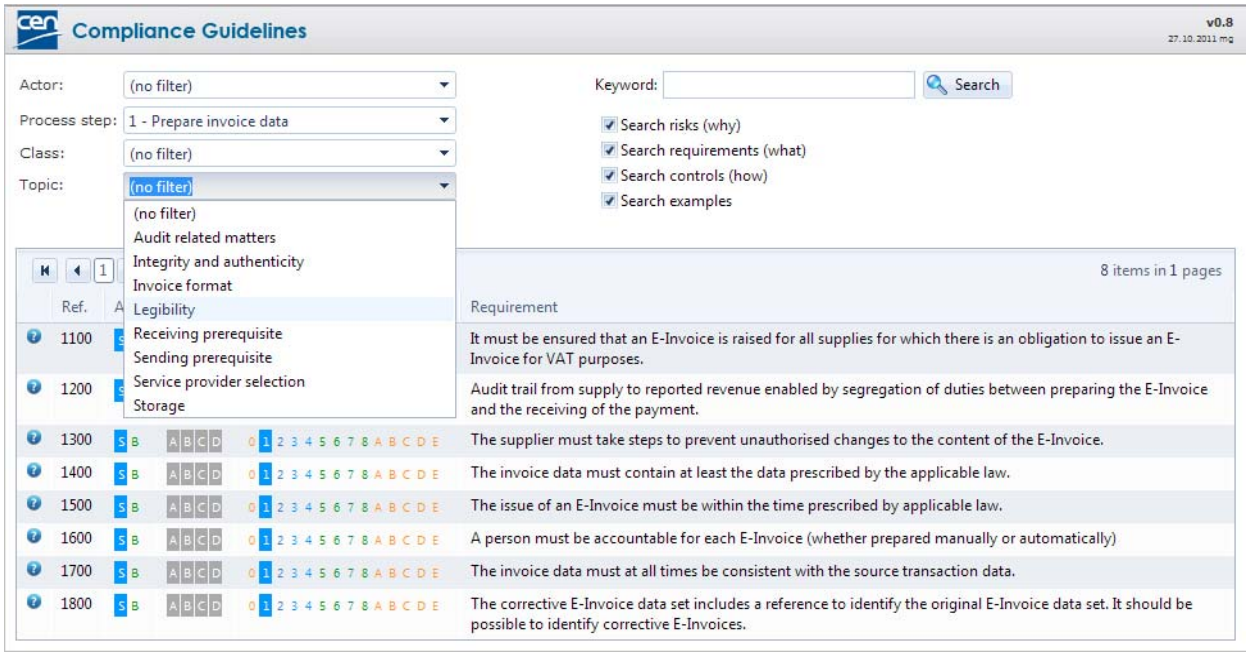
Annex 2: Interactive User Interface

The information contained in the Compliance Matrix can be accessed via an interactive web page, where a combination of filters can be applied to narrow down which requirements may be applicable to certain scenarios. These filters are:

- Actor, i.e. whether the requirement applies to Buyer, Seller or both.
- Process step, i.e. which part of the e-invoicing process the requirement applies to.
- Class, i.e. whether the requirement could belong to Class A, B, C or D.
- Category, i.e. what particular type of requirement it is.

In addition, a keyword search can be applied to search in texts in each of the columns Risks, Requirements, Controls, Examples, Guidance or Implementation.

The actors, classes and process steps are shown graphically along with the defined requirement. The summary, including information from other columns can be viewed for each requirement.



The Interactive User Interface is accessible from:

http://130.208.242.38/ComplianceWeb/MatrixApplyFilters.aspx

The above are also both accessible from the E-Invoice Gateway:

http://www.e-invoice-gateway.net/

Annex 3: Topic assignments

In order to allow filtering of Compliance Requirements in the Matrix based on context, post-processing was used to define a new filter in the Interactive User Interface. This filter is created by defining topics and specifying keywords to look for in three columns of the Matrix, These columns are Risk (Why), Requirements (What) and Controls (How).

The following table defines these topics and below the assignments results are summarized..

6 Topic	7 Description	8 Keywords
Service provider involvement	Specific issues that may arise when using a service provider.	Service provider
Audit related matters	Cases where audit trail or auditability are concerned.	Audit, audit trail, auditability, trace, track
Sending prerequisite	Cases where the sender has a specific requirement to be met before sending of an invoice.	Contract, agreement
Receiving prerequisite	Cases where the recipient has a specific requirement to be met when receiving an invoice (which may or may not affect the sender).	Contract, agreement
Integrity and authenticity	Cases where integrity, authenticity and presentation could be compromised if not fulfilled.	Integrity, authenticity, semantics, malware, content, origin, signature, certificate
Legibility	Cases where legibility is concerned.	Legibility, human readable, machine readable, transformation, conversion
Invoice format	Cases where invoice format is a concern.	Legibility, format, form, data, semantics, transformation, conversion
Storage	Cases where storage is a concern.	archive, archiving, storage, long term

Key Name	Requirements	Service provider involvement	Audit related matters	Sending prerequisite	Receiving prerequisite	Integrity and authenticity	Legibility	Invoice format	Storage
0100	Support general commercial good security practices								
0200	The responsibilities of each party must be clearly delineated.								
0300	Documentation of processes and procedures should be in place.								
A100	The trading partners must ensure proper trading partner identification and clearance.								
A200	The decision to send and accept E-Invoices is auditable.								
A300	The trading partner should ensure that other trading partners sign a comprehensive and enforceable agreement before providing access to t								
A400	The trading partners/service providers should ensure that the trading partner in question is trained to perform the required system activitie								
A500	Security mechanisms employed across parties involved with exchange of E-Invoice shall address identified risks in a coherent manner.								
A600	The proper technical functioning of the trading partner's access to the e-Invoicing system should be ensured prior to production.								
A700	An interchange agreement is required if EDI E-Invoices are sent and received, otherwise the E-Invoice is not valid (VAT law).								
A800	The proper technical functioning of the trading partner's EDI-structures should be ensured prior to production.								
1100	It must be ensured that an E-Invoice is raised for all supplies for which there is an obligation to issue an E-Invoice for VAT purposes.								
1200	Audit trail from supply to reported revenue enabled by segregation of duties between preparing the E-Invoice and the receiving of the payr								
1300	The supplier must take steps to prevent unauthorised changes to the content of the E-Invoice.								
1400	The invoice data must contain at least the data prescribed by the applicable law.								
1500	The issue of an E-Invoice must be within the time prescribed by applicable law.								
1600	A person must be accountable for each E-Invoice (whether prepared manually or automatically)								
1700	The invoice data must at all times be consistent with the source transaction data.								
1800	The corrective E-Invoice data set includes a reference to identify the original E-Invoice data set. It should be possible to identify corrective E								
2100	Ensure authencity and integrity of invoice data whilst being sent.								

Key Name	Requirements	Service provider involvement	Audit related matters	Sending prerequisite	Receiving prerequisite	Integrity and authenticity	Legibility	Invoice format	Storage
D100	The invoice signer must ensure sole control of the private key and comply with its obligations regarding security and reporting of potential c								
D200	The CA must operate under good practice for PKI (Public Key Infrastructure) systems								
D300	CA issuing any certificates used to protect data exchange must operate under good practice for PKI systems								
D400	Before using the self-signed certificate, it must be authenticated to all trading partners as coming from a trusted source.The use of self-signe								
3050	Ensure E-Invoice does not contain executable code.								
3100	It must be ensured that an E-Invoice can only be created once without â€œcopyâ€written on it. It must be clear between the parties what co								
3150	Method to verify the issued E-Invoices								
3200	Service provider shall not add invoice data (outside of an agreed enrichment service)								
3250	The E-Invoice as created by the service provider must contain all agreed upon data.								
3300	The service provider must create all of the E-Invoices provided by the supplier.								
3350	The supplier is still responsible for the accuracy and completeness of the content of the E-Invoices. The supplier must (be able to) access all								
3400	The E-Invoice is provided with an advanced electronic signature to protect its integrity and authenticity.								
3450	The E-Invoice must be provided with an advanced electronic signature with a valid certificate.								
3500	All mandatory data according to applicable law must be signed.								
3550	Structure of the E-Invoice must comply with the structure of the E-Invoice as agreed in the current interchange agreement.								
3600	To the extent that a summary document is used for evidencing completeness, the integrity and authenticity of the summary document (pap								
3650	It must be ensured that an E-Invoice can only be created by the designated issuer in the contract. It must be clear between the parties who i								
4050	The supplier must ensure that E-Invoices are sent or made available, timely according to applicable law								
4100	E-Invoices have to be sent/made available (general).								
4120	E-Invoices have to be sent (e-mail).								
4150	When a certificate is used to protect the transport of an unsigned E-Invoice, the certificate must be valid.								
4200	Authenticity and integrity of the E-Invoice must be guaranteed within the EDI-process								
4250	There must be an understanding between trading partners when an E-Invoice is sent or is made available.								
4300	In order to correctly perform the receipt process, the buyer must review the E-Invoices.								
4350	E-Invoices may only be presented once and must be uniquely identifiable.								
4400	All E-Invoices must be presented. Special attention for corrective E-Invoices.								
4450	The server on which the E-Invoices are accessible must authenticate itself verifiably towards the buyer								
4500	The E-Invoice cannot be changed in authorised manner whilst on web server.								
4550	It must be ensured that a E-Invoice can only be issued by the designated issuer in the contract. It must be clear between the parties who iss								
4600	Conversion is required for automatic data processing in back-end systems, but the original E-Invoice needs to be kept from which the conve								
4650	Conversion is required for automatic data processing in back-end systems, but the original E-Invoice must be made available and considered								
D500	Ensure authenticity and integrity of data whilst being sent.								
C100	Advanced electronic signatures must remain verifiable during the storage period.								
C150	Advanced electronic signatures must remain verifiable during the storage period.								
C200	The issued and received E-Invoices must be archived for the statutory archiving period under the applicable law(s)								
C250	At the request of the tax inspector, the E-Invoice must be made available promptly over the full mandatory period.								
C300	The authenticity and integrity of the content of the E-Invoices stored must be guaranteed throughout the storage period.								
C350	The E-Invoice archiving service provider must set up a proper Information Security Management System addressing media management								
C400	The E-Invoice archive system must ensure the stored documents are readable								
C470	The E-Invoices archiving system shall have in place an Information Security Management Systems envisaging a reliable Business Continuity F								
C530	Storage time needs to be extended to match the applicable retention period or any extension thereof (e.g. ongoing litigation)								
C600	Archives for each taxable person should be separated, at least logically, in order to meet the necessary confidentiality needs, Applicable cou								
C630	E-Invoices cannot be stored physically in a specific country/region not accepted by the applicable legislations/rules (tax and account/comme								
C670	Minimum search/retrieval parameters must be supported, at least as per the applicable legislation, addressing, where necessary, also the st								
C700	The information owner must be able to access its own E-Invoice regardless of the number of storage service providers.								
C730	Any authorised person shall be able to read the E-Invoice any time it is necessary.								
C770	It must be demonstrable that the invoice content in human legible form matches the machine readable form data.								
C800	All information necessary to allow invoices to be correctly interpreted must remain available for audit purposes								
C900	Adequate audit trail must be available throughout the storage period								
5050	The technical availability for receiving E-Invoices must be ensured. The accurate, complete and prompt receipt of E-Invoices must be adequa								
5100	Multiple receipts of E-Invoices must be detected. Multiple E-Invoices must be removed and eliminated from further processing.								
5150	E-Invoice must be technically correct before being further processed. The rejected E-Invoices must be separately identifiable.								
5200	The buyer or the service provider on his behalf must receive all E-Invoices sent.								
5300	Ensure E-Invoice does not contain executable code								
5350	Measures of authenticity and integrity in transport should be in place until the moment of formal receipt. From the moment of formal recei								
5400	The authenticity and integrity of the E-Invoice must be ensured by means of an advanced electronic signature. The authentication mechanis								
5450	Record time that the advanced electronic signature is verified.(Different EU-member states have different rules.)								
5500	The process/software applied to verify the advanced electronic signature should be identifiable and reliable.								
5550	E-Invoice must comply with the (technical) requirements of the current interchange agreement								
5600	It must be possible to detect whether issued E-Invoices are modified during transfer								
5650	There can only be one E-Invoice and an audit trail must be maintained between it and any sets of invoice data derived from it.								
5700	Conversion of invoice data must not modify the original E-Invoice content. Authenticity and integrity measures should remain verifiable.								
5750	Only data already available in or from the E-Invoice must be converted to the system of the buyer.								
5800	E-Invoices must be accessible								
5850	All notifications must lead to accessing the E-Invoice								
5900	On-line E-Invoices may only be consulted on websites whose identity and authenticity can be verified.								
D600	Signature verification must use only self-signed certificates authenticated as coming from known and trusted trading partners.(The use of se								
D700	Signature verification must use certificates issued by a CA which does properly manage its operations.								
D800	Signature verification must check the status of certificates.(The use of self signed certificates is not accepted in all EU Member States.)								
D900	Signature verification must check the status of certificates.								
D950	Data exchanges must be protected using certificates from trusted certificate issuer.(The use of self signed certificates is not accepted in all E								

Key Name	Requirements	Service provider involvement	Audit related matters	Sending prerequisite	Receiving prerequisite	Integrity and authenticity	Legibility	Invoice format	Storage
B500	It must be possible to reproduce the correct E-Invoice including referenced data								
6100	E-Invoice must comply with the country specific mandatory data.								
6200	The authentication of origin and integrity of the E-Invoice must be verified by verifying the advanced electronic signature.								
6300	Integrity of all mandatory data shall be protected by advanced electronic signature. The buyer shall verify this.								
6400	The authentication of origin of the E-Invoice must be verified by verifying the channel trough which the E-Invoice is received.								
6500	The E-Invoice must come from a supplier with whom there is an interchange agreement								
6600	The authentication of origin of the E-Invoice must be verified by verifying the channel trough which the web server is accessed								
6700	The recipient of an electronic E-Invoice should be allowed to accept or reject the document at either the document level or the line item lev								
7500	Ensure authenticity and integrity of invoice data whilst being sent.								
8300	Each E-Invoice shall only be booked once								
8400	The consistency of each transaction and the content must be checked within an appropriate time on receipt for processing.								
8500	Only process E-Invoices that correspond to business expectation								
8600	The accountable person needs to be identifiable								
E300	The trading partners must ensure that termination does not impact tax control and auditability. Authenticity and integrity must remain verif								
E700	If the physical connection is not available due to contract termination, the E-Invoices must still be available for the entire retention period.								