How CEN E-Invoicing Compliance Guidelines Impact Your Company

By Phillip Schmandt and Christiaan van der Valk

February 2010

How CEN E-Invoicing Compliance Guidelines Impact Your Company

By Phillip Schmandt and Christiaan van der Valk

Content

Introduction.....1

Existing legal framework for electronic invoicing in Europe.....1

Compliance challenges.....2

The role of European standards bodies.....3

Nature of the Guidelines.....3

Principal components and structure of the Guidelines.....4

Underlying process model.....4

Basic end-to-end process requirements.....6

Options for e-invoice integrity and authenticity guarantees.....6

Integrity and authenticity-enhancing technologies.....8

Concept of original invoice and conversion of invoices.....11

Why perform a self-assessment?.....12

The Guidelines and EU policy development.....12

Introduction

Value-Added Tax (VAT) generates approximately one-third of all public revenue in many of the world's wealthiest countries; in some EU Member States, the VAT contribution to the fiscal mix is close to 40 percent.

Electronic invoicing remains one of the most challenging areas of conducting e-business in and with the European Union. Tax administrations want long-term access to the invoice as the ultimate guarantee of proper VAT treatment of a sales transaction. Businesses, meanwhile, want a seamless and efficient electronic invoicing system that brings value through automation and the robustness of electronic data.

This article introduces the new CEN E-Invoicing Compliance Guidelines and explains how businesses can use these guidelines to implement e-invoicing processes with more legal certainty.

Under the current legal regime in the EU, parties have very limited choice in relation to the control methods they use to ensure integrity and authenticity -- the focus has been almost exclusively on

advanced electronic signatures and a narrowly defined EDI process, thereby excluding many other options available to businesses to ensure auditability. This article and the CEN E-Invoicing Compliance Guidelines seek to redress this by comprehensively addressing all process and technology control options currently available to businesses (even though not all controls or processes may be currently available in all Member States).

Existing Legal Framework for Electronic Invoicing in Europe

The European Commission, which is the Union's executive body headed by non-elected Commissioners, views e-invoicing as an important driver of economic competitiveness and environmental protection. A Commission proposal for a Directive setting out changes to the invoicing rules of the Value Added Tax (VAT) Directive was formally adopted in 2001 and entered into force on Jan. 1, 2004.

On the Directive level, the rules for e-invoicing are different from paper-based invoicing in one major way: Article 233 of the VAT Directive specifies that Member States must accept electronic invoicing provided taxable persons guarantee the authenticity of the origin and the integrity of their content are guaranteed by one of the following methods:

1. by means of an advanced electronic signature within the meaning of Section (2) of Article 2 of Directive 1999/93/EC of the European Parliament and of the Council of Dec. 13, 1999, on a Community framework for electronic signatures;

2. by means of electronic data interchange (EDI), as defined in Article 2 of Commission Recommendation 1994/820/EC of Oct. 19, 1994, relating to the legal aspects of electronic data interchange, provided that the agreement relating to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data;

3. as a third, slightly different option, electronic invoices may also be sent or made available by other electronic means (read: with or without guarantees of integrity and authenticity), subject to acceptance by the Member States concerned.

Within the three methods above, a number of different implementations exist among Members States. For all other invoices, the VAT Directive in Article 246 lays down functional requirements for safeguarding integrity and authenticity, but no specific methods or technologies for achieving these results are mentioned.

EU Directives are not federal law: They have to be transposed into the national laws of Member States. The result of this transposition process for the 2001 Invoicing Directive was that Member States chose different combinations of Article 233 options. Many Member States transposed options (1) and (2) without option (3), while a few others transposed only option (3). This led to discrepancies among Member States on the level of primary legislation.

Compliance Challenges

The differences in primary Member State legislation that resulted from the transposition of choices in Art 233 of the Invoicing Directive were compounded by variations in tax administrations' audit practices and among those hard-to-define yet tightly knit fabrics of countries' general legal and tax cultures, business practices and standards frameworks. Because there are no hard-and-fast rules concerning the applicability of origin and/or destination legal requirements when an invoice crosses an internal EU border, this non-uniform transposition creates legal uncertainty for businesses transacting between Member States.

EU tax administrations typically have audit departments that specialize in the verification of systems and processes utilizing information technologies. When an invoicing process is fully electronic, the underlying systems and processes logically fall within the jurisdiction of such expert auditors. From a business implementation perspective, therefore, there is a lot more to compliant e-invoicing than the few lines about integrity and authenticity-specific measures one can find in a Member State's law. In theory, a company's e-invoicing process -- after many years of successful operation -- may be declared non-compliant by tax auditors based on shortcomings that are hard to relate to explicit statutory requirements.

The combination of these two factors -- inconsistent primary law and implicit requirements applied in tax audits -- has had a negative impact on investment decisions by businesses. Few tax administrations have channels for companies to obtain certainty prior to implementing an e-invoicing process. Audits or design reviews by tax consulting firms provide no formal certainty either.

The Role of European Standards Bodies

The European business community and tax administrations, gathered under a combined CEN (European Standardization Committee)/CENELEC (the European Committee for Electrotechnical Standardization) umbrella, have worked on a common body of good practice around e-invoicing since 2005. Since 2007, two task forces (respectively tasked with "Compliance of electronic invoice implementations" and with "Cost-effective authenticity and integrity of electronic invoices regardless of formats and technologies") have worked on the Guidelines, which were adopted as a CEN Workshop Agreement. A CWA is not a formal standard but an agreement among participants in a CEN workshop. The participants in the task forces comprised representatives of e-invoice service providers and tax administrators. The task forces also received input from businesses and commercial enterprises using e-invoicing.

The authors of the Compliance Guidelines looked for guidance from the FISCALIS 2013 framework. FISCALIS is a tax administration cooperation program funded by the European Commission. As part of the FISCALIS activities, the Dutch tax administration (Belastingdienst) had spearheaded initial work among tax administration toward a set of tax audit guidelines based on a process analysis framework in use in the Netherlands.

The close resemblance of the work products from CEN and FISCALIS was not a coincidence. The uncertainty surrounding e-invoicing is not restricted to companies who must assure compliance: Tax administrations also are unsure about how to assess e-invoicing processes and judge their adequacy. These uncertainties arise because businesses and tax administrations lack a common platform to analyze business processes and their inherent risks from a VAT perspective. The CEN E-Invoicing Compliance Guidelines were developed to fill this void.

Nature of the Guidelines

Before explaining the potential utility of the Guidelines for companies trading in or with the EU, we will briefly list what the Guidelines are not:

- The Guidelines are a CEN Workshop Agreement and not a formal CEN standard.

- The Guidelines are not a substitute for meeting specific obligations under applicable national law, but a strong basis for practices complying with the current legal requirements across Europe. If, for example, French VAT legislation says a company must generate summary statements of invoices produced in EDI systems but the Guidelines do not mention such a control option, a company issuing invoices electronically in France using the EDI option must still produce such summary statements to avoid potential sanctions.

- The Guidelines do not address the substantive and core administrative aspects of VAT (determining applicable VAT law, VAT rates, reporting, payment, reclaims, etc.) but rather the process and technologies required to ensure that a business can prove -- and a tax administration verify -- that the invoices that form the critical component of most countries' tax audit frameworks are reliable.

The purpose of the Guidelines is to provide business practitioners with an instrument for (self-) certification and to set a framework for effective tax audits by tax authorities. In summary, therefore, the Guidelines aim to enable cost-effective e-invoicing implementation and auditability to the benefit of businesses and tax administrations alike. Therefore, despite their inherent shortcomings, the Guidelines can be very useful because they are (1) technologically neutral, (2) applicable across market verticals and (3) a jurisdiction-independent common sense foundation for an e-invoicing process.

A company using the Guidelines can obtain the following benefits:

- Minimize the number and extent of country-specific measures to be implemented to meet specific form and other requirements per applicable VAT law.
- Maintain a layer of generic good practice controls that make affected processes less vulnerable to regulatory change[1].

It should also be noted that the Guidelines are already fully applicable and useable for domestic transactions within countries -- e.g. the UK, the Netherlands, Sweden -- which have chosen not to transpose specific form or method requirements in their national legal frameworks for electronic invoicing.

[1]The Guidelines have been endorsed as a good practice definition by the Expert Group on Electronic Invoicing set up in 2008 by the European Commission, and several tax administrations in jurisdictions with stringent form or method requirements have stated they plan to align their audit frameworks to the Guidelines. The Guidelines also take into account proposals for the amendment of this Directive as specified in "Proposal for a Council Directive amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing" COM(2009) 21

Principal Components and Structure of the Guidelines

The core of the Guidelines is a matrix (the Compliance Matrix) containing 105 process steps and 10 key columns. Accompanying the Compliance Matrix is a narrative Commentary providing more information about the structure, underlying process analysis model and objectives of the Matrix.

Underlying Process Model

The Compliance Matrix is based on a high-level process analysis that essentially subdivides e-invoicing into (a) transaction processes (from Prepare Invoice Data on the supplier's side to Process Invoice on the Buyer's side) and (b) fundamental overarching processes (manage source data; integrity and authenticity; and archiving and auditability). The objective is to track an invoice and its compliance aspects from beginning to end of its formal life cycle.

Trading partners may decide to outsource any part of the process to third parties; conditions for such outsourcing are comprehensively discussed in the Guidelines.

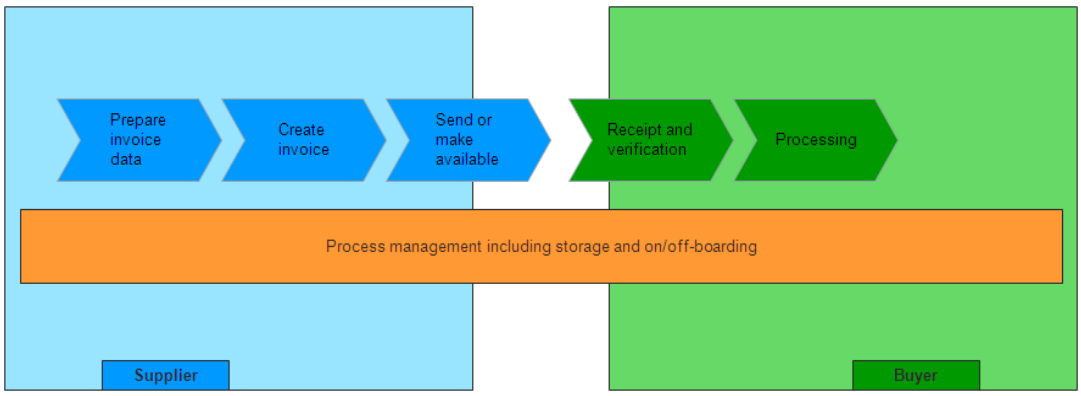

Figure 1: End-to-end process model

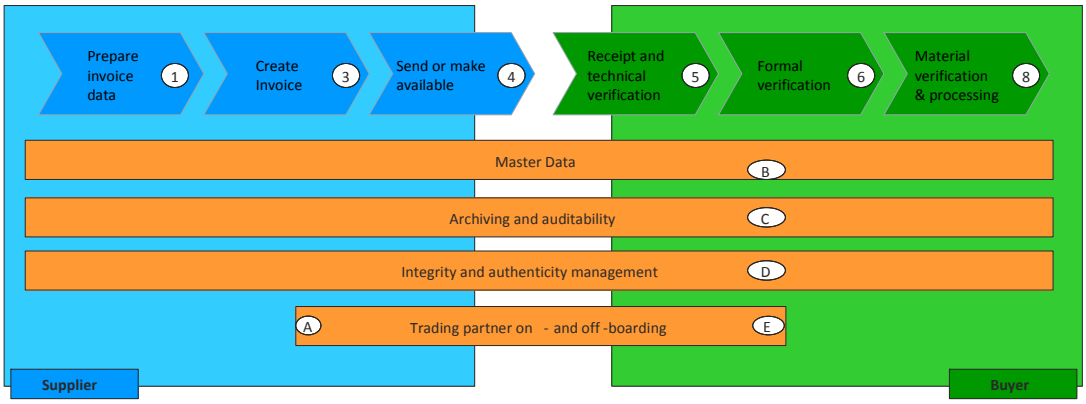

Figure 2: Extended process Model without Service Provider involvement

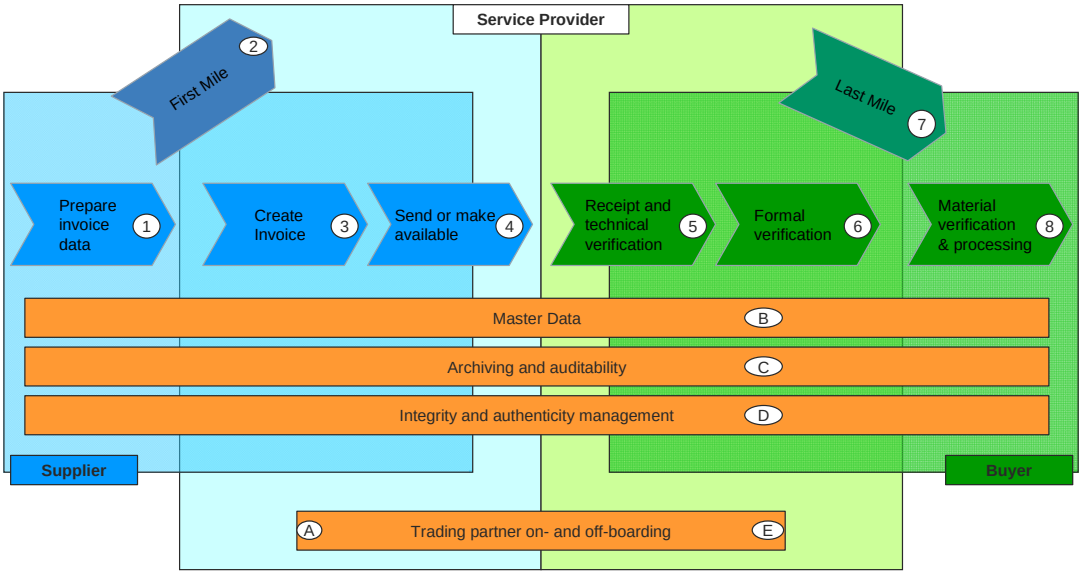

Figure 3: Extended process Model with Service Provider involvement

Basic End-to-End Process Requirements

The Guidelines start from an end-to-end process analysis covering all business controls required for the life cycle of an e-invoice. They formulate the following five top-line requirements for e-invoicing processes:

1. Auditability: The current and historical operation of an organization's Invoicing process, including resulting Invoices, is auditable;

2. Authenticity: The authenticity of the origin of Invoices is maintained;

3. Integrity: The integrity of the content of Invoices is maintained;

4. Continuity: The Tax Invoicing process correctly handles Invoices (including ensuring their uniqueness) and related documentation through their stages; and

5. Legal requirements: Invoice requirements under applicable law, including for storage and access, are in compliance.

Options for E-Invoice Integrity and Authenticity Guarantees

To understand and use the Guidelines, one should begin by differentiating between the process-level versus data-level controls for achieving integrity and authenticity:

- Process-level controls rely on the ability of an auditor to verify the correctness of historical processes on the basis of audit trails, documentation and/or third party audits. Within the current EU VAT Directive's Article 233, the EDI option is a process-level control method.

- Data-level controls provide a single technical means of verifying the integrity and authenticity of individual e-invoices through checks performed on the invoice itself without reliance on historical context or the data carrier medium. Within the current EU VAT Directive's Article

233, the advanced electronic signature option is a data-level control method.

This basic dichotomy is used to further classify a number of logical clusters of control methods that are frequently found in e-invoicing implementations. These implementation "classes" are merely an analysis framework and not a straightjacket. Indeed, many real-life implementations, in reality, mix and match aspects of various classes. Nevertheless, this classification can be useful for a process designer to set a high-level compliance strategy in relation to proving the long-term integrity and authenticity of electronic invoices.

The classes are only meaningful if understood against the backdrop of the basic end-to-end process requirements described in the previous section. Each class assumes a foundation of common sense business processes called "basic business controls" in the Guidelines.

Importantly, the Classes are not a straightjacket but a mental framework to ensure cost-effective auditability for different types of business scenarios. Many real-life implementations will contain elements from more than one Class.

The classes:

- Class A: Business solutions exclusively relying on the transparency of individual trading partners' internal business controls to prove sales transactions to tax administrations. Examples of companies that may consider relying on Class A for auditability:

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

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

    Companies that are capable of using Class A-type controls may not need to implement a "legal archive" where the invoices as sent or received are stored for future evidence purposes: The evidence of correct VAT treatment of sales transactions is in the transparency of the internal control process itself. The invoice as a separate object truly becomes immaterial in all meanings of the word. Evidence of sales transactions in Class A implementations arises from the sum of comprehensive internal controls rather than from a tightly controlled end-to-end invoice exchange process.

    Hence, in Class A implementations, the processes between trading partners are relatively unimportant. Lack of audit trails and other controls around conversion of the invoice during the transmission and lack of security in the transmission channel will, for example, not in themselves substantially affect auditability: If the lack of such controls leads to incorrect invoices being delivered, the internal control process that was verifiably in place at the time of a transaction would have rejected such incorrect invoices. For the same reason, Class A is not included in the end-to-end process analysis of the Compliance Matrix.

- Class B: Business solutions relying on basic business controls augmented by controlled data exchanges (e.g. EDI) to ensure that real and unchanged Invoices exist between trading partners and can be made available to tax auditors. Class B implementations place the emphasis on controls in the transmission and its beginning and end points. Typically, this concerns EDI processes where the supplier creates a data file in a structured format under an automated process directly from the accounting system. An interchange agreement makes the supplier responsible for ensuring that the invoice contains all mandatory and agreed items, as well as for sending the invoice using an agreed secure transmission method to an agreed destination. Under the same agreement, the buyer is responsible for specific entry-point technical and content controls. This type of EDI process typically uses a direct secured transport channel between the trading partners so that the exchange process is tightly controlled and input/output points tightly coupled to upstream and downstream processes (including archiving).

  As with all other implementation classes, any part of these processes can be outsourced to third parties. In principle, invoices are exchanged in a pre-agreed structured format; however, if the transmission process includes conversion steps and the technical file format received by the buyer is not the same as the one sent by the supplier, then parties must agree on ways to prove that the conversion process was well controlled and did not expose the invoice content to any changes. Class B implementations typically include a legal archive that is separate from the supplier's and buyer's ERP database, so that the input and output of the exchange can be independently audited.

- Class C: Business solutions relying on basic business controls augmented by data-level controls (e.g. Advanced Electronic Signatures) to ensure that real and unchanged invoices exist between trading partners and can be made available to tax auditors. Class C implementations place the emphasis on controls around the mandatory invoice data itself. When the invoice is issued, it is sealed, and this verifiable seal remains with the invoice until the end of the storage period for both parties.

  If these controls are performed according to good electronic signature practices, the integrity and authenticity of the invoice remain verifiable without a need for additional process-level evidence such as audit trails, reproducible business logic or third-party audits. Class B implementations typically include a legal archive that is separate from the supplier's and buyer's ERP database, so that the sealed input and output of the exchange can be independently audited.

- Class D: Business solutions relying on basic business controls augmented by central "safe-keeping" of e-invoices to ensure that real and unchanged e-invoices exist between trading partners and can be made available to tax auditors. Class D implementations always involve one party (which can be a third party or one of the trading partners) who assumes responsibility for containing the entire transaction within a tightly controlled environment, including an archive.

  The end-to-end invoicing process thus takes place within one "sealed off" environment. The evidence of transactions emerges from the fact that this single transaction environment is inviolable. Tax auditors can access the environment and view the invoices; however the invoices never leave the control of the safe-keeper until the end of the storage period.

Classes A and D are not explicitly mentioned in the current VAT Directive; however, they are available in all countries that have transposed the "other means" option.

Integrity and Authenticity-Enhancing Technologies

Classes B-D implementations cannot be implemented without conscious choices about technical security mechanisms to be used in the end-to-end process. This chapter discusses some of the available technical standards and protocols for the secure transmission, processing and/or archiving of invoices. Where relevant, we will briefly describe whether these technical methods fit into the process-level or data-level control category.

Pure Class C implementations (where a digital signature is created by the invoice issuer, verified upon receipt by the buyer and stored by each party with signature, certificate and certificate validity evidence) are not discussed in this section.[2]

- SSL / TLS with client passwords

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

  In a Web-based environment, use of simple identity and password mechanisms may be sufficient, although care needs to be taken in operating in such a Web-based environment.

  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.

  This security mechanism is frequently used to ensure security of point-to-point data transmission steps in process-level control environments; they can play a significant role in Classes B or D, but they can also be found as a business security measure in Class A implementations.

- AS1, AS2 and AS3

  A set of security protocols have been defined specifically for securing business data (including invoices) interchange. These are commonly referred to as AS1, AS2 and AS3, where "AS" standards for "applicability statement." AS1 is aimed at business interchanges using email. AS2 is aimed at business interchanges using Web (HTTP) protocols. AS3 is aimed at interchanges using file-transfer protocols.

---

[2] Trading partners choosing to forego the security of advanced electronic signatures will need to consider the effect of Directive 1999/93/EC on a Community Framework for Electronic Signatures and national legislation issued pursuant thereto by the member states. Under Article 5(1) of that Directive, advanced electronic signatures based on a qualified certificate and which are created a secure signature device are required to be afforded the same treatment as a handwritten signature and must be admissible as evidence in legal proceedings. Electronic signatures without such an advanced electronic signature fall under Article 5(2) of that Directive, which provides the weaker level of protection of not being denied legal effectiveness "solely on the grounds" that they are in electronic form or not based on a similar advanced electronic signature. Trading Partners not using advanced electronic signatures may wish to include language in their interchange agreement agreeing that, as between themselves, electronic invoices without an advanced electronic signature transmitted in accordance with the interchange agreement should be given the same legal effect as a handwritten signature and waiving any right to object to introduction of the invoice as evidence in legal proceedings.

These protocols are essentially designed for point-to-point security, but they combine transport layer security with data-level controls (digital signatures) to have additional authenticity protection on the payload. These mechanisms are typically used in Class B implementations; however they could theoretically be used for Class C controls if the signed payload is preserved and stored.

- Secure Email

  General purpose email security protocols exist that may also be applied to invoicing. These include S/MIME and the secure messaging service defined in ITU-T X.400. These mechanisms can be used in process-level control strategies for secure transport. Even though S/MIME includes the possibility to digitally sign email messages, this method is often less appropriate for Class C implementations.

- Registered Email

  Registered email is a variation of secure email that provides additional services to give proof of submission and delivery of the email similar to the physical registered postal service. This has the advantage of providing further evidence that the e-invoice has been successfully transmitted between the trading partners. A recent standard specification has been issued for Registered E-Mail (REM) in ETSI TS 102 640. Even though this standard includes the possibility to digitally sign email messages, this method is often less appropriate for Class C implementations.

- 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-invoicing is maintained and that correct routing between identified partners is assured. This security mechanism is frequently used to ensure security of point-to-point data transmission steps in process-level control environments; it often plays a significant role in Class B, but it can also be found as a business security measure in Class A implementations.

- Integrity measures, such as hash totals or reconciliation overviews

  These measures can include hash totals sent separately with the invoice and subsequently 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. These security mechanisms can be used to complement process-level control environments; they often play a significant role in Class B, but they are can also be found as a business security measure in Class A implementations.

- Service Providers

  Where Service Providers are used, each provider must validate the authenticity of inbound documents, maintain documented and auditable internal processes for routing or transformation of e-invoices, and verify the security of the transmission of e-invoices to the buyer or next service provider in the process. This type of control is indispensible in Class B scenarios where

service providers are involved.

- Use of encrypted/signed data fields within an unsigned document

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

Finally, in relation to the use of EDI (Class B), practitioners should note that the Guideline's definition of EDI is not limited to UN/EDIFACT, ANSI-X12. The definition of EDI in the Guidelines expressly provides that EDI "is a generic term that covers conventional EDI file formats (UN/EDIFACT, ANSI-X12) as well as later developments using XML (Extended Markup Language) using UN/CEFACT or other formats." The definition of EDI is not bound to a particular technology, but to a process whereby the parties have agreed via an Interchange Agreement on the data formats as well as various technical, security and business procedures, including those aimed at ensuring and proving the authenticity of the origin and integrity of the data.

The Guidelines, therefore, provide an opportunity for trading partners using XML formats with an interchange agreement, to the extent permitted under applicable national laws, to claim that their exchange of electronic invoices is governed by Article 233, Section 1(b) of the Vat Directive's specification on EDI rather than via "other available means" (which not all member states allow).

Concept of Original Invoice and Conversion of Invoices

To avoid use of the controversial and confusing term "original invoice," the Guidelines have adopted the term "tax invoice." The tax invoice is the dataset companies intend to present to a tax auditor when asked for the invoice. This is a critical concept, as it opens the door for companies to demonstrate compliance by maintaining controls and processes designed to avoid altering the data set, while allowing the rest of the invoice to be modified by, for example, converting its format.

Conversion is essential for automatic data processing, since backend systems require different formats to extract invoice data from invoice messages. This business need conflicts with the fact that many tax administrations interpret "original invoice" as "identical semantically and in syntax." This means that it remains important in many EU Member States to only convert invoice data (invoice information not yet or no longer constituting a tax invoice) and not the invoice itself. Content conversion (e.g. using different code lists or units of measure), where permitted, requires trading partners to pay particular attention to the controls they put in place to avoid errors or misunderstandings.

For example, a field or fields of data containing the information "10 Kilogram Cement Sack" may be transformed to "Cement Sack, 10.00 Kg" but the transformation must not interfere with the recipient's ability to determine the correct number of kilos or that it is cement. Conversions that only change the format of the electronic invoice in accordance with agreed and reproducible maps are considered not to substantively alter the data contained in the electronic invoice.

Especially if multiple Service Providers are involved, it is currently common practice in many

countries and industries to pass along multiple objects: The electronic invoice, which is never converted, and electronic invoice data that can be converted as required by, e.g., the buyer's ERP system. This leads to the unfortunate result that the trading partner may be required to store the e-invoice in one format for tax compliance purposes and invoice data in another format for commercial purposes.

In addition, the trading partner may act on the invoice data that its computer's back-end system can automatically consume, while the data in the tax-compliant invoice may sit forever ignored and never be read unless there is an audit. The Compliance Guideline's focus on the "data set" as the invoice, coupled with control and technical processes for conversion of the invoice format, is intended to avoid these expensive and non-common sense results of having two sets of invoices, one actually used in commerce and the other only existing for tax compliance purposes.

Why Perform a Self-Assessment?

Your Company should consider a self audit of its electronic invoicing practices and request that your service providers report on their self assessment. If you are a service company, you may want to proactively demonstrate to customers and potential customers that you are compliant.

The Guidelines and EU Policy Development

The European Commission has initiated a process to force more uniformity among Member States through a new proposal for a Directive [reference] amending the VAT Directive. While it is impossible to predict the outcome of the discussions about this Commission Proposal, it is known that a number of EU Member States do not favor the complete removal of requirements for e-invoicing in the VAT Directive.

Whatever ends up happening with the regime for e-invoicing, however, it is already certain that Article 246 of the VAT Directive will not be modified. The base requirements for auditability of invoices therefore remain, and it would be naïve to believe that tax administrations will scale down or stop auditing as a result of any Directive changes: Indeed, tax audits are almost entirely each Member State's prerogative.

Therefore, the Guidelines will fill a crucial void between businesses and tax administrations almost regardless of changes in primary law that may result from Commission efforts. For this reason, the European Commission Expert Group recommends use of the Guidelines in its Final Report.

Phillip Schmandt is head of the technology practice group at McGinnis Lochridge & Kilgore. Christiaan van der Valk, CEO of TrustWeaver, is Co-Chair of the ICC EBITT Commission's Task Force on Security and Authentication.