



International Chamber of Commerce

The world business organization

Policy Statement

Electronic invoicing in and with the European Union

Prepared by the Commission on Commercial Law and Practice

International Chamber of Commerce

38 cours Albert 1er, 75008 Paris, France

Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59

Web site www.iccwbo.org E-mail icc@iccwbo.org

Table of Contents

1. Introduction	1
2. The e-invoicing Directive and general information compliance	1
3. Ongoing standardization and harmonization efforts.....	2
4. Content rules.....	2
5. Receivers' acceptance	3
6. Language and localization	3
7. Market trends	3
8. Security compliance.....	5
8.1. Applicable law for security compliance purposes	5
8.2. Web-EDI classification.....	6
8.3. The EDI compliance option	6
8.4. The e-signature compliance option.....	8
8.4.1. General.....	8
8.4.2. Advanced and Qualified Electronic Signatures	9
8.4.3. Electronic signatures and self-billing	11
8.4.4. E-invoice outsourcing	11
8.5. Storage	11
8.6. Paper-electronic parallel (hybrid invoicing).....	12
8.7. Timestamping.....	13
8.8. Notification issues	13

1. Introduction

Invoicing is an important business process that through automation can help both businesses and tax authorities realize multiple tangible benefits. ICC members strongly support the European governments' endeavours to make electronic invoices acceptable, under harmonized conditions, throughout the European Union. Such explicit acceptance allows business to exploit new technologies with a high level of legal certainty.

This legal certainty is, however, reduced by a lack of implementation-relevant information on available compliance alternatives. This paper summarizes our views and experiences with electronic invoicing from an international business perspective. It also outlines a number of areas of uncertainty whose resolution would, in ICC's view, help European governments vastly improve the conditions for e-invoicing in the EU. ICC would be pleased to work with the European Commission, Member States and other governments to provide international business input into all processes that aim to further define and facilitate conditions for electronic invoicing.

2. The e-invoicing Directive and general information compliance

ICC remains a staunch advocate of technology neutrality in all laws affecting business. Technologically-neutral formulation of legal requirements allows new technologies and business practices to develop and compete freely, which will in the long run allow businesses to meet regulatory objectives with the best and most cost-effective measures. When governments nevertheless want to require specific technologies in order to lower the cost and increase the effectiveness of controls and enforcement, then they should ensure that businesses can freely choose from a maximum of functionally-equivalent technologies. In order to provide a basis for choice optimization by users, as well as to stimulate solution vendors to compete towards high price/quality ratios, technologically-specific requirements in laws should create a level playing field among the relevant technologies. This implies, among other things, that such technologies should be defined with the same level of detail and clarity.

Technology neutrality would also call for paper and electronic communications to be put on an equal footing from a regulatory perspective. ICC would like to recall this principle, which private sector representative groups and most governments explicitly subscribed to in the early Internet days, but which is increasingly disrespected in new legislation. Indeed, electronic invoicing has become a key example of an area where governments have created different – and objectively more stringent – rules than for its paper equivalent.

As a general matter, businesses prefer choice above prescription in order to meet compliance objectives. However, if and when governments choose to enact prescriptive laws, businesses need sufficient information about how such requirements can be met in practice. This implies, in addition to a need for laws to be clear and consistent, that governments should put in place information services that can allow businesses to make informed compliance implementation choices.

However, because information is never perfect, it is also very important for governments to build an appropriate level of flexibility into their enforcement practices. One useful mechanism to achieve such flexibility is to have clearly stated ‘period of grace’ and escalation rules. A period of grace rule could be that if a company is found, prior to or during its relevant operations, to be non-compliant then this company should have a meaningful opportunity to remedy such non-compliance before sanctions are applied. Clear escalation rules aim to reduce uncertainty about the hierarchy of decision makers in the enforcement process. Such rules should be supplemented with clear and easily accessible procedures, which should be made available in as many languages as possible.

ICC believes that many Member States could significantly improve the information they provide to businesses in relation to compliance with the e-Invoicing Directive. In some Member States, officials in charge of e-invoicing matters are very reluctant to engage into any dialogue with the private sector or supply information over and above official laws and decrees. The resulting uncertainty creates significant barriers to the adoption of compliant e-invoicing.

The e-invoicing Directive entered into effect on 1 January 2004. While ICC has many observations about the practical implementation of this Directive, it would also warn against any measures to ‘patch’ the already complex regulatory landscape without having thoroughly weighed the costs and benefits of such measures. ICC believes that this Directive is primarily in need of a more uniform and pragmatic interpretation by national governments. Significant improvements could in particular be achieved by national governments providing a coordinated multi-lingual information service in order to lower the complexity of compliant cross-border e-invoicing.

3. Ongoing standardization and harmonization efforts

Through its members and through direct contacts with organizations active in the e-invoicing space, ICC actively monitors and participates in the efforts that have recently started within the Comité Européen de Normalisation (CEN) and UN-CEFACT.

While ICC strongly supports voluntary standardization, it also wishes to stress that standardization can never be a substitute for good laws and enforcement practices. There exists a lack of standardization at many levels in both e-invoicing and e-business practices generally, however these issues are primarily to be resolved in an industry-driven process as and when required by the market. ICC therefore urges the European Commission, European governments and standards bodies, to ensure that standardization initiatives only address areas that can be effectively standardized, and that the principles of market-driven, voluntary and broad participation and acceptance remain respected.

4. Content rules

ICC is pleased with the Directive’s approach to content harmonization. Having a clear maximum set of content rules throughout the EU benefits invoice interoperability and reduces implementation costs.

5. Receivers' acceptance

While many Member States recognize, de jure or de facto, the mandatory acceptance of invoices in electronic form by customers to be tacit/implicit, ICC believes that the rules concerning the way in which such acceptance should be documented or evidenced would benefit from more uniformity across the EU in order to lower the threshold for cross-border e-invoicing.

6. Language and localization

The general rules on invoice translation and currency conversion are sufficiently clear and helpful; however, language and other localization-related uncertainties arise in connection with a number of common compliance measures. For example, in countries where a written e-invoicing acceptance agreement (which will often be implemented as part of an interchange/trading partner agreement), outsourcing agreement and/or self-billing agreement are mandatory it appears that in practice there exists an assumption that such agreements will be drawn up in every party's local language. Similarly, when electronic signatures are used questions arise as to language and localization obligations in respect of public key certificates, as well in respect of related policies, practices and user agreements/notices that will often be required to establish an acceptable level of security and compliance. Governments should take a pragmatic attitude to such issues, and we recommend that as a general rule such compliance rules and agreements may be drawn up in the local language of one of the parties involved, or alternatively in a neutral language agreed between them; governments should then have the right, if and when necessary and justified, to require translation of such materials on an ad hoc basis. In relation to reliance on public key certificates, it would be natural to require that invoices issued to consumers should be signed with the support of certificates in a language that the consumer in question would in other commercial circumstances (e.g. acquisition of consumer goods or services on the Web, via a web site secured with a web server certificate) be expected to have the capacity to reasonably rely on.

ICC strongly believes that for B2B invoicing purposes the principle of party autonomy should rule as regards such reliance-related language issues.

7. Market trends

ICC is pleased that the Directive has chosen to set forth clear rules enabling parties to outsource invoices processes to third parties, including to their customers under so-called 'self-billing' procedures. Both outsourcing and self-billing are significant market trends that derive from a common need for invoices and other business documents in electronic form to be processed and stored in a more or less centralized fashion for cohesive groups of transacting parties. Such centralization allows parties to realize economies of scale and to optimize their resources while ensuring high levels of availability, stability and security. Solutions models for such centralized processing and storage of e-business transactions include, at a high level:

- Build-it-yourself: this involves a project managed by one or more of the organizations in a group to assemble the software and hardware components required to operate what is sometimes referred to as an 'internal hub'.

- Hosted internal hub: when such an ‘internal hub’ is operated by a third party on behalf of one or more of the organizations in the group, the result is often referred to as a hosted solution.
- ASP/external hub: the centralized processing and storage of electronic business documents can also be outsourced to a specialized organization, which is then often called an Application Service Provider.

In real life, many larger companies apply hybrid models, often based around a shared infrastructure (whose operation may or may not be outsourced to a hosting partner) that interoperates with one or multiple external hubs. Such solutions will often serve as a focal point for various EDI, scanning, manual interface (‘web EDI’) and other types of document interchange and storage solutions with a view to offering maximum flexibility and the lowest-possible participation threshold to suppliers, customers and business partners. A virtually unlimited number of combinations of models is possible, and few groups will have exactly the same infrastructure.

Philosophically, the trend towards centralization of electronic business processes for cohesive groups of organizations calls into question a number of distinctions that many laws and enforcement agencies still work with. It is increasingly difficult to distinguish between the public and the private domains in business; complex, often loosely-coupled networks of businesses will be working alongside and with one another in dynamically-changing constellations that defy all categorization. As further discussed below, the distinction created by the Directive between EDI and non-EDI is therefore essentially an artificial one, and one that long-term will not remain sustainable without creating significant confusion in the marketplace.

ICC believes that the Directive and a significant number of Member States’ laws transposing the Directive do not go far enough in their acknowledgement and facilitation of the business trends described above. Electronic invoice sending and storage can be outsourced, but outsourcing of all transactions in a group to the same party (which may be a large customer in a supply chain, or a service provider; both are rule rather than exception in many business networks) will in many instances not be permitted. A common interpretation of German law, for example, when the electronic signature compliance option is chosen, the signing and the validation of the signature on the invoice must be performed by a different party. In some countries there has been the suggestion that signing or signature validation ‘is expected to’ (read: must for compliance purposes) physically take place in the country of the signatory or verifying party. Rules of this nature can require business groups to distribute complex technology to customers and suppliers of varying sizes, which can lead to higher costs and lower reliability and security in the group system.

ICC believes that EU governments should increase their understanding of market trends and realities. EU governments should further minimize the number of rules that create barriers to rational business choices, in particular when such choices present a clear potential to improved compliance with fundamental regulatory objectives such as fraud prevention.

A strongly related trend, which will be discussed in more detail under the electronic signature compliance section, is the use of both internal and external Certification Authorities (CAs). ICC advocates an open approach to the deployment of electronic signature and other authentication

technologies; non-discrimination between ‘public’ and ‘private’ CAs is an important precondition for such policies.

8. Security compliance

The Directive’s second main condition for acceptance of electronic invoices by Member States is that certain security objectives must be met: the authenticity and integrity of invoices must be ‘guaranteed’ in both transport and storage. The Directive essentially offers two ways for organizations to comply with this requirement: through (1) electronic signatures or (2) EDI with contractual security procedures.

A further requirement is that invoices in storage should remain legible. This is not a security requirement, but we will address it in this section because the subject is in practice closely related to security choices.

8.1. Applicable law for security compliance purposes

In cross-border invoicing situations it is sometimes difficult to establish which law should determine the security measures to be applied to different parts of the invoicing transaction.

ICC’s interpretation of the Directive is that as a general rule, Member States must accept invoices secured in compliance with the country of the sender’s applicable VAT number for that invoice. Our understanding is further that each party’s local rules (‘local’ here being the country of VAT registration) apply for storage of sent and received invoices. The only formal exception to this rule is where the Directive allows Member States to reject incoming invoices secured under the ‘other means’ rule of the Directive. In practice, however, a second exception to the sender country rule appears to arise frequently in countries requiring Qualified Electronic Signatures: these countries often enforce their internal requirements – de facto requiring use of nationally-accredited Certification Authorities – also for invoices sent from other Member States. While these policies are rarely explicit, the result of lengthy delays and other administrative obstacles are from a commercial perspective identical to non-acceptance. Needless to say, such de facto contradictions of a system built for lowering barriers to e-invoicing in the Internal Market are unhelpful for businesses that want to set up cost-effectively compliant systems.

In practice, single companies often use multiple VAT numbers for different invoicing purposes. This means that a company based in country A may need to ensure compliance as a sender of electronic invoices from countries B, C and D, and store these invoices in

compliance with the local rules in each of these countries. Aside from the fact that this can lead to multiple and sometimes conflicting requirements applying to one company’s invoicing processes, such situations can create problems in terms of granting tax authorities access to ‘their’ invoices through a local web interface; indeed, the company may not have a physical establishment in all countries where it is registered for VAT.

8.2. Web-EDI classification

A relatively common way to set up e-invoicing with smaller suppliers is to make a web-based form available in which invoice data can be entered manually. This significantly lowers the threshold for supplier connectivity, since the supplier only needs a PC with an Internet connection and a browser. However, despite its name that suggests that these practices are a form of EDI, it has become clear that the strong manual intervention on the sender's side in the view of many tax authorities makes it impossible to apply the EDI compliance option to such invoices. This would then place web-EDI invoices in either the electronic signature or (if available) 'other means' compliance categories. Deployment of electronic signatures in such a scenario, however, makes it important to determine whether the system will be qualified as a 'normal' (outsourced or direct) invoicing process or as self-billing; questions relating to the use of electronic signatures in self-billing systems are discussed in 8.4.3.

8.3. The EDI compliance option

Electronic Data Interchange (EDI) is one of the two main ways (the other being electronic signatures) to fulfill the authenticity and integrity requirements.

The definition of EDI the Directive refers to is a European Commission Recommendation from 1994 relating to the legal aspects of EDI. EDI is defined as "the electronic transfer, from computer to computer, of commercial and administrative data using an agreed standard to structure an EDI message." EDI message is further defined in the same Recommendation as a "set of segments, structured using agreed standards, compared in computer-readable format and capable of being automatically and unambiguously processed." This definition was crafted at a time when the prevailing form of automated B2B transactions used EDIFACT messages over Value Added Networks (VANs). A much-discussed issue is whether the EDI compliance option in the e-Invoicing Directive is also applicable to automated B2B transactions that use, for example, XML over the plain Internet. This question is currently being addressed by CEN. ICC believes that neither the transport medium nor the standard used should be significant in classifying a system as EDI, as long as the main components of the above definition have been met (structured, agreement including on standards, capable of automated processing). In particular, ICC believes that there should not be a need for official government 'recognition' of specific types of transport media or formats before they can be recognized as EDI.

A definitional question of greater practical importance than the nature of the format or transport medium is when a system is 'automated enough' to fall under the EDI definition. When a series of documents (forecast order, order, acknowledgement, receipt etc) are exchanged leading up to an invoice, which of these steps need to be automated

to what extent for the system to be classified as EDI? It would be useful if this point could be clarified at the EU level.

When a system has been recognized as EDI, this system then needs to meet the requirement that the interchange agreement must provide for the use of "procedures guaranteeing the authenticity of the origin and integrity of the data". Our discussions with various EU tax authorities have shown that this issue is currently mostly resolved through reference to the

model interchange agreement incorporated into the afore-mentioned EU Commission Recommendation. Among other things, this model agreement stipulates in article 6:

“6.1 The parties undertake to implement and maintain security procedures and measures in order to ensure the protection of EDI messages against the risks of unauthorized access, alteration, delay, destruction or loss.

6.2. Security procedures and measures include the verification of origin, the verification of integrity, the non-repudiation of origin and receipt and the confidentiality of EDI messages.

Security procedures and measures for the verification of origin and the verification of integrity, in order to identify the sender of any EDI message and to ascertain that any EDI message received is complete and has not been corrupted, are mandatory for any EDI message.”

ICC believes that while this language can be modernized to reflect current best security practices in EDI communities, it is a good touchstone for regulators when they need to evaluate whether a system classified as EDI fulfils the invoice authenticity and integrity requirements. Traditional EDI implementations often include sufficient security services, and their standard agreements typically reflect these. If invoices are transferred over the plain Internet without value-added service providers adding e.g. receipts and integrity checks, then governments should consider as compliant any parties that adopt such measures themselves and that document them in their interchange agreement.

Many Member States have further used the Directive’s option to require a monthly summary statement. In some countries this summary statement must be on paper, in others it may be both in paper form or electronic. Some of the latter Member States allow the summary statement to be in electronic format only when the electronic summary statement is electronically signed (e.g. with a Qualified Electronic Signature). Some Member States have laid down specific rules as to the procedure of creating summary statements and their content. While ICC understands the need for tax authorities to have insight in the automated exchanges of parties, it also believes that if parties have implemented sufficient measures to prove the authenticity and integrity of invoices, then it would seem discriminatory for the EDI compliance option, especially in comparison with the electronic signature compliance option, that an additional evidence measure like a summary statement must be produced. One pragmatic step that Member States might consider, therefore, is to enforce the requirement for summary statement only when the system does not apply a method of authenticity and integrity protection that offers sufficient time-independent proof of these security attributes. In this context a distinction can be made between, on the one hand, techniques that can provide good de facto authenticity and integrity protection (e.g. basic Secure Sockets Layer or message hash comparison), and techniques (such as certain types of electronic signatures including the EU Advanced Electronic Signature) that have been designed in addition to allow such security attributes to be evidenced regardless of time.

A further requirement imposed by some Member States under the EDI compliance option is that a partner folder, created under certain specific conditions, be present in the system. ICC believes that these additional requirements (which are not included in the e-Invoicing Directive) can create unnecessary barriers to cross-border invoicing. While Member States need the freedom to adopt EU Directive rules to their national circumstances, they should be aware that even the smallest additional requirements can create significant cost obstacles for invoicing in a European Union with 25 Member States.

Finally, the Directive's requirement that the integrity, authenticity and legibility of invoices be guaranteed throughout the storage period applies to invoices under both the EDI and the electronic signature compliance options. Member States that have issued specific decrees and/or other official information on meeting these requirements generally remain vague about how they expect parties that do not use electronic signatures to provide evidence of invoice authenticity and integrity in storage. ICC believes that many types of secure storage products and services offer sufficient security. However, it might be useful if tax authorities could provide more specific guidance on these aspects. Section 8.5 addresses this and other storage issues in a broader context.

8.4. The e-signature compliance option

8.4.1. General

The Directive cross-refers to the EU Electronic Signature Directive for several aspects of the e-signature compliance option.

This cross-reference has caused many problems because the e-Signature Directive addresses a very different aspect of e-signatures than the e-signature compliance option in the e-Invoicing Directive: the former is geared towards “legal” signing e.g. expressing the intent to be bound by a contract, while the latter prescribes e-signatures exclusively for security purposes. These two dimensions of e-signatures are not properly addressed in the EU e-signature legal landscape, and ICC regrets that these problems have now been inherited by the e-Invoicing Directive.

ICC further regrets that transposition and enforcement of the Electronic Signature Directive has led to a relatively high level of diversity among Member States. This fact has undermined the effectiveness of the reference to the Electronic Signature Directive. While ICC respects and supports the EU's ongoing commitment to electronic signatures for creating higher levels of trust in electronic commerce, it also believes that many of the underlying assumptions of current EU rules in this area have been overtaken by market realities. In particular, the vision of a limited number of highly trusted public roots to which massive amounts of certificates could be anchored to instill trust in

various types of electronic interactions has proven to be unrealistic. While the use of certificates continues to grow, this growth is mostly due to a more pragmatic approach by businesses that primarily seek to make their business processes more secure and legally predictable. Public Certification Authorities certainly play an important role in many successful implementations of Public Key Infrastructure (PKI), however businesses often choose in-house Certification

Authorities for larger and more complex business environments. New pragmatic types of PKI networks are thus growing from the business process level, and businesses are applying increasingly effective ways to ensure interoperability – in the widest sense – among such networks. These extended trusted enterprise networks are precisely where the exchange of critical documents such as invoices takes place. Imposing specific types of external certificate use in parallel to existing enterprise trust infrastructures will often be not only unnecessary, but also overly burdensome and potentially weaken rather than strengthen security and auditability. Therefore, ICC urges the European Commission and EU governments (including tax authorities) to ensure that for all information compliance purposes, enterprise security measures are subject to a same set of neutral criteria as public security service providers.

It is also important to note that the successful deployment of PKI in recent years has been enabled by the growth of a more realistic vision of the possibilities and limitations of PKI as a trust-enhancing infrastructure. PKI is not a silver bullet technology but a complex multi-disciplinary technique that, just like all other trust techniques, requires trustworthy policies, practices and procedures – in addition to continuous management attention and education – in order to produce any business benefits. By emphasizing the certificate as the pivotal trust carrier in electronic signatures, governments risk sending the wrong messages to the business community. Even the best certificate issued by the most secure and trusted CA is worth very little if simply ‘stuck into’ an otherwise non-secure application or IT environment. Security is always a process; while certificates and PKIs can play an important role in upholding security, they can never do so alone.

It is thus important, in a tax compliance context, that EU governments align their views and expectations of PKI-supported electronic signatures with market realities.

8.4.2. Advanced and Qualified Electronic Signatures

The Directive allows Member States to require either Advanced Electronic Signatures or Qualified Electronic Signatures (the latter not being an official EU term). ICC has a number of observations on these alternatives.

The EU definition of Advanced Electronic Signature is very broad. While most experts agree that this definition is primarily about PKI-based digital signatures, there exists no perfect industry consensus around this view. Experts do agree, however, that the definition primarily aims at PKI-based digital signatures. To the extent that digital signatures are meant, then, most experts agree that the requirement that the Advanced Electronic Signature must be “capable of identifying the signatory” implies that purely technical digital signatures cannot be Advanced Electronic Signatures. In ICC’s view it is important for governments to more explicitly support the concept that security and trust cannot be built on technology alone. Indeed, it is easy even for moderately skilled

technicians to issue certificates using freely downloadable software from the Internet. If these certificates are not issued and managed under procedures that are communicated to certificates holders and relying parties in a way that is adequate in the circumstances, then they are practically useless as a trust instrument – they can even quite easily be an instrument of fraud or

intrusion. ICC believes that EU governments should urgently clarify this, but without creating yet another set of rules. One pragmatic advice to businesses would be to recommend use of the framework of policies, practices and agreements embodied in the IETF Request for Comment (RFC) 3647 (formerly RFC 2527).

Concerning the confusion arising from the different objectives of e-signatures between the e-Signature Directive and the e-Invoicing Directive, ICC is very grateful that many EU Member States have now created conditions (through legal changes, clarifications or modified enforcement practices) for Advanced Electronic Signatures to be created by legal persons for e-invoicing purposes. Electronic invoicing is all about automation of invoicing processes, and thus signatures should be capable of being created automatically. The analogy with the paper signature, which is at the root of the misconception that legal persons (and thus servers) should not be capable of creating electronic signatures, is incorrect when the electronic signature is required for security purposes only (rather than for 'signing' in a legal sense). This improvement should also urgently be extended to the Qualified Electronic Signature. The EU could use the new Swiss legislation in this area as an example of a pragmatic way forward.

Another problem stemming from the e-Invoicing Directive's reference to the e-Signature Directive is that this in some countries (in general countries requiring Qualified Electronic Signatures) makes so-called What-You-See-Is-What-You-Sign (WYSIWYS) requirements applicable to the invoicing process. While in some of these countries tax authorities have suggested creative ways of meeting this requirement in a way that would still permit some level of automated 'batch' signing, these requirements should in ICC's view be removed as soon as possible. The principal benefits of e-invoicing derive from process automation, and if so many other critical e-invoicing-related processes can be entrusted to carefully-programmed machines, then this must also be true for the creation of the signature. Just like the requirement that the signature be placed by a natural person, WYSIWYS requirements are based on the misconception that the electronic signature is always a signature in the legal sense rather than merely a security measure.

Another set of legal barriers to effective roll-out of e-invoicing in or with the EU concern implicit or explicit requirements that the creation of the electronic signature and/or its validation (verification) take place within the country where the party performing this action is physically based. Such requirements hinder various common outsourcing and centralized processing methods. The same is true for requirements that the creation of the electronic signature and/or its validation be handled by two different legal entities; such requirements have led to e-invoicing service providers taking expensive yet fully artificial measures of channeling these different services through different legal entities under their control.

A final issue is that in certain countries requiring Qualified Electronic Signatures, stringent requirements exist not only on the process of validating a signature on a received invoice, but also on the software used for this process, and in these same countries a log of the validation process must be stored together with the received invoice. While countries are of course free to choose the Qualified Electronic Signature level under the e-invoicing Directive, such rules can be burdensome because they are much more demanding than the frameworks in other Member

States, where tax authorities will content themselves with being able to re-perform validation at the moment they access the stored invoices.

8.4.3. Electronic signatures and self-billing

When a system is classified as self-billing, the rule in many countries is that the invoice should be presented to the supplier for approval before being formally issued. One difficult issue in this context is whose law determines the security requirements for the invoice; logically, since the formal invoicer is still the supplier, we assume that the main rule continues to apply (security requirements are determined by the law of the country from which the invoice is sent for VAT purposes). Secondly, as with outsourcing to a service provider, the question arises whose certificate the customer creating the invoice should sign with: can the certificate be in the customer's name or does it have to be in the supplier's name? These issues, which can have relatively significant implications at the implementation level, are left unanswered in most Member States.

8.4.4. E-invoice outsourcing

When parties outsource their invoicing to a service provider ('platform' or 'hub'), the following uncertainties arise in relation to the use of electronic signatures:

- Applicability of the signature requirements to the 'first mile' of the transaction (the sending of invoicing data to the service provider). Most countries consider the signature requirements not to be applicable to this transport, however ICC considers it would be helpful if the European Commission could place more emphasis on the fact that the sending party (the supplier) remains fully responsible for the invoice. Invoicers should be better informed that they can potentially be held responsible for any errors that occur in the 'first mile' due to faulty or insufficient security.
- Which law's security requirements apply? It is often unclear whether the signature placed by the service provider should meet the requirements of the law of the service provider's country of residence, or that of the country from which the invoicing party is formally invoicing (i.e. the country of the VAT number used by the invoicer).
- Whose certificate? When invoicing service providers create electronic signatures for invoicing parties, it is obvious that the service provider needs to sign with a private key hosted in its technical environment; however, most Member States have not provided any guidance as to whether the associated certificate should be in the name of the service provider or of the invoicer. The answer to this question can have far-reaching practical and cost implications.

8.5. Storage

As a general rule, EU companies have to archive their sent and received invoices in the form and format in which they were sent/received.

In certain cases, local laws other than the law transposing the e-Invoicing Directive lay down technical requirements on the archive to be used; it would be of significant help to companies trying to set up cross-border invoicing if governments could provide information on such requirements in conjunction with information provided on electronic invoicing requirements.

Another set of issues that might arise is practices around storage and, in this connection, how evidence of authenticity and integrity of archived invoices can be provided when electronic

signatures are not used. While the established legal framework around electronic signatures in the EU provides a set of relatively well-understood parameters for providing evidence of the authenticity and integrity of information regardless of time, outside this framework one will presumably need well-documented procedures and logs around the technical storage solution in order to demonstrate that invoices in the archive have not been changed during the mandatory storage period. Very few countries have provided any guidance on how companies that archive electronic invoices without signatures can prove that these invoices are authentic and have not been changed.

In some countries, finally, specific measures such as additional time-stamping of invoices once archived are required; needless to say, such requirements do not facilitate e-invoicing deployment. Such rules are in our view unnecessary because digital signature technology, best practices and the EU regulatory framework together form a very good basis for allowing the original signature to be verified regardless of time.

As mentioned, some countries require the receiver of an electronic invoice not only to store the received invoice, but also – in case the electronic signature compliance option is used – a log of the signature validation process. In the end, therefore, certain parties have to store a relatively large number of supplementary items with an invoice:

- In some countries parties have to store any converted versions of the received invoice.
- Due to readability requirements, parties may have to store style-sheets or PDFs to make machine-readable information intelligible to tax inspectors.
- In order to allow long-term verifiability of signed invoices, parties may have to store Certificate Revocation Lists as well as, in certain cases, applications that were used to perform the original signature validation (note that this will also frequently cause parties to keep related hardware during the storage period).

The combination of explicit and tacit storage-related requirements on the one hand, and business practices and business objectives on the other, can create massively complex schemes for parties that want to organize cross-border invoicing with their customers and suppliers.

8.6. Paper-electronic parallel (hybrid invoicing)

Many companies today already possess the technological capacity to send and receive invoices electronically. Because they (rightly) view the situation concerning legal requirements as complex, such systems are today often used for convenience, while paper flows and storage are maintained in parallel in order to ensure regulatory compliance. Not all companies will succeed, or aim, to fully dematerialize all invoicing flows. Many companies will continue to use scanning processes for invoices from certain classes of suppliers.

It appears that some countries require there to be a parallel compliant paper-electronic invoicing flow for some time before companies are authorized to fully rely on their electronic flows. Other countries seem to prohibit such parallel flows from the start. Needless to say, these requirements can in cross-border practice be quite confusing and cause roll-out costs to increase significantly. ICC believes that the most sensible rule is that companies can choose which invoices are to be viewed as electronic, and which as paper, for compliance purposes; based on this choice, tax authorities should then determine whether these invoices comply with their respective

requirements. Whether companies in practice operate parallel flows on another type of support, without presenting these flows for formal compliance purposes, should be of no consequence for tax authorities.

8.7. Timestamping

While few national laws explicitly require electronic invoices to be time-stamped using any specific type of technology, some experts claim that many national laws (if not invoice-specific rules, then related accounting laws) implicitly require use of PKI-based timestamping connected to highly reliable time-sources. ICC acknowledges that (for both compliance and business reasons) it can be important to establish when an invoice was created, sent and/or received; however we also believe that the lack of clarity around these issues is causing too much confusion in the marketplace. Governments, ideally through a common mechanism such as the European Commission, should advise businesses on minimum measures concerning the recording of time in invoicing processes to ensure compliance.

8.8. Notification issues

A number of countries have used the option provided in the e-Invoicing Directive to require organizations to notify the tax authorities prior to switching to electronic invoicing. This option runs out on 31 December 2005. However, in some countries organizations may be required to notify their use of certain types of cryptographic systems, such as those that companies might need to use in connection with PKI-based signatures and encryption. Where such related notification requirements exist, it would be helpful if governments could note this when providing information on electronic invoicing requirements.

Document n° 460/592

1 December 2005