Issues of Security and Interoperability in Electronic Public Procurement

Christine Kirchberger & Jon Ramón y Olano

1 Introduction

In this paper the new legal framework for public procurement in the EU will be discussed from the point of view of electronic security and interoperability. The importance of homogeneity as relevant factor resulting from the new legislation will be stressed and specific problems will be identified. For this discussion it will be necessary first of all to define some concepts: public procurement, electronic procurement and electronic public procurement. Once these concepts are defined, the needs for electronic security and interoperability within the new public procurement procedures and systems will be presented. Then different issues that might hinder future developments of electronic commerce business models within the field of public procurement will be analysed.

2 The Concept of Electronic Public Procurement

2.1 Public Procurement

In the European Union, with the exception of a few key strategic economic sectors where public involvement is greater, the State very rarely manufactures and produces through State-owned enterprises the goods and services which public authorities require in order to perform their public duties. Public authorities normally resort to the market to purchase and contract their needs. This purchasing is legally articulated through the conclusion of contracts between public authorities and the providers of works, goods and services and it is known as public or government procurement. In other words, public procurement generally relates to the contractual business relationship between any public authority and its suppliers and contractors.

The contracting entities awarding these contracts are required to follow certain procedural rules in putting out their contracts to tender. The procedural rules apply to contracts exceeding set threshold values, but the principles extend to all contract awards. Some of these include the principle of equal treatment, the principle of non-discrimination, the principle of transparency, and the principle of proportionality.

Suppliers, service providers and works contractors therefore have the right to fair play and equal treatment by the contracting entities. On their side, however, the contracting entities aspire to discharge their functions in an effective, efficient and economic manner, achieving value for money in selecting the lowest priced offers or, alternatively, of the economically most advantageous valid tenders.

2.2 Electronic Procurement and Electronic Public Procurement

Electronic procurement in the private sector can be defined as the use of electronic methods in every stage of the purchasing process from identification of requirements through to payment, and potentially to contract management. This business relationship is commonly termed "Business to Business" or "B2B". Electronic procurement in the public sector is termed "electronic public procurement", "Business to Government" or "B2G". This process does not include the consumer type relationship between a public authority and its citizens. Nor does it relate to payment of fees and charges, by external organisations. Electronic payment mechanisms, other than those between the contracting public authority and its suppliers and contractors, are excluded from the electronic procurement process, although the underlying technologies may be similar.

2.3 The Calls for Electronic Public Procurement in the EU

Already in 1998, the European Commission called upon Member States to stimulate a "pan-European electronic procurement environment" [1] in which 25% of procurements take place electronically by 2003, whilst the conclusions of the Presidency from the Lisbon European Council of March 2000 called upon the Commission, Council and Member States to ensure that it is possible by 2003 for all Community and government procurement to take place on line.[2]

The importance attached to electronic public procurement has also been underlined by the Council of the European Union in its Conclusions from November 2003 on the Role of e-Government for Europe's future. In these conclusions the Council invites the Commission and the Member States to launch, in 2004, a set of pan-European e-Government pilot projects with a view to evaluating necessities, obstacles and solutions. The Council specifically mentions electronic public procurement as one of the pilot projects to be launched in order to contribute to the competitiveness of European businesses.

These statements of the Council are fully in line with the relevant objectives of the e-Europe Action Plan 2005 "Government online: electronic access to public services". The e-Europe Action Plan, which the Commission adopted in 2002, sets very ambitious goals, focusing on "stimulating services, applications and content that create new markets and reduce costs and eventually increase productivity throughout the economy". Amongst the goals set is that modern online public services should be available to businesses and citizens by 2005.

On public procurement, the Action Plan specifically states that Member States should carry out a significant part of public procurement electronically, i.e. as a service provided online to businesses. With a view to establishing pan-European e-Government services to businesses and citizens, the Action Plan states that the Commission will issue an agreed interoperability framework in

1 European Commission Communication, *Public Procurement in the European Union*, COM (98) 143.

2 Point 17 of the conclusions.

support thereof. This framework will address information content and recommend technical policies and specifications for joining up public administration information systems across the European Union.

The e-Europe Action Plan, which covers the period until the end of 2005, will be succeeded without doubt by an e-Europe Action Plan 2008 or 2010, the latter being the target date for implementing the Lisbon Strategy of which the e-Europe Action Plan is a part.

The Lisbon Strategy, endorsed by the European Council meeting in Lisbon in March 2000, aims at making "the European Union the most competitive and dynamic knowledge-based economy in the world, capable of sustainable economic growth with more and better jobs and greater social cohesion."

This vision of Europe reminds of a complex puzzle with many pieces, one of which is electronic public procurement or e-Procurement. Another is the underlying interoperability in relation to e-Procurement, especially technical, semantic and organizational interoperability.

The main goals of developing e-Procurement within Europe are:

- To support the new public procurement procedures using electronic means like "dynamic purchasing system", "e-Auctions" and "e-Catalogues".

- To automate the repetitive processes in order to save time and money on both the demand and supply sides.

- To decrease the potential risk of corruption with more transparency to widen the access to European calls for tenders especially for SMEs.

- To support the development of the Internal Market in ensuring interoperability within Europe.

Finally, in March 2004, the European Union adopted a legislative framework for electronic public procurement procedures as part of the legislative package of public procurement directives.[3] The Member States now have to implement this framework (within a more realistic time span) so that public procurement can be handled electronically by early 2006.

3 Directive 2004/18/EC of the European Parliament and of the Council on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts [hereinafter Public Sector Directive]. Directive 2004/17/EC of the European Parliament and of the Council coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors [hereinafter Utilities Directive].

3 Some Features of Electronic Public Procurement

3.1 Electronic Public Procurement as a Process: a Vision

The following vision of electronic public procurement could be presented:[4]

The procurement process starts when the contract awarding authority plans the specific procurement. The authority obtains data for its procurement planning from a range of databases that may cover potential suppliers, purchasing statistics, etc. A procurement computerised chronogram is produced, and a decision taken about the procurement procedure to be used, e.g. open procedure. A procurement request is then displayed on the screen. The contracting authority can decide whether or not standard conditions are to be used for the procurement in question, and if so, which. If standard conditions are chosen, the computer produces the respective standardised call for tender, that in any case can always be amended or modified by the contracting authority. The requirement specification is formulated at product level on the basis of a product classification system such as the Common Procurement Vocabulary (CPV).

Once the call for tender has been completed, it is automatically submitted for advertisement to OJ/TED.[5] The submission is made in SIMAP[6]-compatible format. The call for tender is also posted on the contracting authority's website from where it can be downloaded by suppliers. Anyone interested in additional information regarding the call for tender can apply for it using the website. The suppliers' computers download the call for tender and navigate through it automatically, entering most of the information requested, e.g. price, package size, product attributes, etc, without human intervention. After a final manual check, the tender is submitted electronically to the awarding authority.

The awarding authority keeps the tenders confidential but it is not able to open them before the prior appointed opening date. Various qualification data are obtained electronically from different authorities and registries to ensure that the suppliers are qualified. The tenders can be opened, selected and evaluated automatically, producing a draft ranking of the suppliers in the light of the review criteria and the weighting/ranking system established in advance by the contracting authority. The awarding authority checks the tender evaluation manually and awards the contract. A final contract is assembled automatically and then sent to the selected supplier for electronic signature. The contract is then returned to the contracting authority, which also signs it. Once the contract has been concluded, the losing suppliers are automatically notified.

Then the actual contract management process starts. Then public entities order goods, services of works from existing contracts that might be materialised

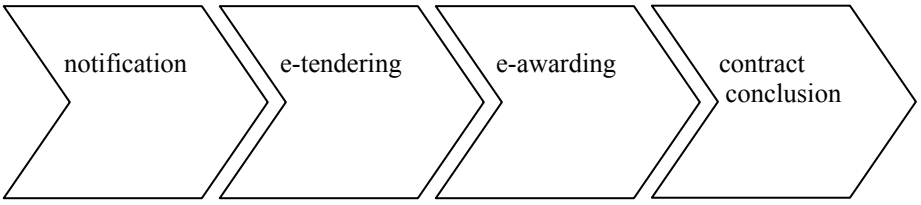
4 *Report 1 on electronic public sector procurement*, Swedish Association of Local Authorities (Svenska Kommunförbundet), 2000, Section 4.2.

5 OJ: Official Journal of the European Union. TED: Tenders Electronic Daily; Supplement of the Official Journal of the European Union. All public tenders exceeding specific contract values must be published in the Supplement to the Official Journal of the European Union and published throughout the EU.

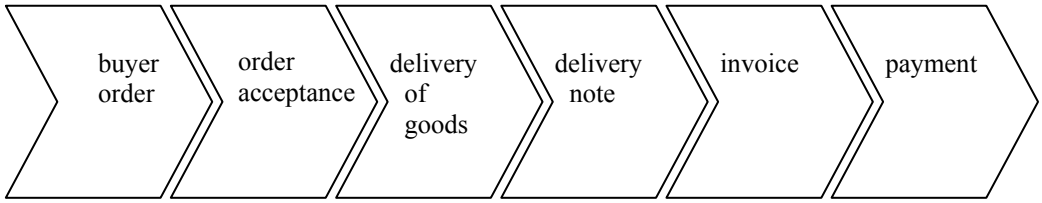
6 Systėm d'Information pour les Marchés Publiques. The first European information worksite for electronic public procurement, which can be found at "http://simap.eu.int/".

in the form of e-catalogues for example, receive delivery, are invoiced for the goods received and subsequently make payment, closing the e-commerce cycle.

This vision presents electronic public procurement as a process that can be divided into two sub-processes: contract establishment and contract management. Contract establishment then contains the following main activities:



Contract management contains the following main activities:



3.2 Electronic Public Procurement as an Open Process

The electronic procurement process that has been described can be based on either EDI/EDIFACT or Internet as access technology. Three types of access solutions can be applied in relation to electronic public procurement: A virtual private network (VPN), an extranet or an open access web site.

1. VPN (Virtual private network)

   A VPN utilizes the infrastructure of a public network such as the Internet. All data is communicated between the connected computers via encrypted "tunnels". The solution requires use of certain additional software applications, which ensures a high level of security in exchange of data. It is impossible for users who are not part of the VPN to gain access to the system unless they become members of the VPN. VPN solution are relatively cost intensive in the initial stage and require also organisational resources.

2. Extranet

   In an extranet solution, users are granted access to the intranet of an entity, which normally is only accessible to employees of this entity. Outside

users receive a username and a password and can consequently access the system via their web browser, which means that no additional applications are required. The lack of software requirements leads to less costs for the investments, compared to the VPN.

3. Open access

Granting access to users via an Internet website is the main idea of an open access solution. Accessing the website is commonly controlled by a username and a password. Investment costs are minimal as the only requirement for this solution is internet access and a web browser.

The three solutions are not mutually exclusive and can be combined. Open access is the most widely applied solution in the EU, followed by the use of extranet and virtual private network solutions.[7]

The clear tendency towards the use of open access solutions, on the one hand, demands few investments and makes the easiest access to the procurement, thus promoting market transparency and competition. On the other hand, these solutions demand different technical inputs that will be discussed in Chapter 5 and 6 in order to balance the trade-off between market access and security. Openness makes issues such as security, commodity coding systems and interoperability of essence. Without all these instruments, any open solution would expose any procurement procedure to risks that would make it totally unreliable, thus making compliance with the legal principles of public procurement impossible. Still market access and competition demand, at least in the first phases of the procurement process, open access solutions. For later phases of the procurement involving communication between buyer and selected (or awarded) supplier, some buyers tend to prefer the higher level of security offered by VPN or extranet solutions. Even in these phases of the procurement, open access solutions are being developed, which claim to offer a sufficient level of security for the majority of procurements.

4 Principles of Public Procurement

The EU public procurement market is a fundamental part of the Single Market and is governed by rules intended to remove barriers and open up new, non-discriminatory and competitive markets. The principle of public procurement is to open up the choice of potential suppliers to the public sector and utilities resulting in reduced cost, while at the same time, opening up potential markets for companies. The rules aim to ensure the free movement of goods and services within the EU[8] and that public sector purchasing decisions are based on value for

7 *Analysis of electronic public procurement projects in the EU*, Study carried out by PLS-Ramboll for the European Commission Internal Market DG, November 2000, p. 23.

8 Recital (2) of the Public Sector Directive.

money achieved through competition.[9] By-product of these basic principles, the following ones will be also of application:

1. the principles of equal treatment and non-discrimination,[10] by which contracting authorities should treat all enquiries equally to avoid discrimination on the grounds of nationality or the origins of goods and services and encourage the use of EC based technical standards as opposed to national ones;

2. the principle of mutual recognition of documents and certificates issued by authorities of the Member States;

3. the principle of proportionality, by which qualification requirements and requirements regarding the subject matter of the contract must have a natural relation to the supplies, services or works which are being procured; and

4. the principle of transparency,[11] which involves the predictability and openness of the procedures. For this, the contracting authorities should advertise the calls for tender above the Directives' thresholds across the EU, use objective criteria in tendering and contract award procedures and provide suppliers with access to appropriate documents as early as possible and public access to the outcome.[12]

Finally and as a specific principle of public procurement, "the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential; such information includes, in particular, technical or trade secrets and the confidential aspects of tenders".[13] This is the principle of confidentiality that apparently clashes with the principle of transparency, in particular in the case of electronics auctions, during which the bids are partially communicated to the pool of suppliers. In this case, the principle of confidentiality would be subordinated to the principle of equal treatment (all participants receive the same information) and to the principle of transparency.

9 *Ibid.*

10 Article 2 of the Public Sector Directive.

11 *Ibid.*

12 *The Legal and Market Aspects of Electronic Signatures*, Jos Dumortier et.al., Study for the European Commission - DG Information Society, Leuven: Interdisciplinary Centre for Law & Information Technology, 2003, available at "http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf", p. 44.

13 Article 6 of the Public Sector Directive.

5 Security and in Particular Electronic Signatures

The recently adopted EC legislative framework on public procurement establishes several legal evaluation criteria. These include, inter alia, confidentiality, integrity and authentication.[14] Confidentiality requires that information is not disclosed in any unauthorised manner, which also includes ensuring that the content of request for participation and tenders is not examined before the deadline. Integrity means that information is not altered or modified in an unauthorised way or that modifications are at least detectable. Last, but not least, authentication is necessary to guarantee the identity of the bidder when participating in a tender.

Article 42.3 of the Public Sector Directive refers explicitly to integrity and confidentiality:

> Communication and the exchange and storage of information shall be carried out in such a way as to ensure that the *integrity of data* and the *confidentiality of tenders and requests* to participate are preserved, and that the contracting authorities examine the content of tenders and requests to participate only after the time limit set for submitting them has expired.

One way to fulfil these requirements, which are also mentioned in Annex X of the Public Sector Directive, is the use of electronic signatures. Recital (37) as well as Paragraph (a) in Annex X of the Directive refers explicitly to the Electronic Signature Directive[15]. Recital (37) states that

> Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ("Directive on electronic commerce") should, in the context of this Directive, apply to the transmission of information by electronic means. The public procurement procedures and the rules applicable to service contests require a *level of security and confidentiality higher than that required by these Directives*. Accordingly, the devices for the electronic receipt of offers, requests to participate and plans and projects should comply with specific additional requirements. To this end, *use of electronic signatures, in particular advanced electronic signatures*, *should, as far as possible, be encouraged*. Moreover, the existence of voluntary accreditation schemes could constitute a favourable framework for enhancing the level of certification service provision for these devices.[16]

14 *eProcurement Feasibility Study*, Final Report DG Entr, 2003, "http://europa.eu.int/ISPO/ida/export/files/en/1793.pdf", p. 15.

15 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [hereinafter Electronic Signature Directive].

16 Emphasis added by the authors.

Annex X of the Directive states, inter alia, that

> Devices for the electronic receipt of tenders, requests for participation and plans and projects in contests must at least guarantee, through technical means and appropriate procedures, that:
>
> (a) electronic signatures relating to tenders, requests to participate and the forwarding of plans and projects comply with national provisions adopted pursuant to Directive 1999/93/EC;

In a statement in December 2003 the European Commission referred to the use of "qualified electronic signature" in the course of electronic public procurement, although the adopted Directives use the term "advanced electronic signatures". The Commission further announced that the integrity of data and the confidentiality of tenders "do not depend on the choice of whether to require electronic signatures and in which form." [17]

5.1 Types of Electronic Signatures

An electronic signature is a technical tool to authenticate certain data.[18] This is not to be confused with methods for entity authentication, e.g. accessing a bank account with a PIN-code. Confirming a money transfer, however, with a PIN-code is considered as data authentication and therefore regarded as an electronic signature.[19]

It should be kept in mind, that the term "signature" in the Directive refers to a legal concept, and not to a technical method.[20] The directive, does, however, not establish any legal effect of electronic signatures as such, except the admissibility of electronic signatures as evidence in court and the principle that certain types of electronic signatures have to be regarded equivalent to handwritten signatures in the national laws of the Member States.[21]

From a technical point of view, electronic or digital signatures are usually created by using asymmetric encryption that utilizes two pair of keys: a private key to encrypt data and a public key to decrypt data. Information encrypted with the private key can only be decrypted with the public key and vice versa. By encrypting a message using the secret private key (only accessible to the signatory) the sender is signing it electronically. This guarantees authentication

---

17 Public procurement: Commission welcomes conciliation agreement on simplified and modernised legislation, 03/12/2003, IP/03/1649.

18 *See* Recital (8) of the Electronic Signature Directive "capable of authenticating data electronically". Authentication can be understood as involving both signer authentication (the signature indicates who signed the document) as well as document authentication (the signature identifies what is signed, thus making it impossible to falsify or alter the content without detection).

19 The Legal and Market Aspects of Electronic Signatures, *supra* note 12, p. 29.

20 *Ibid.*

21 *See* Article 5 of the Directive.

(i.e. the message was signed by the signatory) and can to a certain extent enable identification of the signatory, depending on the existence of a trusted third party confirming the identity with a certificate. The receiver of the message will then decrypt the document by using the public key, which was either attached to the message, or is publicly available at a depository usually administered by a trusted third party (also called Certification Authority). A system allowing to administer the various public keys is commonly called PKI (Public Key Infrastructure).[22] The technique utilized for digital signatures also allows for establishing integrity, as any attempt to alter the content of the message would invalidate the signature.[23]

From the wording of Article 2 of the Electronic Signature Directive it seems clear that the definition of "electronic signature" refers to the use of public key cryptography.[24]

The Electronic Signatures Directive basically distinguishes between three types of electronic signatures, depending on the level of security required:

1. (simple) electronic signatures
2. advanced electronic signatures and
3. qualified electronic signatures.[25]

According to Article 2.1 a (simple) electronic signature can be any data in electronic form that are attached to other electronic data and which can serve as means of authentication.[26] This usually entails encryption, but does not include any methods of identity check of the signatory, i.e. the signature verifies the sender, but does not guarantee the identity of the sender.

Advanced electronic signatures, on the other hand, have to meet certain requirements, according to Article 2.2. The signature has to be:

a) uniquely linked to the signatory;
b) capable of identifying the signatory
c) created using means that the signatory can maintain under her/his sole control, and
d) be linked to the data to which it relates in such a way that any subsequent change of the data is detectable.

---

22 For further information *see* Magnusson Sjöberg, Cecilia & Nordén, Anna, *Managing Electronic Signatures – Current Challenges*, in this volume; Chissick, Michael and Kelman, Alistair, *Electronic Commerce – Law and Practice,* 3 ed, Sweet & Maxwell Limited, 2002, p. 167-188.

23 Reed, C., *What is a Signature?*, 2000 (3) The Journal of Information, Law and Technology (JILT), at "http://elj.warwick.ac.uk/jilt/00-3/reed.html".

24 The Legal and Market Aspects of Electronic Signatures, *supra* note 12, p. 30.

25 The term as such is, however, not mentioned in the Directive, but in several national laws, e.g. the Swedish Act on Qualified Electronic Signatures and the German Signature Act. The Austrian Federal Electronic Signature Law talks about "secure electronic signatures". *See also* The Legal and Market Aspects of Electronic Signatures, *supra* note 12, p. 12.

26 Not to be confused with authorization, which is the process of giving individuals access to a system.

Advanced electronic signatures therefore adhere to the principles of authentication (point a), i.e. the recipient can be sure that a certain message was sent from a certain person, identification (point b), i.e. the recipient can rely on the fact that the sender is also the person she/he claims to be. As already stated identification is not a requirement for (simple) electronic signatures. The notion of integrity, usually linked to electronic signatures, is mentioned in paragraph (d), and includes ensuring that the data was not altered in any unauthorised way.

Qualified signatures, in addition demand certain requirements of the Certification Authority who issues the certificates confirming the identity of the signatory and also establish certain criteria concerning the quality of the certificate. According to Article 1.10 the requirements are stated in Annex I and Annex II of the Directive.

A certificate can be seen as a sort of identity prove which by means of an electronic confirmation links a public key to a certain signatory and confirms her/his identity. In order to be regarded "qualified" a certificate has to fulfil additional requirements, e.g. the certificate has to have a certain content including the identity of the signatory, the time of validity of the certificate, possible limitations concerning the use of the certificate, etc.[27]

5.2 Public Procurement and Electronic Signatures

As already mentioned, Recital (37) of the Public Sector Directive explicitly states that electronic signatures, and in particular advanced electronic signatures, should be encouraged. Although the Directive has only recently entered into force and the member states have not had time to implement the new directives, it is of interest in the context of this article to examine how some of the member states have regulated the use of electronic signatures with regards to electronic public procurement, especially when considering that several European countries are using electronic means in public procurement already today.[28]

The interpretation of a "higher level of security" stated in Recital (37) in combination with the notion of "advanced electronic signatures" is rather unclear at this moment. When evaluated in the light of the statement of the Commission[29] one could argue that the wording "higher level of security" refers to confidentiality and integrity, which makes sense as it is very important in procurement procedures that tenders are not opened before the deadline, which as such has nothing to do with electronic signatures.[30]

---

27 Magnusson Sjöberg, Cecilia, *Elektroniska signaturer - ny lag men fortsatt behov av åtgärder*, JT 2000-01, p. 864-882, at 874. *See also* Article 2.9 and Article 2.10 Electronic Signature Directive.

28 Countries include the United Kingdom, Germany, etc. For a list of different e-procurement initiatives, *see* the website of IDA at "http://europa.eu.int/ISPO/ida/jsps/index.jsp?Fuse Action =showChapter&chapterID=197&preChapterID=0-140-196".

29 IP/03/1649, *supra* note 17.

30 This is also in line with the opinion of the Commission in COM(2003)0503 on the amendment of Article 42 suggested by the European Parliament, concerning a new paragraph in Article 42 that expressly refers to electronic signatures: "The main objective seems to be to obtain a guarantee that it will be possible to detect changes made to tenders after they have

Furthermore, it should be kept in mind, especially when examining e-procurement solutions in different member states, that the Electronic Signature Directive does not mention the term "qualified electronic signature" as such, only the term "advanced electronic signature", which according to the Directive can turn into a "qualified electronic signature" if certain additional requirements are fulfilled. In other words, qualified electronic signatures are a kind of advanced electronic signature. The reference to "advanced electronic signatures" in the Public Sector Directive therefore might include qualified electronic signatures, especially considering the wording "level of security (…) higher than that by" the Electronic Signature Directive.[31]

From a more un-legal point of view, electronic signatures and encryption can contribute to the establishment of trust between the parties[32] in the situation when buyer and supplier do not know each other beforehand, which ocurs more commonly if they are situated in different member states,

The Electronic Signature Directive makes clear that it "does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, (...); for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regards to the conclusion of contracts."[33] This results in the fact that national legislations only have to accept electronic signatures to the extent that documents can be transferred by electronic means. This is, however, the case (either legally or practically) in the following countries.

5.3 Situation in Different European Countries

5.3.1 Austria

In March 2004 e-Tendering, a web based solution for electronic public procurement, was introduced in Austria. Interested suppliers can download the necessary documents and submit their tenders via the portal. Documents handed in must be signed with a secure electronic signatures, which requires a smart card.[34]

---

been submitted and thus reconstitute their original content, and to guarantee that only authorised persons can know about the content of tenders.

In this sense the amendment is superfluous, and it could on the contrary hold back the adaptation of the Directive to technical progress, given that there are other technical means, in accordance with Annex X, of ensuring the security of tenders on reception. In other words, the integrity of data can be ensured by technical or organisational means other than advanced signatures. Since this a field where technological development is rapid, accepting the amendment would mean having to amend the Directive to take account of technical progress."

31 Recital (37) Public Sector Directive.

32 *Public eProcurement, Analysis of eProcurement Initiatives*, Transborder eProcurement, Summary Report, IDA, May 2002, p. 39.

33 Recital (17) Electronic Signature Directive.

34 "http://www.auftrag.at/".

The recently adopted Austrian eProcurement Ordinance[35] refers in Section 2 Paragraph 4 and 5 and in Section 10 to secure electronic signatures.[36] As already mentioned, the term "secure" is equivalent to qualified electronic signatures.[37] Depending on the interpretation of the notion "advanced electronic signature"[38], Austria seems either to be in line with the new legislative framework on public procurement or to demand higher requirements than the Public Sector Directive.

5.3.2 Denmark

The Danish Public Procurement Portal (DOIP) connects public buyers to suppliers in Denmark.[39] According to the website the portal is completely web based, meaning that the only technical requirement is a web browser. Buyers have to sign an agreement with DOIP in order to receive a username and a password granting them access to the system. The use of digital signatures in the future is being discussed.[40]

According to Section 4 of the Cirkulære om indkøb i staten[41], public administrations shall, if possible and economically feasible, use electronic commerce for procurement.

5.3.3 Finland

The Finish e-procurement solution, Sentteri, was developed by Trading House Hansel, the government-owned company responsible for government procurement and purchasing in Finland. The system covers the entire e-procurement process, from notification, tendering, evaluation, ordering, and logistics management to electronic payment procedures.[42]

The Finish Decree on Government Procurement (1416/1993)[43] refers in Section 5 to electronic submitting of tenders and requires a written confirmation

---

35 Verordnung der Bundesregierung betreffend die Erstellung und Übermittlung von elektronischen Angeboten in Vergabeverfahren – E-Procurement-Verordnung 2004.

36 Chapter 3 – „Pflichten des Bieters Form, Verschlüsselung und Signatur des Angebotes § 10. (3) Wird das Angebot in einem einzigen Dokument erstellt, so hat der Bieter dieses Dokument mit einer sicheren elektronischen Signatur zu versehen."

37 Section 2 of the Federal Electronic Signature Law (Signature Law - SigG), in English at "http://www.ris.bka.gv.at/erv/erv_1999_1_190.pdf".

38 *See* above under 5.2.

39 "http://www.doip.dk".

40 *Public eProcurement - Initiatives and experiences, Borders and Enablers*, Study Report, Transborder eProcurement Study, The IDA (Interchange between Administrations) programme, Van Eylen, H. et.al. 2002 "http://europa.eu.int/ISPO/ida/export/files/en/1792.pdf", p. 19.

41 Cirkulære om indkøb i staten, CIR nr 9608 af 20/12/2002 (Gældende), Section on "E-handel § 4. Enhver institution skal, hvor det er muligt og økonomisk fordelagtigt, benytte elektronisk handel til indkøb. Finansministeriet, Økonomistyrelsen, udsender nærmere vejledning herom.", "http://147.29.40.90/delfin/html/c2002/0960809.htm".

42 "http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=528&parent=chapter&preChapterID=0-140-197".

43 Upphandlingförordningen för staten (1416/1993), available in Swedish at "http://www.finlex.

under certain circumstances.[44] It does, however, not mention any requirement concerning electronic or digital signatures.

5.3.4 Germany

The German eProcurement platform eVergabe[45] utilizes asymmetric encryption based on a Public Key Infrastructure (PKI) in order to secure communication between contracting authority and suppliers, as well as the storage of confidential data (e.g. tender related documents). In order to participate suppliers have to acquire a digital signature from a certified certificate service provider, which includes the use of smart cards and smart card readers for storing the digital signatures.[46]

The German Ordinance on Public Procurement (Verordnung über die Vergabe öffentlicher Aufträge) mentions in Section 15 the use of qualified electronic signatures in the course of transmitting tenders.[47] Concerning the requirement of "qualified electronic signatures", the situation is the same as in Austria described above.[48]

5.3.5 Norway

As an approach to eProcurement the Norwegian public sector launched in October 2002 the web portal www.ehandel.no. According to the technical specifications of the eProcurement system, authentication takes place by means of passwords, although more secure means of authentication are planned in the future, e.g. based on PKI.[49] The use of digital signatures in the course of eProcurement is currently being investigated in a project called "Det digitale Trøndelag".[50]

---

fi/linkit/fs/19931416".

44 "Om anbudet har getts per telex, telefax, elektronisk post eller med motsvarande metod, skall en skriftlig bekräftelse av det inbegäras enligt upphandlingens art, värde och skyndsamhet".

45 "http://www.evergabe-online.de/".

46 eProcurement Feasibility Study, *supra* note 14, p. 17. For more information *see Federal Government procurement goes online*, Publication by the German Beschaffungsamt des Bundesministeriums des Inneren, in English at "http://www.bescha.bund.de/media/files/publikationen/englisch_online.pdf".

47 § 15 Elektronische Angebotsabgabe. Soweit die Bestimmungen, auf die die §§ 4 bis 7 verweisen, keine Regelungen über die elektronische Angebotsabgabe enthalten, können die Auftraggeber zulassen, dass die Abgabe der Angebote in anderer Form als schriftlich per Post oder direkt erfolgen kann, sofern sie sicherstellen, dass die Vertraulichkeit der Angebote gewahrt ist. Digitale Angebote sind mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen und zu verschlüsseln; die Verschlüsselung ist bis zum Ablauf der für die Einreichung der Angebote festgelegten Frist aufrechtzuerhalten.

48 *See* above 5.3.1.

49 *Elektronisk markedsplass for det offentlige, Sluttbrukerapplikasjon, Funksjonell kravspesifikasjon*, 2001, "http://www.ehandel.no/data/file/krav_sluttbrukerapplikasjon.pdf", p. 28.

50 "http://www.ehandel.no/index.php/Pressemelding/item/314.html".

At the moment, neither the Norwegian Public Procurement Act[51] nor the Norwegian Ordinance on public procurement[52], mention electronic signatures as such. Section 8-5 of the Ordinance states in paragraph 3 that the tender should be signed. If this includes electronic means can be discussed. Paragraph 2 of the same Section allows for electronic submission of documents if, inter alia, the tender is confirmed as soon as possible in writing to the extent it is considered necessary from an evidence point of view.[53]

5.3.6 Spain

Act 13/1995[54] that regulates contracts entered into by public administrations makes no reference to the use of electronic means. The Royal Decree 1098/2001,[55] which contains the General Regulations to develop Act 13/1995, states in its Additional Disposition 10 that the use of electronic means in public procurement will be regulated in the future by a Ministerial Order produced by the Ministry of Inland Revenue.

The relevant administrative legislation[56] allows the use of electronic means when interacting with public administrations and establishes equivalence with the written form as long as authenticity, integrity, conservation, confidentiality and reception are guaranteed.

Article 3 of the Act 59/2003,[57] which regulates the use of electronic signatures, states that only advanced electronic signatures fulfil all the requisites stated in the above-mentioned legislation. Article 4 of Act 59/2003 states that the regulatory framework established by the Act for the use of electronic signature is

---

51 Available in English at "http://odin.dep.no/nhd/norsk/p10002767/p10002770/024081-990048 /index-dok 000-b-n-a.html".

52 FOR 2001-06-15 nr 616: Forskrift om offentlige anskaffelser, in Norwegian at "http://www.lovdata.no/for/sf/nh/xh-20010615-0616.html".

53 § 8-5. Tilbudets utforming
1) Tilbudet skal være skriftlig og avgis i lukket og merket forsendelse, enten direkte eller pr. post.
2) Tilbudet kan også avgis med elektroniske middel forutsatt at konkurransegrunnlaget åpner for dette og at:
a.tilbudet inneholder alle nødvendige opplysninger,
b. tilbudets fortrolighet bevares frem til vurderingen skal skje,
c. tilbudene av bevishensyn om nødvendig snarest bekreftes skriftlig eller ved avsendelse av en bekreftet gjenpart og
d. tilbudene først åpnes etter utløpet av tilbudsfristen.
3) Tilbudet skal være undertegnet.

54 Ley 13/1995 de Contratos de las Administraciones Públicas.

55 Real Decreto 1098/2001 por el que se aprueba el Reglamento General de la Ley de Contratos de las Administraciones Públicas.

56 Article 45 of Act 30/1992 that regulates the legal regime of the public administrations and the standard administrative procedure, as developed by Royal Decree 263/1996 (Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común desarrollado por el Real Decreto 263/1996), Act 30/1992, Section 9, that regulates different fiscal, administrative and social order measures (Ley 30/1992, apartado 9, de medidas fiscales, administrativas y de orden social), Real decreto 722/1999 that regulates different communications with the public administrations.

57 Ley 59/2003 de Firma Electrónica.

fully applicable to the public administrations and their relations with citizens and enterprises. Additional guarantees can be, however, demanded when one of the parties involved is a public administration.

In Spain public administrations at regional level are developing different electronic public procurement projects. For example, the Basque Government is focusing its electronic public procurement strategy on the development of the so-called "e-Contratacion" project.[58] The Government of Catalonia created in 2001 the so-called "eCataleg",[59] that is the Catalonian Public Administration purchases portal build by SAP. The Government of the Canary Islands is developing an electronic public procurement project based on the platform PLYCA[60] build by Nexus IT. At the same time, private companies are offering sectorial solutions that can be used by different contracting authorities. For example, Saniline[61] offers a comprehensive electronic marketplace to all those contracting authorities dealing with supplies for the public health care sector. In all these cases, advanced electronic signatures play a main role in the security architecture of the respective systems, as demanded by the law both at national and EU levels. Official certification agencies play also an important role in these architectures.

5.3.7 Sweden

The Swedish Act (SFS 1992:1528) on Public Procurement (LOU), refers to the use of electronic signatures in the course of public procurement, although it does not specify any level of signatures. Chapter 1 Section 5 states

> Public contract: a written agreement entered into by a contracting entity regarding procurement in the meaning of this act and that is signed by the parties or signed by them with an electronic signature. [62]

According to the Swedish government, not requiring a certain type of electronic signature has the advantage that the law is more technological neutral and that the contracting authority is able to choose which type of electronic signature is required. Including a certain type of electronic signature in the law, e.g. demanding advanced electronic signatures, would result in less flexibility.[63]

The Swedish Agency for Public Management (Statskontoret) suggested already in 1999 that electronic signatures should be used for electronic

---

58 "https://www.ej-gv.net/n38a/N38Login.jsp?n38id=1571200790".

59 "http://www.ecataleg.cat365.net/Inici/".

60 "https://www.gobiernodecanarias.org/hacienda/apps/jsp/ovirtual.jsp?p=claemp&niv=1.1&r=B".

61 "http://www.saniline.com".

62 "Upphandlingskontrakt: skriftliga avtal som en upphandlande enhet ingår avseende upphandling enligt denna lag och som undertecknas av parterna eller signeras av dem med en elektronisk signatur." The Section was amended by Act 2002:594. For an English version of the Act *see* "http://www.nou.se/loueng.html".

63 *Formel - Formkrav och elektronisk kommunikation*, Departementsserien (Ds) Ds 2003:29, p. 55-56.

communication in the course of public procurement. It was recommended that the contracting authority should be able to choose which type of electronic signature it wants to utilize.[64]

It is unclear at this stage, if the wording of Recital (37) in the Public Sector Directive "advanced electronic signatures, should, as far as possible, be encouraged" will lead to adaptations in the Swedish law.

At present, open access solutions regarding the stage of contract establishment in electronic public procurement in Sweden are not available. Systems concerning contract management are, however, in use. The Swedish government established in 1998 a coordination function for public procurement, Statlig inköpssamordning (Government Procurement Coordination)[65], with the aim to coordinate 300 authorities organised directly under the government. To a large extent, public procurement in Sweden is carried out under framework agreements that link public authorities with suppliers. Framework agreements are based on pre-defined conditions and pricing policies and serve as the foundation for the Public Internet e-Procurement System, IHS, which public administrations can access via a dedicated portal[66] in order to purchase goods or services.[67]

5.4 Security and the Principle of Non-discrimination

When comparing the different national legislations and the Public Sector Directive, some differences are visible. Some countries require qualified electronic signatures in the course of electronic public procurement (Austria, Germany, Spain), some countries allow electronic signatures (Sweden) and some countries do not mention any electronic signatures as such (Denmark, Finland, Norway).

The following chart shows the use of security measures in several European countries.[68]

64 Report *Elektronisk upphandling under tröskelvärdena*, Statskontoret, 1999:39, p. 3.

65 Since 2003 Statlig inköpssamordning resides at Statskontoret (Swedish Agency for Public Management).

66 "http://www.avropa.nu/".

67 "http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=779&parent=chapter&preChapterID=0-140-196-197".

68 Public eProcurement - Initiatives and experiences, Borders and Enablers, *supra* note 40, at 17.

	Finland	*Norway*	*Denmark*	*UK*	*France*	*Italy*	*Germany*
Username and password	1	1	1	1	1	1	1
SSL	1	0	1	1	0	0	1
Smartcard	0	0	0	0	0	0	1
Firewall	1	1	1	1	1	1	1
Backup	1	1	1	1	1	1	1
Digital Certificates (PKI) User-level	1	0	0	1	0	0	1
Digital Certificates (PKI) Server-level	1	1	1	0	1	0	1
	85,71 %	57,14 %	71,43 %	71,43 %	57,14 %	42,86 %	100 %

This paper focuses on the contract establishment process within eProcurement, and issues of ordering or payment are not considered. Procedures involving the ordering or payment within public procurement after already established contracts might lead to the same or additional security aspects, e.g. secure payment methods, etc, but is outside the scope of this article.

Article 42.2 of the Public Sector Directive explicitly states that "the means of communication chosen must be generally available and thus not restrict economic operators access to the tendering procedure." Depending on whether certificates from one Certification Authority can be used for more than one application (e.g. tax declaration, tendering procedures, etc.) and/or if a certificate issued in one member state can be used in other member states, questions of non-discrimination and interoperability arise.

According to Article 4.2 of the Electronic Signature Directive electronic signatures that comply with the requirements of the Directive[69] should be able to circulate freely in the internal market. Depending on the interpretation of these requirements in the member states, especially if not homogenous, obstacles can arise. The Commission published references to standards in this context in 2003. These only concern Certification Authorities (Certification Service Providers) and secure signature-creation devices[70], which means that the referred standards focus on the requirements regarding qualified electronic signatures.[71] Standards and initiatives on a European level are therefore needed in order to enable the "promoted" free circulation of electronic signature devices and to guarantee that a qualified electronic signature created in one member state is technically verifiable in another.[72]

If the use of electronic signatures is required during a tender procedure, the principle of non-discrimination plays an important role, as it has to be ensured that also foreign vendors are able to participate and acquire the necessary certificates or are able to use the certificates issued in their own member state. The use of smart cards that store a digital signature and provide a higher level of

69 Annex I-IV of the Electronic Signature Directive.

70 Article 2.5 "signature-creation device" means configured software or hardware used to implement the signature-creation data" (signature-creation data can be codes or private cryptographic keys, *see* Article 2.4).

71 The Legal and Market Aspects of Electronic Signatures, *supra* note 12, p. 119.

72 The Legal and Market Aspects of Electronic Signatures, *supra* note 12, p. 154.

security might be an obstacle to the internal market due to different technical specifications of the smart card readers and the required software which increases the burden for suppliers to be able to bid in different members states. [73]

The question of recognition of signature certificates from another member state is also influenced by the fact that a Certification Authority on an Europan level is missing. Although, it can be argued whether such a supranational body is necessary, initiatives for standardisation should be developed on a EU level in order to ensure the functioning of the internal market. Examples of such developments include the European Electronic Signatures Standardization Initiative (EESSI)[74] and the previous TIE project (Trust Infrastructure for Europe)[75].

Several projects are currently developed in Europe that would enable Certification Authorities within the EU to certify each other. The European Commission is, for example, planning to develop a Bridge CA within the framework of IDA[76] for use between public administrations in Europe. Another example of such a project is the "European Bridge-CA" initiated by Deutsche Bank and Deutsche Telekom and supported by TeleTrust.[77] These initiatives could, on the long run, lead to a European network of Certification Authorities and thus facilitate the issuing of certificates throughout Europe.

In the context of security and electronic signatures interoperability should be mentioned as well, as technical components on the client side (digital certificates, authentication and connection devices) might require the installation of hardware and software.[78] This question will be dealt with in the following.

6 Interoperability

The above mentioned legal evaluation criteria of the Public Sector Directive also include interoperability.[79] In a strict technical sense interoperability involves the possibility to exchange data between different users, programmes or systems. This depends, inter alia, on the (operating) system, the type or version of the application, or the sort of document format utilized. From a procurement point of view, it is important, especially when establishing a pan-European network, to enable vendors from all member states to interact with the contracting authority, which entails the form of electronic communication used. Certain technologies might discriminate certain suppliers in their access to tendering procedures.

Article 42 .4 of the Public Sector Directive expressly states that

---

73 eProcurement Feasibility Study, *supra* note 14, p. 26.

74 "http://www.ictsb.org/EESSI_home.htm".

75 Funding Programme: ESPRIT 4 – Project Reference Number: EP 26763. *See also* The Legal and Market Aspects of Electronic Signatures, *supra* note 12, p. 121-123.

76 Interchange of Data between Administrations (http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=home), which will subsequently be replaced by IDABC, *see* note 81 below.

77 "http://www.bridge-ca.org"; The Legal and Market Aspects of Electronic Signatures, *supra* note 12, p. 125.

78 eProcurement Feasibility Study, *supra* note 14, p. 24.

79 eProcurement Feasibility Study, *supra* note 14, p. 15.

> The tools to be used for communicating by electronic means, as well as their technical characteristics, must be non-discriminatory, generally available and interoperable with the information and communication technology products in general use.

A Common Position by the Council from 2004[80] also underlines the importance of interoperability when it comes to interaction between public administrations and businesses across borders. Recital (14) emphasises the "availability of efficient, effective and interoperable information and communication systems between public administrations as well as interoperable administrative front and back office processes in order to exchange in a secure manner, understand and process public sector information across Europe." The goal is to establish a Programme for Interoperable Delivery of pan-European eGovernment Services to European Public Administrations, Community institutions and other entities and to European Businesses and Citizens ("IDABC programme").[81] One of the policy area affected by this programme is public procurement.[82]

Furthermore, a communication from the Commission on the Role of eGovernment for Europe's Future[83] emphasises the importance of interoperability and stresses the importance of identifying all "legislative and non-legislative measures required to eliminate obstacles to cross-border electronic public procurement and ensure interoperability of electronic procurements systems."

Lack of interoperability can lead to higher costs for both public and private entities, expensive public administration systems, and a competitive disadvantage for companies compared to local suppliers, which consequently results in obstacles for the proper functioning of the internal market.[84]

6.1 The Notion of Interoperability

From a technical point of view, interoperability can concern different aspects. First, electronic procurement platforms might require certain technical specification on the side of the supplier, e.g. a programme has to be downloaded which requires a certain operating system and therefore excludes all entities that do not have this operating system. Some platforms might be web based and therefore not demand any special software to be installed which results in more interoperability. Two other issues connected with interoperability concern the exchange of information during the procurement process and the use of security measures such as electronic signatures, which will be dealt with in the following.

---

80 Common Position (EC) No 12/2004 of 18 December 2003 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to adopting a decision of the European Parliament and of the Council on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC).

81 *Ibid* Article 1.

82 *Ibid* Annex I, Chapter A, Paragraph 12.

83 COM(2003) 567 final.

84 *Ibid*, p. 19.

Interoperability is, of course not only a technical question, but also has to do with the way public administration organise their procedures in-house and in connection with other national or European public authorities.[85] This paper will, however, focus on the technical issues in the following.

6.2 Document Exchange

In order to facilitate communication and exchange of information in electronic format, the use of a common language, simply put, is of great importance. The fact that a web portal for public procurement is in a certain language excludes all suppliers who do not understand this language. When speaking about automated transfer of documents, systems also have to be able to "understand" each other, to process the incoming data and insert it to the system. In this context the use of a common vocabulary, utilizing tools for structuring data and requesting a certain format of the incoming document play an important role.

Interoperability is guaranteed when using the same structure of documents as this enables automated transfer of data. One way to achieve this is the EDI/EDIFACT standard[86]; another possibility to structure information is the use of XML (eXtensible Markup Language). A European initiative is also combining both.[87]

The XML language requires an underlying document specifying the different types of data of the document, e.g. evrey document contains a field with the name of the supplier, address of the supplier, type of contracting authority, place of performance, estimated costs, etc. This base document can be either a DTD or a Schema.[88] The problem so far has been that different vendors introduced different DTDs, in other words, suppliers had developed their own DTDs, which consequently decreases interoperability. In order to solve this problem, a European-wide common standard should be introduced, such as the ebXML forum for example.[89]

In this context, another question arises. Who should be responsible for the development of standards, private companies due to the de facto high percentage usage of their applications or public entities by initiating projects and co-ordination groups that are able to implement a certain technical standard throughout the European Union? As an example the Directive on the use of standard forms in the publication of public contract notices could be mentioned.[90] Based on this Directive a standard XML format for the

85 *Ibid*, p. 19.

86 Electronic Data Interchange/Electronic Data Interchange For Administration, Commerce and Transport.

87 XML/EDI.

88 For more information on XML *see* "http://www.w3.org/XML/".

89 "http://www.ebxmlforum.org/". Transborder eProcurement Study, Border and Enabler, *supra* note 32, p. 60.

90 Commission Directive 2001/78/EC of 13 September 2001 (Directive on the use of standard forms in the publication of public contract notices).

transmission of notices has been developed by the Official Publication Office.[91] SIMAP[92] and TED[93] could play an important role in this process as well. Besides EU initiatives, national developments lead in the same direction, e.g. the eProcurement XML schemes in the UK, or Denmark, which recently adopted the Universal Business Language (UBL) as a standard for e-procurement in the public sector.[94]

Another obstacle to interoperability is the format of additional documents which can be handed in during the procurement process. Some e-procurement portals might only allow one certain format, e.g. .doc, whereas other national portals might allow additional ones, as .pdf or XML documents. One should be aware that this also could exclude vendors from participating in tenders.

6.3 Commodities Coding System

Given the large number of products that are to be procured by companies and public authorities, a method of identifying similar items is required. A common vocabulary enables vendors and suppliers to describe the items object of public contracts by means of classification systems. These systems assign codes to identify products, which helps a user when searching for a particular item in order to buy it (regardless of supplier) and, subsequently, in providing structure for Management Information (MI) reporting. These precise codes are incorporated into electronic and paper-based procurement documents such as web sites, product catalogues, invoices, purchase orders and inventory/sales slips. By applying standard codes to each product and service to be procured, it is possible to automatically and consistently track the entire procurement activity.

A commodity coding system should be designed to serve two primary functions from the procurement viewpoint:

1. Product sourcing: identification of relevant suppliers of a specific product or service.

2. Spend analysis: reporting on what products are being purchased to support budgeting and strategic procurement decisions.

In order to serve the first function, any system is acceptable. But in order to serve the second function, it is necessary that the coding system chosen allows for aggregation thanks to its hierarchical structure. And not all systems are able to serve this function.

---

91 Transborder eProcurement Study, Border and Enabler, *supra* note 40, p. 60.

92 Système d'Informations pour les Marchés Publics, *supra* note 6.

93 Tenders electronic daily, "http://ted.publications.eu.int/official/", *supra* note 5.

94 "http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&parent=whatsnew&documentID=2107".

There are different established commodity coding systems in the international market. Some of the more commonly used cross-industry commodity coding systems are described in table below.

Coding system		Description
CPV	Common Procurement Vocabulary	It is required for OJ/TED notices. Unique number system. Non-hierarchical. It does not allow for aggregation for financial reporting.
EAN	European Article Number	Most widely used. Used in conjunction with the Uniform Code Council to form the EAN/UCC product codes. EAN-129 provides a barcode application identifier. Unique number system. Non-hierarchical. It does not allow aggregation for financial reporting.
ISIC	International Standard Industry Classification	Non-hierarchical. Geared towards central economic statistical gathering of industry information.
NAICS	North American Industrial Classification System	Shallow hierarchical. Classification at supplier level, code not applied to the product itself. Widely used adopted standard in the US. Supplier-related application.
UN-SPSC	United Nations Standard Product and Services Code	Hierarchical, product classification provides opportunity for complex MI reporting. Widely used at present, although there are many different versions. Most consistently referred to code among e-Commerce systems providers, on the buy and supply sides.

The Common Procurement Vocabulary (CPV)[95] has been used for OJ notices following a European Commission recommendation since 1996. The CPV links certain numerical codes to certain subjects of contracts and is available in all official languages of the EU. It consists of a main vocabulary with around 8200 numerical codes and a supplementary vocabulary, which allows adding of information regarding the nature or destination of the goods. The European Commission issued in 2002 a Regulation on a Common Procurement Vocabulary (CPV), setting the nomenclature reference numbers.[96] Several eProcurement projects in the EU use the CPV, although divergences still arise

95 "http://www.simap.eu.int".

96 Regulation (EC) No 2195/2002 of the European Parliament and of the Council of 5 November 2002 on the Common Procurement Vocabulary (CPV), amended by Commission Regulation (EC) No 2151/2003 of 16 December 2003, "http://europa.eu.int/scadplus/leg/en/lvb/l22008.htm".

due to the fact that the standard is not detailed enough.[97] The new Public Sector Directive[98] mandate the use of CPV by contracting authorities in the Member States as the reference nomenclature for public contracts.

Procuring authorities in countries such as the UK and Sweden are at the same time promoting the use of UN-SPSC (the United Nations standard)[99] as the commodity coding structure for their e-Procurement requirement. This system provides with a hierarchical, product-centred classification that is much more suitable for Management Information reporting, procurement platform integration and statistical purposes.

This duality will demand the use of strict equivalence systems that might involve future problems regarding access to procurement opportunities offered by different Member States.

6.4 Level of Security and use of Electronic Signatures

The Transborder eProcurement study found that more than 100 e-Procurement initiatives existed in the different Member States.[100] As shown earlier, the level of security often varies between different projects, from a simple login with a password to qualified electronic signatures requiring a smart card device. In addition, the existence of national schemes for certificates might impose high costs and administrational burdens for suppliers planning to participate in tenders outside their own country. In this context security issues might represent obstacles for a pan European network.

Article 4.2 of the Electronic Signature Directive emphasises that electronic signature products that comply with the directive should be permitted to circulate freely within the internal market. Recital (5) further underlines that "[t]he interoperability of electronic signature products should be promoted."

Standards for interoperability of electronic signatures have been developed by ETSI[101] within the framework of EESSI.[102] Due to the rather late publishing of the standards by the EESSI in the Official Journal[103], however, several member states either developed their own technical specifications which can differ from other countries, or member states waited for the standards which lead to a lacking behind in introducing products or services connected to electronic signatures.[104] Further initiatives are, therefore, necessary to ensure a standardised use of electronic signatures within the European Union and a

97 Public eProcurement - Initiatives and experiences, Borders and Enablers, *supra* note 40, p. 11.

98 Recital 36 and Article 1.14 of the Public Sector Directive.

99 "http://www.un-spsc.net".

100 Public eProcurement - Initiatives and experiences, Borders and Enablers, *supra* note 40, 57.

101 European Telecommunications Standards Institute (ETSI)

102 The Legal and Market Aspects of Electronic Signatures, *supra* note 12, p. 13.

103 Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council.

104 The Legal and Market Aspects of Electronic Signatures, *supra* note 12, p. 126.

harmonised implementation of the Electronic Signature Directive in order to adhere to the principles of non-discrimination and equal treatment and to avoid obstacles for the internal market.

6.5 Interoperability and the Principle of Non-discrimination

As already mentioned, Article 42.4 of the Public Sector Directive expressly refers to interoperability and non-discrimination.[105] Article 3.7 of the Electronic Signature Directive allows Member States to demand additional requirements regarding the use of electronic signatures in the public sector. These requirements shall, however, be "objective, transparent, proportionate and non-discriminatory" and "may not constitute an obstacle to cross-border services for citizens."

Establishing national standards for communication and requesting electronic signature certificates issued in a certain member state results in discrimination based on nationality, as it excludes vendors from other member states from participating in call for tenders. In order to adhere to the principle of non-discrimination, public administrations have to ensure that vendors from all member states are able to bid in tendering procedures. This can be achieved by guaranteeing interoperability.

The main focus in this context should be on the development of common standards for the exchange of information. Standards should be introduced not only concerning exchange of documents during the tendering procedure, but also with regards to authentication and supplier identification.[106]

Initiatives on a European level will further contribute to interoperability. Besides the above-mentioned developments, the European Commission could be one of the driving forces behind standardisation of security and electronic signatures by publishing reference numbers of commonly recognised standards. An example could be the above-mentioned publication of standards by the Commission.[107]

7 Conclusion

The new public procurement EU Directives (Public Sector and Utilities) aim at the creation of a pan-EU public procurement environment. This pan-EU environment demands both legislative flexibility and legislative homogeneity from different viewpoints.

Legislative flexibility is demanded for three reasons. First of all, the inexistence of an ample set of precedents that could allow identifying and

105 "The tools to be used for communicating by electronic means (…) must be *non-discriminatory*, *generally available* and *interoperable* with the information and communication technology products in general use."

106 Transborder eProcurement Study, Border and Enabler, *supra* note 40, p. 70.

107 Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers, *supra* note 103.

regulating future new situations, as oppose to what happens in the field of electronic commerce for example. Secondly, the wide range of technological solutions in this field. Excessive rigidity would obstruct the use of new technological solutions and even the rejection of technologies considered as obsolete or inadequate in the future. And finally the need for multi-disciplinary professionals able to manage the complexities of the three fields in question: public procurement, electronic procurement and security. This multi-disciplinarity demands an open space of expertise not constrained by artificially erected legislative barriers.

On the other hand, legislative homogeneity is also demanded. There are several issues that affect electronic public procurement in that respect: the use of electronic signatures, interoperability and commodity coding for example.

The new EU public procurement Directives make reference to superior levels of security considering the nature of the activity involved and to the use of electronic signatures as regulated in the respective Directive. The heterogeneous implementation of said legislative framework within the borders of the EU could jeopardize the achievement of a truly pan-European public procurement market, with serious negative consequences in terms of competitiveness and common internal market and cost cutting policies that would affect the EU and its Member States. The same can be said of interoperability and commodity coding. In this sense a deeper analysis of all the aspects mentioned in this paper are of great importance.