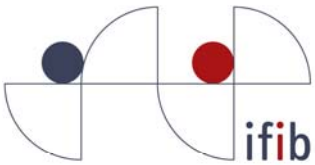
June 2009



Institut für
Informationsmanagement
Bremen GmbH

Electronic Signatures as Obstacle for Cross-Border E-Procurement in Europe

Lessons from the PROCURE-project

Ralf Cimander
Meik Hansen
Prof. Dr. Herbert Kubicek

Institut für Informationsmanagement Bremen GmbH (ifib)
Am Fallturm 1
28359 Bremen
{cimander; mhansen; kubicek}@ifib.de

ABSTRACT

E-procurement is considered one of the most promising services within e-government in terms of cost and time efficiency. Within the European Union, the Internal Market requires cross-border e-procurement. The European Council has issued directives and guidelines for this purpose. While e-procurement works on national levels, cross-border e-procurement in Europe does not. This is mainly due to lacking technical interoperability and legal harmonisation in particular concerning the use of e-signatures. By a comparative study of the different legal provisions in the Czech Republic, France, Germany, Spain and Sweden this article provides an overview of the current state-of-play and makes suggestions on how to overcome the remaining obstacles to pan-European e-procurement.

1. INTRODUCTION

In many national and international official papers and studies on electronic government, electronic procurement is seen as one of the most promising public electronic services in terms of cost and time efficiency[1]. However, while e-procurement systems work on national levels, cross-border e-procurement in Europe does not.

There is a general consensus that the reason for this is a lack of common legal requirements and technical interoperability. But while there have been many studies done on these subjects and several recommendations issued over the past ten years, it seems that either the analysis has not been specific enough to identify exactly what needs to be done, or that there hasn't been any implementation of the recommendations, or both. In particular, actions in the field of legislation and governance have only taken second place to those targeting technical interoperability.

In a market validation project for the European Commission (EC) within the eTEN programme, called PROCURE (see: www.eten-procure.com), an electronic procurement platform based on French legislation was to be transferred to various European regions. While the technical adaptation to the various regional requirements

could be achieved, it did not result in significant cross-border e-procurement among the regions. As such, it provided a meaningful and practical context in which to analyse the legal framework for the use of e-signatures in e-procurement and assess its role as an inhibitor for pan-European e-procurement.

This article starts with a brief definition of the main concepts and a review of the contents of the official (legal) documents and studies that relate to the use of e-signatures in e-procurement. Then, success-factors and barriers for their cross-border adoption are discussed from a legal point of view. Based on a comparison of the national profiles from Germany and the PROCURE pilot participants Czech Republic, France, Spain, and Sweden, recommendations for European legislation and individual measures to better align national regulations and the mutual recognition of electronic signatures in e-procurement among the Member States are made.

2. DEFINITION OF THE SUBJECT: LEGAL CONTEXT OF E-SIGNATURES IN E-PROCUREMENT ON EUROPEAN LEVEL

2.1 GENERAL DEFINITIONS

The term e-procurement is not well defined by the European directives and adhering legal documents. But the e-procurement community within the epractice.eu portal of the European Commission defines it as the use of electronic means in conducting a public procurement procedure for the purchase of goods, works or services by public authorities (eProcurement Community 2009). Just like public procurement in general, e-procurement can be grouped into different phases consisting of the internal assessment of demands, the tendering phase including the publication of notification, the awarding and contracting and the ordering phase including invoicing and payment (Coscia and Rubattino 2008).

This article focuses on the tendering phase and the contracting phase. The first one is crucial because it best achieves the objective of opening the Internal Market, as tenders have to be published widely across Europe. The second one deals with the most

relevant legal step, the signing of a contract. Conclusions for these two phases can be transferred to the other phases.

E-signatures play an important role in both phases and are regulated by European directives. A ‘directive‘, in general, is a legislative act of the European Union which requires Member States to achieve a particular result without mandating the means to achieve it in greater detail. This leaves a certain amount of leeway to the Member States when adopting the exact rules (Toth 1990: 177). The sovereignty of Member States is honored and diversity allowed, even though harmonisation of legislation and the agreement on standards is envisaged.

The harmonisation of legislation among European Member States is aimed at removing legal barriers for cross-border services. Technical barriers, in turn, are to be overcome by standardisation. Different systems which need to interchange data have to be interoperable, based on interoperability standards. Standardisation, as understood here, covers the technical, syntactic, semantic and organisational interoperability layers (Kubicek and Cimander 2009).

When adopted, directives give Member States a timetable for the implementation of the intended outcome. Occasionally the laws of a Member State may already comply with this outcome. But more commonly Member States are required to make changes to their national laws to correctly implement the directive.

Beside directives, there are supporting documents that accompany their implementation, set priorities or give other guidance to the Member States to interpret the regulations and objectives of the EC. Often such documents are so-called action plans or other official communications of the Commission to the Council. These documents however are not binding legislation. They aim to improve the situation, but do not confer any legal rights upon anyone.

2.2. E-PROCUREMENT AND E-SIGNATURES IN EUROPEAN LEGISLATION

European e-procurement is regulated by directives 2004/17/EC and 2004/18/EC and e-signatures by Directive 1999/93/EC. All 27 Member States have officially transposed these directives into their national laws and provide for electronic public procurement. Whereas the requirements for e-signatures in e-procurement are usually stated in the procurement laws of the countries, in most Member States particular e-signature laws exist for regulating e-signatures.

Generally, regulations of the European procurement directives concern those procurement procedures that have relevance for the European Internal Market. For all other procurement procedures, the Member States are free to set up their own regulations. Criteria are the value or particular importance for the Internal Market of the object that is to be tendered. The value thresholds are agreed upon by the European Commission and are adapted on a two-years basis (with the last adaptation as of 1 January 2008)[2].

The e-signature directive regulates three different types of electronic signatures with different degrees of authenticity: simple, advanced and qualified. Generally, the more mature a signature is, the more complex or intricate is its application, maintenance and operation, in particular for occasional users.

While the procurement directives allow for the use of e-signatures, they do not prescribe them (Art. 48(5) of Directive 2004/17/EC and Art. 42(5)b of Directive 2004/18/EC). I.e. Member States may decide whether tender documents have to be furnished with an electronic signature or not. If they do, it has to be at least of an advanced type (for definitions, see below).

One could assume that if Member States have transposed these directives into national law, cross-border e-procurement should be possible. However, this is not the case. As experienced within PROCURE and explained in detail below, e-procurement procedures with relevance for the Internal Market are still in most cases prevented by diverging national regulations. Vague formulations within the directives have led to

national differences in the technical infrastructures for e-signatures available in the EU today. These governance problems have often been overlooked by Community funded projects and studies, which have focussed overwhelmingly on technical-organisational aspects.

2.3. STANDARDISATION IN E-PROCUREMENT AND E-SIGNATURE IN EUROPE

In the area of e-procurement no binding standards for interoperable data exchange have been set on a European level yet. Also, the e-signature directive does not prescribe which technical solutions or standards shall be used in order to fulfil its legal requirements. Moreover, European standardisation is not under the authority of the European Commission. Rather it is delegated to the European Committee for Standardisation (CEN) and to the European Telecommunications Standards Institute (ETSI). To address e-signatures, the European Electronic Signature Standardisation Initiative (EESSI) has been founded by the European ICT Standards Board (ICTSB). EESSI is supported by CEN and ETSI as well as by the European Commission.

Many standards in the e-signature field have been issued in the form of CEN Workshop Agreements (CWA) or ETSI Technical Specifications (TS). Three of these standards have been referred to by Commission Decision 2003/511/EC[3]. Also, the ‘Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market’ (EC 2008) intends to amend Directive 199/93/EC with more standards by the second quarter of 2009 (p. 8).

Products manufactured according to these standards give a 'presumption of conformity' to the essential legal requirements in the directives but they are not ‘harmonised standards’ in the sense of being European Norms. Other standards may also be used, such as those made by many national standardisation organisations. Consequently, a wide range of non-legally binding national and European standards is available today[4]. This creates confusion among public authorities and certification-service-providers (CSPs) about which standards are best to be used in order to employ or offer e-signature products and services.

3. SUPPORT FOR THE IMPLEMENTATION OF DIRECTIVES BY THE EUROPEAN COMMISSION

The interoperability problems around the use of different types of electronic signatures have already been identified by the Commission's Action plan on e-procurement at the end of 2004 (EC 2004). Considering that there had been a specific study on legal and market aspects of e-signatures that clearly pointed to inconsistencies in the legal frameworks of the Member States and recommended clarifications of the e-signature directive by providing additional interpretation guidelines (Interdisciplinary Centre for Law & Information Technology 2003: 9-14), one should have expected concrete measures to address these problems.

But neither the i2010-Strategic Framework (EC 2005b), issued half a year later in 2005, which only laid out broad policy orientations, nor the guidance for conducting electronic procurement (EC 2005a) published by the Commission also in 2005 addressed the necessary legal and governance issues. The latter focussed again on technical aspects of interoperability of national e-procurement solutions, basing its recommendations on a hypothetically harmonised legal framework, which neither then existed nor does it today.

In 2006, the existing deficits in legislation for the choice of a certain e-signature type in e-procurement procedures were again addressed in a status report on implementation of the e-signature directive (EC 2006b). In 2007, a study by IDABC on 'eID Interoperability for PEGS' identified lacks in the European legal framework concerning the capability of an e-signature to unambiguously identify the signatory and the identity attributes to be entered in an e-signature certificate (Siemens - Time.lex 2007a: 196). Similar advice had been provided by the ELDOC Study (Interdisciplinary Centre for Law & Information Technology 2006) a year earlier, in which the use of e-signatures was also a side-topic.

Even though the Commission has often recognised that legal problems occur or *may* occur (EC 2005a: 14) these were never followed-up with the necessary insistence. This is true for the specific plans such as the Commission's 2007 'roadmaps' (HIS eGovernment ad hoc group 2006; EC 2007b; HIS Expert Group 2007b) to achieve

public e-procurement in at least seven member states by the end of 2010, when the i2010-Strategic Framework is scheduled to be implemented (EC 2005b), or political commitments on harmonisation and cross-border interoperability such as the Ministerial Declaration from the Lisbon eGovernment conference in 2007 (EU 2007).

Often reference is made only to the e-signature directive or to the general principles of non-discrimination, generally availability, proportionality and transparency as aspects of limitations that have to be considered. Member States are not committed to common legal rules and concrete instructions for e-procurement, in particular concerning the required level of e-signature security that is important to allow for legally binding e-procurement procedures.

Evidence to this assessment is once more provided by the recently published Commission's 'Action plan on e-signatures and e-identification to facilitate the provisions of cross-border public services in the Single Market' (EC 2008). This action plan underpins only the regulations already made in the e-signature and e-procurement directives and stresses the necessity of functioning cross-border e-signature recognition. But it does acknowledge that there is fragmentation in the legal framework and that problems on the technical interoperability layers currently limit the cross-border use of e-signatures. It is also recognised that – due to the generic definition of e-signatures in the e-signature directive – there is already a diversified field of solutions with different security levels based on different national (legal) concepts.

The 'Preliminary Study on Mutual Recognition of e-signatures for e-government applications' (Siemens - Time.lex 2007b) identifies among others, legal obstacles, in the types of signature required for a certain application, the required content of e-signature certificates and the interpretation of the e-signature directive's provisions for accreditation and supervision of CSPs and calls on the Member States and the application owners, not the EC, to clarify these issues. Likewise the 'Study on the standardisation aspects of eSignature' ascertains that the concept of electronic signatures with its different security levels seems not to be fully understood by

applicants and attributes this problem to the unclear wordings of the e-signature directive itself (Sealed 2007: 24).

A study on compliance verification in e-procurement prepared for the EC clearly states that ”the development and use of e-signatures lags someway behind the development of other aspects related to e-procurement, and in fact its use and implementation appears to be hindered in many countries by an inadequate legal base, which needs further definition before this feature can be employed“ (CARSA 2007: 23).

One reason which could explain why there is still no solution for cross-border aspects of e-procurement even though the problems have been identified again and again could be the methodology of many studies. For example, the ‘Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures’ (Siemens - Time.lex 2007c) and (Siemens - Time.lex 2007d) compiles valuable information on legal aspects of e-signature requirements in its country profiles. However, while assessing interoperability problems on a country-by-country basis for 27+ countries, cross-border aspects are not highlighted. For this, it would be necessary to describe the situation by cross-tabulating the compatibility of each country with each other country (e.g. 27x27).

Another intrinsic problem of country related studies is that these generally are prepared by respective national experts and hence strongly depend on the expertise of these surveyors. However, the expertises may vary as their authors not always work in the same lines of business or have different views on the same subject. This makes comparisons of the country profiles questionable.

While projects include practical research and development activities, studies survey a state of the art or provide conceptual recommendations. However, practical problems cannot be identified by such studies if there are no use-cases for the issues under investigation. To address this, the EC has funded a variety of practical implementation projects which can be found in the e-procurement community within the epractice.eu portal (Coscia and Rubattino 2008) and in an attachment to the ‘i2010 eGovernment

Action Plan' (EC 2007b). One of these has been the PROCURE-project which is at the centre of this article.

Most recently, the European Commission has endorsed a comparatively large approach to solving the practical interoperability problems in the form of the PEPPOL-project. PEPPOL (Pan-European Public eProcurement On-Line) is funded by the CIP program of the European Commission as a so-called large scale pilot. At least seven Member States have to participate, in PEPPOL there are eight so far, with an enlargement scheduled for 2009. Its goal is to set up a pan-European pilot solution that is based on the existing national solutions. Besides the technical and organisational issues also the legal and governance aspects are to be considered as concretised in the 'Guidelines to Common Specifications for Cross Border use of Public eProcurement' (HIS Expert Group 2007a).

At the time of writing this article, PEPPOL is just ending its specification phase. But judging from the results of the PROCURE project it seems to be the right way to create real use-cases on a European level in such or similar projects as in PEPPOL rather than trying to compare the varied legal aspects of 27 or more countries in a study without concrete practical foundation.

4. GENERAL ASPECTS OF ELECTRONIC SIGNATURES

When comparing the use of electronic signatures in e-procurement three issues are important: the different types of electronic signatures, the types of e-signature certificates, and the supervision and accreditation of the certification-service-providers (CSPs).

4.1 E-SIGNATURE TYPES

In accordance to Art. 2(1) of Directive 1999/93/EC the simple form of e-signature is just called 'electronic signature' and is defined as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication". This kind of electronic signature can be regarded as weak in terms of

reliability and security of authentication. It allows only the authentication of a claimed identity of an entity or user, but not the authentication of the real identity and data-origin. An alteration of a message (e.g. an e-mail) can happen unnoticed. Examples are a signature or photo in scanned format that is attached to an e-mail.

In contrast, an 'advanced electronic signature' in accordance to Art. 2(2) will uniquely identify and authenticate the signer of a message, and will allow to check the integrity of the signed data. Mostly, asymmetric cryptographic technologies, such as PKI and digital certificates, are used for advanced electronic signatures. The long term perennial characteristic of electronic signatures, also required for advanced electronic signatures, can be achieved with the input of a Trusted Third Party for time stamping and notarisation. This is important to proof that the signature was valid at the time of its creation (Certipost 2005: 8).

Beside the definition of 'simple electronic signatures' and 'advanced electronic signatures' Directive 1999/93/EC stipulates in its Art. 5(1) that Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation-device (SSCD) are to be recognised by them as legally fully valid signatures in electronic format with the same legal consequences as of a handwritten signature. This provision in effect creates a third type of electronic signature, the 'qualified electronic signature'. This type of e-signature is technically the same as an advanced signature, except for the use of a SSCD, but its quality is higher because the contents of the certificate, e.g. the information who the owner of the certificate is, is 'qualified' as explained in the next section.

4.2 E-SIGNATURE CERTIFICATES

A "'certificate' means an electronic attestation which links signature-verification data to a person and confirms the identity of that person" (Art. 2 (9) of Directive 1999/93/EC). The requirements for a qualified certificate are laid out by Annexes I and II of the Directive. According to Annex I, a qualified certificate must contain, among other things, the name

of the signatory or a pseudonym, the identification of the CSP and the State in which it is established and several attributes pertaining to the allowed uses of the certificate. Annex II stipulates a number of requirements for CSPs issuing qualified certificates, e.g. demonstration of reliability, operation of a prompt and secure directory and a secure and immediate revocation service.

Any certificate that does not meet the requirements of a 'qualified certificate' in terms of Directive 1999/93/EC is a simple certificate with limited liability and – for example – can not be a constitutional part of a qualified e-signature. On the other hand, advanced e-signatures can be issued with simple (non-qualified) or qualified certificates.

4.3 SUPERVISION AND ACCREDITATION OF CSPS

Pursuant to Art. 3 of Directive 1999/93/EC "each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public". Member States may decide how they ensure the supervision of compliance and have in most cases assigned this task to public supervision authorities on state level.

Besides mandatory supervision, Member States may introduce voluntary accreditation systems that aim at enhanced levels of certification service-provision. I.e. enhanced levels of trust, security, and quality can be set up to encourage the development of best practices among CSPs. These accreditation schemes must be "objective, transparent, proportionate and non-discriminatory" (Art. 3(2)) and should not reduce competition for certification services (Preamble 12).

The names and addresses of the bodies responsible for supervision and accreditation as well as of all accredited national CSPs have to be notified to the EC and the other Member States (Art. 11).

A sufficient security level for e-signatures is achieved by the mandatory supervision of CSPs. National accreditation, in turn, is not seen as an obligatory requirement by the Directive, even though its definition is acknowledged as a value. However, the practice

in many European countries shows that accreditation can hardly be seen as voluntary. Many national e-government programmes only accept accredited CSPs (Interdisciplinary Centre for Law & Information Technology 2003: 5).

5. REGULATION OF E-SIGNATURES IN VARIOUS COUNTRIES

A survey of the legal regulations of e-signatures in e-procurement carried out within the PROCURE project between the Czech Republic, France, Spain and Sweden - plus Germany - shows the different requirements for both the early tendering and the final contracting phases across Europe today.

5.1 CZECH REPUBLIC

The Czech Electronic Signatures Act (Act 227/2000 Coll.) defines electronic signatures and advanced electronic signatures in the same way as the European directive. Besides those it defines a third type called ‘electronic mark’, which is a kind of an advanced electronic signature that can be assigned to legal bodies to be used in an automated manner without human interaction. The Czech definitions of certificate types (simple and qualified) comply with the European specifications and are supplemented by a third one, the so called qualified system certificate, which is the basis for an electronic mark (Czech Electronic Signatures Act, Section 2).

Qualified e-signatures are not explicitly defined, but a higher level of e-signatures is known as ”based on a qualified certificate and created using a secure signature creation device” (Act 227/2000 Coll, Section 3 (2)). As these e-signatures enable the unambiguous identification of the signing person they are to be seen as the equivalent of a handwritten signature, even if the handwritten signature is not explicitly referred to in the act.

However, in section 11 a ’recognised electronic signature’ is defined. That is an advanced electronic signature based on a qualified certificate issued by an accredited CSP. This kind of e-signature is sufficient for the use in public administration. It, and also the electronic mark, too, become the equivalent of a handwritten signature even

though the use of a SSCD has been dropped. No case-law enforces the use of SSCDs, either.

CSPs that issue qualified certificates are supervised by the Ministry of Interior and can undergo an optional accreditation process. By April 2009, three CSPs are officially accredited (EC 2009).

According to Section 11 (1) of the Czech Electronic Signatures Act, in the *sphere of public authorities*, it shall only be possible to use advanced electronic signatures, based on qualified certificates issued by an accredited CSP. This accreditation can be granted by any European Member State. The public contracts act (137/2006) however, in its article on the use of electronic means in public procurement (Czech Public Contracts Act, Art. 149), also requires an advanced electronic signature and a qualified certificate, but does not explicitly demand for accreditation of CSPs. I.e. there are conflicting regulations concerning the requirement for accreditation.

Currently it is discussed in the Czech Republic whether public procurement belongs to the authority of general public administration (and hence would require the accreditation from CSPs) or is rather independent with its own domain specific regulation. The latter case is the preferred interpretation by the Czech Ministry of the Interior as this would be non-discriminating for economic operators in particular from abroad as they would be released from the requirement for accreditation.

No distinction is made in the Czech legislation for electronic signatures in the early tendering procedure and the final contracting phase. In both cases, contracting authorities as well as the bidders have to use legally compliant e-signatures.

5.2 FRANCE

The French Electronic Signatures Decree (Decree No 2001-272) defines two different e-signature types: electronic signatures and secure electronic signatures. Whereas the first is defined in the same way, the second type is defined differently as by the EC, but still corresponds to advanced electronic signatures (French Electronic Signatures

Decree, Art. 1). Qualified e-signatures are not explicitly defined, but a higher level of e-signatures is known (e.g. SSCDs are defined but not applied) (French Electronic Signatures Decree, Art. 3). Secure e-signatures used under certain conditions, fixed in the respective case-law, have the same value as handwritten signatures (French Civil Code, Art. 1316). The French definitions of certificate types (simple and qualified) are also the same as the European specifications (French Electronic Signatures Decree, Art. 1). CSPs that issue qualified certificates are supervised and can undergo an optional accreditation process.

By April 2009, there are 15 CSPs officially accredited by the French Ministry of Finance (Ministère de l'Économie de l'industrie et de l'emploi 2009).

The conditions for public electronic procurement are laid down in the French Public Contracts Act (Code des marchés publics), Articles 48-I, 56-I and 56-III, and are concretised by the Order of 28 August 2006. Its Article 1 and 2 stipulate that the contracting authority can offer consultation documents online. Article 4 allows economic operators to send bids and requests to participate in electronic form, if permitted by the contracting authority. According to Article 5 such documents shall be furnished with electronic signatures that must, in consideration of Article 6, be based on certificates issued by a CSP that has achieved accreditation by the French Ministry of Finance. This certificate must not be a qualified one. With respect to Article 81 of the Public Contracts Act, in order to close a contract in public e-procurement online, the economic operator only needs to sign the contract award notice.

In order to be legally compliant, signatures as specified in Article 6 of the French Public Contracts Act are required for the early tendering procedure and the final contracting phase by both the contracting authority as well as the bidders.

5.3 GERMANY

The German Electronic Signatures Act (SigG) defines simple electronic signatures, advanced electronic signatures and qualified electronic signatures. All three e-signature

types are defined in accordance with the European directive[5] and the German e-signature law also provides for simple (non-qualified) and qualified certificates. Only qualified electronic signatures are equal in law to handwritten signatures in Germany (German Administrative Procedures Act, § 3a; German Civil Code, Art. 126a).

German CSPs issuing qualified certificates are supervised and can undergo an optional accreditation process to get a quality distinction of the competent state authority (German Electronic Signatures Act, §15). The accreditation, though not obligatory, is also governed by a law. By April 2009 there are 12 CSPs whereof 9 are accredited (Bundesnetzagentur 2009).

According to the German contracting rules for the public sector all electronic tenders and requests to participate must be furnished with an advanced or qualified electronic signature (German Public Contracting Rules: VOB/A , §21), i.e. advanced electronic signatures constitute the minimal requirements for the early tendering phase. For the final contracting qualified electronic signatures are needed, because this kind of contract regularly demands for contracting in written form.

5.4 SPAIN

The Spanish Electronic Signatures Act (Act 59/2003) defines three different e-signature types: ordinary electronic signatures, advanced electronic signatures, and recognised electronic signatures. The first two types are defined in the same way as by the European directive. The third type corresponds to qualified electronic signatures with regard to the regulations of Directive 1999/93/EC and has the same probative value as a handwritten signature (Spanish Electronic Signatures Act, Art. 3). The definitions of certificates and qualified certificates are nearly the same as the European specifications (Spanish Electronic Signatures Act, Art. 6 & 11), but stipulate that the national identity number (or a unique pseudonym) for natural persons and the national tax identification code for legal persons must be used in the certificates in order to identify the signatory.

Spanish CSPs issuing qualified certificates are supervised and there are legal options for voluntary accreditation services (Spanish Electronic Signatures Act, Art. 26). These regulations can be concretised or extended by provisions of the Spanish autonomous regions with the necessary legal competences (Smits 2005: 10). In order to overcome diversity due to different regional provisions, Spain has implemented a multi-PKI validation platform (ePractice 2009b) that checks the electronic identity of a citizen or legal person independently of the involved CSP.

Besides the regional departments that issue eIDs such as CatCert in Catalonia or the Valencia region's CSP that also include e-signature functionality, by April 2009, there are 18 commercial CSPs (Ministerio de Industria Turismo y Comercio 2009). The CSPs that issue certificates for economic operators may be prioritised in accordance to the clients they provide with certification services, such as CAMERFIRMA of the Chamber of Commerce or FIRMAPROFESSIONAL for legal representatives of companies.

There is no distinction between the early tendering procedure and the final contracting as only recognised e-signatures by all involved parties are accepted according to the 19th additional adjustment of the Public Contracts Act. Thus, the minimal requirements of e-signatures in e-procurement in Spain are actually the highest possible: qualified e-signatures for all procedure steps with accreditation of CSPs as regulated on regional level for some regions.

5.5 SWEDEN

The Swedish Qualified Electronic Signatures Act (SFS 2000:832) defines simple electronic signatures, advanced electronic signatures, and qualified electronic signatures. The first type extends the European concept of electronic signatures with the demand for integrity. I.e. even simple electronic signatures must verify that the signed data has not been altered. The last two types are defined in the same way as by the European directive and qualified electronic signatures are deemed to be equal to handwritten signatures (Swedish Qualified Electronic Signatures Act, § 17). The

definitions of certificates and qualified certificates are also the same as the European specifications (Swedish Qualified Electronic Signatures Act, § 2).

Swedish CSPs issuing qualified certificates are supervised; the option of accreditation is not provided by the Swedish legislation.

By April 2009, there is one supervised CSP (Swedish Post and Telecom 2009).

On 1 January 2008, the new act on public procurement (SFS 2007:1091) came into force, implementing the European procurement directive 2004/18/EC but leaving out many of its optional regulations. The new act allows complete electronic processes, including the contract conclusion. Contracting authorities may require the use of advanced electronic signatures for the early tendering phase, but there are no regulations that enforce their use, so that electronic tendering is also possible without any signature. Only for the conclusion of the final contract both parties have to use qualified electronic signatures for electronic documents. Thus, at the beginning of 2009, the Swedish minimal requirements for e-signatures in e-procurement are actually the lowest possible as no electronic signature is needed for the early tendering procedure.

5.6 CROSS-TABULATION OF CROSS-BORDER FEASIBILITY

The following tables compare the legal requirements on e-signature use of contracting authorities of the respective Member State (x-axis) with the e-signature facility on hand of the bidder in accordance to its respective applicable law (y-axis). The cross-tabulation considers that the bidder has an e-signature created in its home country in accordance to its applicable law and not an e-signature created in the Member State where the contracting authority is located or from a CSP that is accredited in that Member State.

5.6.1 Cross-Border Feasibility for Early Tendering

In accordance to European legislation, Member States are free to demand for the use of electronic signatures in the early tendering phase. If e-signatures are used, they have to be at least in the form of an advanced e-signature.

Contr. authority in… recognises bid from…	**CZ**	**FR**	**GE**	**ES**	**SE**
CZ		NO[1]	YES	NO[2]	YES
FR	YES[4]		YES	NO[2]	YES
GE	YES[4]	NO[1]		NO[2,3]	YES
ES	YES	NO[1]	YES		YES
SE	YES[4]	NO[1]	YES	NO[2,3]	

Table 1 : Cross-Border Feasibility for Early Tendering

[1]: FR - CZ/GE/ES/SE: contracting authority from FR can only recognise e-sig. from bidders that have an e-sig. from a CSP accredited in FR.

[2]: ES - CZ/FR/GE/SE: contracting authority from ES can only recognise qual. e-sig.

[3]: ES - GE/SE: e-sig. certificates need to contain a unique national person identifier that is not provided by GE/SE laws.

[4]: CZ - FR/GE/SE: in case bidder uses advanced e-sig. based on a qualified certificate.

5.6.2 Cross-Border Feasibility for Final Contracting

In accordance to European legislation, the qualified e-signature is needed for liable cross-border contracting.

Contr. authority in… closes contract with bidder from…	**CZ**	**FR**	**GE**	**ES**	**SE**
CZ		NO[1,2]	NO[3]	NO[3]	NO[3]
FR	YES[4]		NO[5]	NO[5]	NO[5]
GE	YES[6]	NO[1,2]		NO[7]	YES
ES	YES[6]	NO[1,2]	YES		YES
SE	NO[8]	NO[1,2]	YES	NO[7]	

Table 2 : Cross-Border Feasibility for Final Contracting

[1]: FR - CZ/GE/ES/SE: contracting authority from FR can only recognise e-sig. from bidders that have an e-sig. from a CSP accredited in FR. Equivalent to handwritten signature is differently defined in FR.

[2]: FR - CZ/GE/ES/SE: in FR, the qual. e-sig. is not defined as the equivalent to the handwritten signature.

[3]: GE/ES/SE - CZ: equivalent to handwritten signature is differently defined in CZ so that CZ bidder has no qual. e-sig. in place due to the missing definition of SSCDs.

[4]: CZ - FR: in case bidder uses advanced e-sig. based on a qualified certificate. However, the CZ requirements for the equivalent to the handwritten signature are not conform to the European legislation.

[5]: FR - GE/ES/SE: equivalent to handwritten signature is differently defined in FR so that in practice FR bidder has no qual. e-sig. in place. But contracting authorities from GE/ES/SE can only recognise qual. e-sig.

[6]: CZ - GE/ES: in case bidder uses e-sig. issued by an accredited CSP.

[7]: FR - ES: e-sig. certificates need to contain a unique national person identifier that is not provided by GE/SE laws.

[8]: CZ - SE: SE does not provide for accreditation of CSPs. But contracting authorities in CZ can only recognise e-sig. from accredited CSPs.

6. RELEVANT DIFFERENCES AND POSSIBLE EXPLANATIONS OF DIFFERENT ELECTRONIC SIGNATURE REGULATIONS

Apart from significantly being different, the Member States' regulations on electronic signatures in e-procurement do not seem to fully meet the conditions set out by the procurement and signature directives. In clear violation of Art. 3(7) – the public sector clause – of Directive 1999/93/EC, at least three additional requirements enacted by certain Member States are an obstacle for cross-border e-procurement:

a) Conflicting requirements regarding the type of electronic signatures allowed. Member States determine in their national laws whether or not and which type of electronic signature may or has to be used. Art. 5(2) of the e-signature directive specifies that Member States should not discriminate against electronic signatures of a non-qualified nature, as Spain does by demanding qualified signatures in the early tendering phase.

   In the contracting phase, the procurement directives demand for advanced e-signatures and stipulate, that only qualified e-signatures generally satisfy legal equivalency to handwritten signatures. The Czech and French provisions for e-signatures violate these principles. The Czech's omission of the SSCDs prevents their qualified certificates of accredited CSPs from having legal effect in a pan-European context. The French regulations even allow the use of non-qualified e-signature certificates. The results in France are missing functionalities for qualified signing due to the missing SSCDs and a lack of technical and organisational infrastructures for dealing with qualified signatures coming from abroad.

b) The requirements for accreditation: France compensates its comparatively low requirements of the type of e-signature (advanced) and e-certificate (non-qualified) by prescribing a specific procedure for accreditation of CSPs following French legislation, technical standards and regular practice. Below the European thresholds, the validity of electronic signatures is checked at the awarding stage the earliest. Hence, there are comfortable procedures for French CSPs, whereas participation of foreign actors is impeded.

   In the Czech Republic, there is currently no clear interpretation what need there is for accreditation. Following the Ministry of the Interior's view, it would not matter in which Member State accreditation has been provided to the CSP, completely opposite to France. In Spain, there could also be different regulations for accreditation by the regional authorities.

   Moreover, accreditation may also be interpreted as a kind of discrimination itself, at least towards those Member States who don't have an accreditation scheme in place. As there are mandatory requirements for CSPs issuing qualified certificates (as defined by Annex II of Directive 1999/93/EC) and as these CSPs have to be supervised by Member States, an equal level of trust in CSPs in Europe can be achieved without accreditation. Accreditation would only be a plus.

c) The requirement for unequivocal identification of the signatory in form of unique national specific person identifiers. The Member States have interpreted Art. 2 (1, 2b, 9) of the e-signature directive, which calls for the assurance of the identity of the signatory, differently. Some countries demand unique national person identifiers in qualified certificates (like Spain) and some do not (like Germany and Sweden). This obviously splits the 27 Member States in two groups and creates significant barriers for cross-border use. While it could be argued that some Member States have not really implemented the unequivocal identity in their national definitions[6], it is not clear whether the requirement for a unique national identifier is non-discriminating to other Member States that do not have such an identifier in their country in general.

These variations in the use of electronic signatures are exemplarily for the overall situation in the EU (EC 2007a; ePractice 2009a). One cause for this is the absence of a requirement for qualified e-signatures in the procurement directives to enable electronic contracting. Another reason might be the current lack of practical relevance of cross-border e-procurement in the public sector. This lack is caused by the traditional procurement behaviour of the Member States focussing both on their specific local markets and the use of paper. Protectionist policies of Member States to safeguard their own national economic market could be an underlying principle why legislations are still – ten years after enactment of the e-signature directive – not harmonised. Presumably, no concerted initiative to bring along legal harmonisation will be started from the Member States themselves. Another factor might be the current absence of economic relevance of electronic signatures for multi-national operating companies; who, otherwise, would lobby harder for harmonised e-signature legislation if the benefits are substantial.

Unless Member States change their legislations and current practices, the ambitious objectives of the EC of 100% electronic availability and 50% real use of e-procurement by 2010 will fail (EC 2006a: 8). The EC already started with common regulations for the mandatory electronic announcements of tenders via SIMAP (EU Publications Office 2009a) and TED (EU Publications Office 2009b). But this is not enough. Combined actions by the EC and the Member States are needed to leverage the full potential of e-procurement on European level.

7. SOLUTIONS TO OVERCOME DIVERSITY

Projects like PROCURE or PEPPOL allow the demonstration of technical solutions but are severely constrained by inconsistent legislation. Their dilemma is that they have to begin operation under adverse and non-conducive legal frameworks. But they may not have the resources to change them. The PROCURE project tried to negotiate a workaround in form of an agreement on the mutual recognition of electronic signatures to be signed by all parties involved in this particular project. While this was in line with

the action plan on e-procurement of the European Commission (EC 2004: 6), the plan failed as most national legislations do not allow for (formal or informal) exceptions, not even for testing purposes. The Catalonian partners in PROCURE, for example, were not allowed to recognise French and Czech advanced e-signatures. Only the French could suspend their need for national accreditation, but only for the duration of the pilot phase.

Based on these findings it seems that only measures at the European level will enable cross-border e-procurement procedures. Also, immediate action is needed because every new application, which does not conform to the hypothetical standardised procedure for the use of European e-signatures in e-procurement, will cause adaptation work in the future and hence costs and troubles.

Currently, in the framework of the i2010 eGovernment Action Plan (EC 2006a), the European Commission and the Member States have started to review their e-procurement related legislation (EC 2005b). Also, the PEPPOL large-scale pilot will certainly provide solutions for technical issues of interoperability. But this technical system can only become successful within a 'Network of Trust', in which partners recognise by formal agreement e-signatures issued and validated by others and accept existing differences. This in turn requires legal adaptation in several Member States.

There is a strong interdependence of the following three elements when it comes to building an effective and sustainable solution:

- mutual recognition by use of a functional validation service,
- bridging diversity by a 'Network of Trust', and
- smart change of legislation.

It is crucial that these and their dependency on each other will be recognised by the Commission in its recently initiated review processes.

7.1 MUTUAL RECOGNITION BY USE OF A FUNCTIONAL VALIDATION SERVICE

To achieve technical, syntactic, semantic and organisational interoperability, mutual recognition of electronic signatures could be assured by a functional validation platform. Such a platform has to validate the authenticity and integrity of the e-signature certificate, interpret its content correctly, verify the electronic signature and warrant the authenticity and integrity of the overall validation procedure. The feasibility of this on a national level has been proven by the successful operation of the Spanish multi-PKI validation service. However, creating such a platform on the European level constitutes a huge organisational challenge and determining reliable common semantics is difficult. Also, it might violate Art. 4 of the e-signature directive[7]. Considering the non-transparent field of standards and formats of e-signatures available and in operation today, the maintenance and operation of a PKI validation platform would be less complex if a limited set of standards would be recommended by the Commission. This recommendation process has been started with Commission Decision 2003/511/EC in 2003 and should indeed be amended further as planned in the respective action plan.

With studying the feasibility of a federated validation service, the EC already pursues the policy of managing the technical aspects of interoperability by use of a PKI validation platform whereby the results of the feasibility study should feed into the PEPPOL project (EC 2008: 9-10). PEPPOL takes up existing systems in operation, which include the validation of electronic signatures, such as RASP in Denmark or OSCI in Germany, and makes them interoperable on a European level by creating an architecture which allows web-services to be implemented in a cross-national context between these existing technical solutions in Member States. This seems to be an appropriate approach if the action plan is followed. However, it can only be part of the solution and needs to be accompanied by further action.

7.2 BRIDGING DIVERSITY BY TRUST

Differences in e-signatures that are not founded on technical aspects but on divergent legislations can’t be bridged by the technical means of a validation service. Currently,

the Expert Group following the Services Directive pursues to "compile a 'Trusted List of Supervised Qualified Certification Service Providers' at European level. This list will centralise all the required information on existing and supervised qualified certification service providers in order to facilitate the validation process of e-signatures based on qualified certificates" (EC 2008: 8). The trusted list, forming a so-called 'Network of Trust' together with the validation platform, is supposed to finally create mutual trust, so that Member States acknowledge an e-signature, created and recognised in another Member State, as equal to its own requirements in terms of validity and security. This work has to cover the innumerable and variable number of actors (CSPs) in the 27 Member States. Such a 'Network of Trust' - however - does not relieve the Member States of adapting their legislation in case their laws actually do not allow for the recognition of e-signatures that are different from their own ones. Contracting authorities within such networks are bound to their national rules and can not opt out. Hence, Member States should at least amend their legislation with a legal clause enabling contracting authorities the mutual recognition.

7.3 SMART CHANGE OF LEGISLATION

The adaptation of the legislation needed to support mutual recognition by validation services and trust, which would then help the transformation of government procurement from traditional means to electronic cross-border procurement, should consider two interlinked steps:

- forceful elimination of discrimination of Member States' laws and
- balancing the required level of e-signature.

7.3.1 Forceful Elimination of Discrimination of Member States' Laws

The evaluation has shown that Member States have interpreted directives differently and that each Member State itself considers its own legislation as in coherence to the European regulations. Even if the national legislation for e-procurement, generally speaking, is considered to be coherent to the European legislation, due to the different

interpretations of certain rules (e.g. the 'public sector clause' (Art. 3(7) of Directive 1999/93EC)) barriers for cross-border e-procurement have been created. The Commission should systematically identify this discrimination and forcefully push for their elimination by the respective Member State. A most prominent barrier concerns the provisions for the accreditation of CSPs in some Member States, such as in France. Accreditation should be accepted regardless of the place of accreditation.

Another important barrier observed in the surveyed countries concerns the composition of e-signature certificates. Despite the detailed list in Annex I of the e-signature directive, the European legislation leaves room for interpretations of e-signature certificate requirements. As a consequence, Member States have dealt differently with names, pseudonyms and additional attributes of the signatory. Some, such as Spain, require unique national identifiers to be included in the qualified e-signature certificate. Others do not have such a unique identifier at all. Considering also other examples, such as the registration of companies across borders case between Estonia, Portugal and other countries[8], Europe runs the risk of being split up into two groups: countries requiring unique identifiers and those who do not. Obviously, it needs also to be clarified by the Commission whether the use of unique national identifiers is an infringement of the non-discrimination principle towards those countries that do not have such identifiers or where data protection legislations prohibit their use. To counteract this particular development, and to ease the use of e-procurement and other electronic services, for example those called for by Art. 8 of the Services Directive (2006/123/EC), the EC and the Member States should re-consider if their required levels of e-signatures are always necessary.

7.3.2 Balancing of the Required Level of E-Signature

The differences between the kinds of e-signature required come from security considerations and general considerations of which kind of electronic signatures can be equal to handwritten signatures. While there are controversial positions concerning the whole e-procurement process, a compromise seems to be achievable when different

requirements and risk assessments are taken into account for different phases. In the early tendering phase the objective is to receive as many bids as possible. For this purpose barriers should be as low as possible. If signatures are required at all, advanced e-signatures should be sufficiently safe. In contrast, in the final contracting phase where handwritten signatures are normally required, qualified electronic signatures should be regarded as equivalent.

This solution which is already possible in Sweden and Germany could open up cross-border bidding, as advanced electronic signatures are more readily available than qualified e-signatures in Europe. Following this approach, the major part of e-procurement procedures could be dealt with. Thus, the EC and the Member States should balance the required level of electronic signatures for the respective process phases, also considering the resulting reduction of administrative burden in this case as well.

This two-phase approach, with the lower security level in the early tendering phase and the higher level in the final contracting phase, could be considered as a role-model also for many other pan-European e-government services and should be focussed upon more by the European Commission and the Member States.

Such a change of legislation will not be initiated by the Member States alone, but has to be pushed for by the Commission, and possibly even harder than in previous attempts. Because without such a legal harmonisation, the technical validation platforms and the ‘Networks of Trust’ can not be used for cross-border e-procurement between all Member States. This is not just a hypothesis but an experience already made on a small scale in the PROCURE project and the most important lesson to be learned from this exercise.

REFERENCES

Bundesnetzagentur (2009) 'Zertifizierungsdiensteanbieter' (consulted Mar. 2009): http://www.bundesnetzagentur.de/enid/Qualifizierte_elektronische_Signatur/Zertifizierungsdiensteanbieter_ph.html

Bundesrat (1996) 'Drucksache 966/2/96; 20.12.1996'.

Bundestag (1997) 'Deutscher Bundestag, 13. Wahlperiode: Drucksache 13/7385; 9.04.1997'.

CARSA (2007) 'Compliance Verification of Electronic Public Procurement. Final Report. Prepared for the European Commission, DG Internal Market and Services'. Brussels.

Castrillejo, E. (2008) 'European eProcurement: an overview. Prepared for the European Commission, DG Enterprise and Industry'. Brussels.

Certipost (2005) 'Recommendations for creation & verification of signatures and for authentication processes, EBGCA-DEL-020, v 03.doc.'

Coscia, E. and C. Rubattino (2008) 'eProcurement map' (consulted Mar. 2009): http://www.epractice.eu/document/5328

EC (2004) 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Action plan for the implementation of the legal framework for electronic public procurement'.

EC (2005a) 'Commission Staff Working Document - Requirements for conducting public procurement using electronic means under the new public procurement Directives 2004/18/EC and 2004/17/EC. SEC(2005) 959; Brussels'.

EC (2005b) 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions (2005): i2010 - A European Information Society for growth and employment; SEC(2005) 717; Brussels, COM(2005) 229 final'.

EC (2006a) 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions (2005): i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All; SEC(2006) 511; Brussels, 25.04.2006 COM(2006) 173 final.'

EC (2006b) 'Report from the Commission to the European Parliament and the Council - Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures COM(2006) 120 final.'

EC (2007a) 'EC eSignature Workshop, Brussels, 12.12.2007' (consulted Mar. 2009): http://www.epractice.eu/document/4135

EC (2007b) 'Information sources relevant for the definition of Common Specifications for cross-border use of Public eProcurement. i2010 eGovernment Action Plan. High Impact Services. Version 1.0'. Brussels, DG Information Society.

EC (2008) 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions'. Action plan on e-signatures and e-identification to facilitate the provisions of cross-border public services in the Single Market. Brussels.

EC (2009) 'Electronic Signature Notification of the Czech Republic' (consulted Mar. 2009): http://ec.europa.eu/information_society/eeurope/2005/all_about/security/esignatures/index_en.htm#Czech

ePractice (2009a) 'Eurochambers' Conference on Cross Border use of eSignatures in eProcurement Processes, Brussels, 18.09.2009' (consulted Mar. 2009): http://www.epractice.eu/document/4958

ePractice (2009b) 'The Spanish Multi-PKI Validation Platform' (consulted Mar. 2009): http://www.epractice.eu/cases/1984

eProcurement Community (2009) 'The Public Electronic Procurement (eProcurement) and related topics' (consulted Mar. 2009): http://www.epractice.eu/community/eprocurement/guide_page/page2/

EU (2007) 'Ministerial Declaration of 4th Ministerial eGovernment Conference, approved unanimously in Lisbon, Portugal on 19 September 2007.'

EU Publications Office (2009a) 'Gateway to European public procurement - information and tools' (consulted Mar. 2009): http://simap.europa.eu/index_en.html

EU Publications Office (2009b) 'Tenders Electronic Daily' (consulted Mar. 2009): http://ted.europa.eu/

HIS eGovernment ad hoc group (2006) 'High Impact Services eGovernment ad hoc group and European Commission DG Information Society and Media eGovernment Unit: A roadmap for public eProcurement for the Implementation of the eGovernment Action Plan in support of the eProcurement Action Plan, draft 1.8'. Brussels.

HIS Expert Group (2007a) 'Expert Group for High Impact Services for the European Commission DG INFSO-CIP ICT PSP: Guidelines to Common Specifications for Cross Border use of Public eProcurement'. Brussels.

HIS Expert Group (2007b) 'High Impact Services Expert Group: Public eProcurement Detailed Roadmap'. Brussels.

Hühnlein, D. and Y. Knosowski (2003) Aspekte der 'Massensignatur'. Tagungsband 'D A CH Security'. P. Horster, IT-Verlag: 293-307.

Interdisciplinary Centre for Law & Information Technology (2003) 'The Legal and Market Aspects of Electronic Signatures. Prepared for the European Commission, DG Information Society.' Catholic University Leuven.

Interdisciplinary Centre for Law & Information Technology (2006) 'Legal study on legal and administrative practices regarding the validity and mutual recognition of electronic documents (ELDOC); D3.4 - First Interim report (country reports). Study prepared for the European Commission, DG Enterprise and Industry.' Catholic University Leuven and Lawfort.

Kubicek, H. and R. Cimander (2009) 'Three dimensions of organizational interoperability. Insights from recent studies for improving interoperability frameworks' European Journal of ePractice 6(Key enablers for eTransformation? eID, Interoperability and Open Source).

Ministère de l'Économie de l'industrie et de l'emploi (2009) 'Prestataire de service de certification électronique (PSCE)' (consulted Mar. 2009): http://www.telecom.gouv.fr/rubriques-menu/entreprises-economie-numerique/certificats-references-pris-v1/categories-familles-certificats-references-pris-v-1-506.html

Ministerio de Industria Turismo y Comercio (2009) 'Prestadores de servicios de certificatión de firma electrónica' (consulted Mar. 2009): http://www11.mityc.es/prestadores/busquedaPrestadores.jsp

Sealed (2007) 'Study on the standardisation aspects of eSignature. Prepared for the European Commission, DG Information Society and Media. Final Report, Brussels.'

Siemens - Time.lex (2007a) 'eID Interoperability for PEGS (Pan-European e-Government Services): Analysis and Assessment of similarities and differences - Impact on eID interoperability. Prepared for the IDABC programme. European Communities.'

Siemens - Time.lex (2007b) 'Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications. Prepared for the IDABC programme. European Communities'.

Siemens - Time.lex (2007c) 'Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures. Report on comparison and assessment of eID management solutions interoperability. National Country

Profiles. Prepared for the European Commission, DG Internal Market and Services, Brussels.'

Siemens - Time.lex (2007d) 'Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures. Strategy and implementation roadmaps. Final report. Prepared for the European Commission, DG Internal Market and Services, Brussels.'

Smits, J. (2005) 'Diversity of Contract Law and the European Internal Market. MPRA Paper No. 8192.'

Swedish Post and Telecom (2009) 'List of Accredited CSPs' (consulted Mar. 2009): http://www.pts.se/sv/Bransch/Internet/Elektroniska-signaturer/

Toth, A. G. (1990) The Oxford Encyclopaedia of European Community Law. Oxford.

STATUTES AND LEGAL DOCUMENTS

'Commission Decision 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. L 175/45. Official Journal of the European Communities, Brussels, 15.07.2003.'

'Czech Electronic Signatures Act 227/2000 Coll.'

'Czech Public Contracts Act No. 137/2006 Coll.'

'Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. L 13/12. Official Journal of the European Communities, Brussels, 19.01.2000.'

'Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors. L 134/1. Official Journal of the European Union, Brussels, 30.4.2004.'

'Directive 2004/18/EC or the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts. L 134/114. Official Journal of the European Union, Brussels, 30.4.2004.'

'Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. L 376/36. Official Journal of the European Union, Brussels, 27.12.2006.'

'French Civil Code'.

'French Electronic Signatures Decree No 2001-272'.

'French Public Contracts Act'.

'German Administrative Procedures Act VwVfG'.

'German Civil Code BGB'.

'German Contracting Rules for the Award of Public Contracts VOB/A, VOL/A, VOF'.

'German Electronic Signatures Act SigG'.

'Spanish Electronic Signatures Act 59/2003'.

'Spanish Public Contracts Act 30/2007'.

'Swedish Public Procurement Act SFS 2007:1091 '.

'Swedish Qualified Electronic Signatures Act SFS 2000:832'.

NOTES

We would like to thank Martin Hagen for reading earlier drafts of this article and for his sound advice. Information on the PROCURE project and any related deliverable can be obtained from www.eten-procure.com.

1 In accordance to the EC e-procurement action plan, assumed are savings of up to 5% on expenditure for governments and up to 50-80% on transaction costs for both buyers and suppliers (EC 2004). With reference to Castrillejo (2008) public procurement is acknowledged as a key sector of the EU economy accounting for about 16% of GDP. By 2010 50% of all procedures shall be dealt with electronically. According to the Expert Group for High Impact Services for the EC (2007a) it is assumed that public authorities purchase for 15-20% of the GDP or 1500-2000 billion euro per year and consequently e-procurement has been commonly recognised as one of the high-impact services to be provided by European governments, with a significant savings potential.

2 For details see Directive 2004/17/EC, Art. 16, Directive 2004/18/EC, Art. 7 and Directive 1422/2007.

3 Directive 1999/93/EC, Art. 3(5) states that generally recognised standards for e-signature products may be published by the EC. Commission Decision 2003/511/EC has done so by indicating three CWAs: 14167-1 and /-2 on security requirements for trustworthy systems managing certificates for electronic signatures (Part 1: System Security Requirements; Part 2: cryptographic module for CSP signing operations - Protection Profile) and 14169 on secure signature-creation devices.

4 A fair overview of EU standardisation work is provided by the Study on the standardisation aspects of eSignature. (Sealed 2007: 33).

5 The German e-signature legislation also provides for the automated creation of e-signatures equivalent to the electronic mark as defined by the Czech legislation cp. (Hühnlein and Knosowski 2003: 293-307).

6 This shall be illustrated by the German implementation of the directive that does not provide for unambiguousness of the identity of the signatory in every case (SigG §§2, 7). Considering legal interpretative documents of the e-signature act (Bundesrat 1996: 27; Bundestag 1997: 32) and the current practice in Germany, unambiguous identification of the signatory is generally not provided by qualified e-signature certificates issued by qualified CSPs. Unambiguousness can only be assured in case of individual authentication by the respective application provider. At the first contact, the submission of a personal ID-document is required for registration. Afterwards, unambiguous authentication with this provider is possible via a specific database ID-number allocated to the signatory.

7 For more information, an exhaustive discussion is provided by the Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications. (Siemens - Time.lex 2007b: 112-5).

8 In a joint pilot application by Estonia and Portugal, which is set to expand to Belgium, Finland and Lithuania, the registration of a company across borders using qualified electronic signatures has been realised. From a legal point of view, this has only been made possible by these countries having similar requirements for e-signature certificates. Many other European countries could not join this case due to their divergent legislations in this regard. See https://ettevotjaportaal.rik.ee/index.py?chlang=eng and/or http://www.epractice.eu/cases/CrossBorderDS.