EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Economic and Monetary Affairs

Employment and Social Affairs

Environment, Public Health and Food Safety

Industry, Research and Energy

Internal Market and Consumer Protection

Digital Internal Market

IMCO

EN

2011

EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY

INTERNAL MARKET AND CONSUMER PROTECTION

Digital Internal Market

STUDY

Abstract

The study examines the progress towards a digital internal market. In a first part, it focuses on the state of play and the possible revision of the Directive on electronic signatures. A second part describes the state of play with respect to eProcurement and discusses possible steps to advance the use of eProcurement in practice.

IP/A/IMCO/ST/2011-04 June 2011
PE464.421 EN

This document was requested by the European Parliament's Committee on Internal Market and Consumer Protection.

AUTHOR(S)

FPS Rechtsanwälte und Notare:
- Dr. Annette Rosenkötter
- Dr. Anja Hoffmann
- Dr. Andrea Gyulai-Schmidt
- Aline Fritz
- Elke Kühn

RESPONSIBLE ADMINISTRATOR

Elke Ballon
Policy Department Economic and Scientific Policy
European Parliament
B-1047 Brussels
E-mail: Poldep-Economy-Science@europarl.europa.eu

LINGUISTIC VERSIONS

Original: [EN]
Executive Summary: [DE, FR]

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
poldep-esc@europarl.europa.eu

Manuscript completed in June 2011.
Brussels, © European Parliament, 2011.

This document is available on the Internet at:
http://www.europarl.europa.eu/activities/committees/studies.do?language=EN

DISCLAIMER

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

CONTENTS

LIST OF ABBREVIATIONS

AES	Advanced Electronic Signature(s)
Art.	Article
bn	billion
BBG	Federal Procurement Company
B2B	Business to Business
B2C	Business to Consumer
CA	Contracting Authorities
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
Commission	European Commission
CSP	Certification Service Provider(s)
CWA	CEN Workshop Agreement(s)
DPS	Dynamic Purchasing System
eDocument	Electronic Document
eID	Electronic identification / electronic identity
EESSI	European Electronic Signatures Standardisation Initiative
EN	European Norm(s)
ES	Electronic Signature(s)
ETSI	European Telecommunications Standards Institute
EU	European Union
GDP	gross domestic product
i. a.	inter alia

MS	Member State
PKI	Public Key Infrastructure
QES	Qualified Electronic Signature(s)
QC	Qualified Certificate(s)
SEPA	Single Euro Payments Area
SME	Small and Medium-sized Enterprises
SSCD	Secure Signature Creation Device(s)
TED	Tenders electronic daily
TL	Trusted List(s)
TS	ETSI Technical Specifications
TSP	Trust Service Provider(s)
TR	ETSI Technical Reports
VSP	Validation Service Provider(s)
WP	Work Package

EXECUTIVE SUMMARY

ESIGNATURE DIRECTIVE (CHAPTER 2)

While all member states have implemented the general principles of the eSignature Directive, quite a number of differences in the legal implementation and interpretation of specific definitions or provisions can be identified. Main application fields for electronic signatures in the member states are currently the eGovernment and eBusiness (eInvoicing) sector, while they are rather rarely used in eCommerce.

Though the Directive has introduced legal certainty with respect to the general admissibility of electronic signature and their legal recognition, the market for electronic signatures has not developed as expected. An analysis of the legal implementation and the practical usage of electronic signatures and related standards shows that there are a considerable number of issues that create barriers on the legal, technical and trust level which currently limit the interoperability and (cross-border) use of electronic signatures. The main identified obstacles are the following:

- There is a fragmentation of markets and a lack of cross-border recognition of electronic signatures.
- The eSignature Directive contains unclear wordings and lacks regulations with regard to the provision of other certification services (CSP services) and respective liabilities, supervision and/or accreditation. For example, several services ancillary to electronic signatures have emerged in practice and which are not regulated by the Directive. Some member states have already established national regulations for such services, which have created additional barriers.
- Existing supervision and voluntary accreditation systems for certification service providers issuing qualified certificates differ which makes it very difficult to determine the trustworthiness of certification service providers.
- For advanced electronic signatures, interoperability issues in practice are even greater.
- Specific interoperability issues exist for eGovernment applications which are often designed with a purely national perspective and linked to national identity management schemes.
- From a technical perspective, there is a current lack of common and accepted standards. Standards are numerous but lack business orientation, clear arrangement and helpful guidelines.
- There is a lack of trust in electronic signatures originating from other member states due to legal and technical inadequacies.
- (Qualified) electronic signatures are often not used in practice, simply because not all contractors accept electronic signatures or have the necessary infrastructure and because the costs for the use of electronic signatures are still too high. Therefore, qualified electronic signatures are often replaced by simpler and cheaper signature solutions. Beyond this, there is still a lack of sufficient attractive electronic signature applications.

In order to overcome the identified obstacles, the member states and notably the Commission have initiated a number of measures at national and European level.

Nevertheless, most of the above-mentioned challenges continue to exist which makes further action necessary. Two main strategies to improve interoperability of electronic signatures and facilitate their cross-border use have been proposed:

The first strategy, a large-scale approach envisaging a comprehensive revision of the eSignature Directive, recommends to recast the existing legal, standardisation and trust framework into a common broader, more comprehensive and fully consistent framework covering all types of electronic signatures, the whole range of related products and all types of certification (CSP) services including services ancillary to or using electronic signatures as well as identification and authentification services. Technical details which are reliant on standardisation should – like in the current version – be addressed outside the Directive via Commission Decisions mapping technical standards with functional legal requirements. The existing multitude of inappropriate standards should be replaced by a common framework of rationalised, generally recognised European electronic signature standards (EESS) to be created within the existing standardisation mandate M/460. The results should be supported by appropriate promotional and educational efforts. This approach which is mainly supported by the CROBIES and EFVS Studies further recommends creating a sound and stable Trust Framework through appropriate supervision and voluntary accreditation schemes, certification of products and applications and Trusted Lists for all types of certification (CSP) services.

The second strategy, a small-scale approach, intends to improve the Directive’s business model and its success without amending the Directive. Instead of risking a difficult revision process with lengthy discussions, the supporters of this strategy propose to issue a non-binding Commission document to support a common interpretation of the Directive and clarify specific issues. They also opt for the creation of a rationalised standardisation framework based on real European Norms which should be referenced via Commission Decisions based on Art. 3.5 of the Directive, accompanied by appropriate marketing and promotion efforts.

In spite of the risks flagged, the comprehensive large-scale approach is in our view the preferable strategy. A thorough revision and extension of the eSignature Directive is crucial to create a sound legal basis for all certification (CSP) services which will also facilitate further enhancements on the standardisation and trust level. In order to overcome the specific issues in the eGovernment sector, additional initiatives regarding electronic identities and a clarification of the limits of Art. 3.7 of the Directive are necessary.

On the technical level, the mandate M/460 should be continued to ensure the creation of a rationalised European standardisation framework accompanied by appropriate guidelines and promotion measures. European Norms should be established and linked with the legal requirements of the revised Directive via Commission Decisions. Moreover, an appropriate trust infrastructure based on supervision and voluntary accreditation should be available for all types of certification (CSP) services. Existing pilot projects like PEPPOL, SPOCS and STORK and sector specific harmonisation initiatives should continue but be aligned with the revised Directive and well coordinated with the other initiatives to foster electronic signatures. Beyond this, additional economic supportive measures for electronic signatures should be taken. In particular, (financial) incentives for users and potential application providers to invest in electronic signature solutions, develop alternative business models and create attractive electronic signature applications for the mass market should be considered. Finally, the use of alternative practical types of electronic signatures such as mobile signatures should be fostered.

ePROCUREMENT (CHAPTER 3)

eProcurement as the use of an internet-based electronic system which automates and integrates any part of the procurement process has the potential to increase accessibility, transparency, efficiency and cost reduction in the procurement process.

To unlock this potential, the 2004 Public Procurement Directives 2004/17/EC and 2004/18/EC introduced several provisions aimed at enabling eProcurement uptake in all member states. In addition to the new provisions and to ensure their implementation the Commission adopted in 2004 the Action Plan for the implementation of the legal framework for electronic public procurement.

Considering the state of play today some notable successes have been achieved on national level, but the use of eProcurement remains far behind the expectations of the 2004 Action Plan, especially with regard to cross-border eProcurement. The Commission estimates that less than 5 % of total procurement budgets in the first-mover states is awarded through electronic budget.

The main obstacle that can be identified is the lack of standards: too many different technical solutions are in place, some only in use in one small contracting authority. This market fragmentation complicates the task of economic operators who seek to participate in multiple systems, in particular when it comes to cross-border participation.

Considering the different procurement phases and tools, the submission phase and the invoicing/payment phase seem to encounter the biggest obstacles. Questions of identification, authentication and integrity of data are crucial especially for eSubmission, but have not yet been solved. For all other phases, there seem to be no significant obstacles. The still limited usage in practice could be due to the lack of systematic eProcurement infrastructure which can still be observed in most of the countries.

To promote eProcurement and to achieve a better cross-border use the EU is financing and/or supporting a number of initiatives, including the PEPPOL project, which seems to have the most comprehensive approach. Most of the initiatives are focussed on standardisation.

With regard to electronic signature, there remain significant interoperability barriers which constitute a real challenge to cross-border public procurement. As the Procurement Directives give contracting authorities the freedom to choose the appropriate method of authentication, the member states set different levels of requirements, ranging from a user-ID and password-based model up to qualified electronic signature. Most of these solutions do not enable cross-border use.

The current approach to promote qualified electronic signature for eProcurement should be reconsidered. We recommend encouraging the use of username/password-based models as commonly used electronic signature in eProcurement. These models are less complex and costly and do not pose any (cross-border) interoperability barriers. However, they should be backed by a security token to ensure that the documents being submitted are protected against tampering.

To bring forward the standardisation process as a key issue in eProcurement, a close coordination between the different EU-financed projects is necessary. To avoid the emergence of (again) differing standards, common standards should be developed within the existing system of CEN/ BII2.

The concept of mandatory eProcurement imposed by the EU should, if at all, only be a long term concept with a realistic period of transition and should be decided by each member state.

Furthermore eProcurement should not only be a transposition of the elements of "paper procurement", but has to be simpler than traditional procurement, if uptake is to be achieved. It would also be helpful to clarify certain general questions with regard to the use of eProcurement in the Directive; besides, some of the obstacles could be removed by legislative modification, such as an improvement of mutual recognition of certificates, the permission of self-declarations on the fulfilment of the selection criteria and modifications to enhance the use of Dynamic Purchasing System (DPS). Moreover, more efforts could be done to overcome language barriers. Concerning the permission of self-declarations and the language barriers, these proposed actions would also promote cross-border competition in paper-based procedures.

Finally, the benefits of eProcurement solutions have to be communicated more concisely among all relevant stakeholders.

1. INTRODUCTION

The European Commission Work Programme 2011 (especially the section 'Digital Agenda') contains a number of proposals which are linked to developing a digital internal market. In particular, as part of the re-launch of the Single Market, the Commission will propose the revision of the Directive on electronic signatures (1999/93/EC) in 2011 and a decision to ensure mutual recognition of eIdentification and eAuthentication across the EU by 2012. Electronic identity technologies and authentication services are essential for all kinds of online transactions.

Furthermore, the Commission last year launched a consultation on eProcurement. The Commission will seek the views of interested parties on how the EU can help member states to speed up and facilitate the procurement process.

The present study examines the current state of play in the progress towards a digital internal market. In a first part, the study will focus on the issues relevant to the state of play and the revision of the Directive on electronic signatures (Chapter 2). The second part will describe the state of play with respect to eProcurement and will discuss further possible steps to advance the use of eProcurement in practice (Chapter 3).

2. eSIGNATURE DIRECTIVE

The Directive 1999/93/EG (hereinafter: "(eSignature Directive") was enacted to enable trustworthy systems for identification and authentication of data in a rapidly growing market on the internet.[1] Based on a technologically neutral approach, the European Legislature established a legal framework for the national and cross-border use of electronic signatures (ES[2]) in various areas of practice. Main principles of the Directive are a free market for electronic services, legal recognition of ES as evidence in legal proceedings, mutual acceptance of certificates that comply with the minimum standards of the Directive as well as liability rules for service providers.[3]

In a first Chapter (2.1), we will examine the current state of play of the eSignature Directive. The second Chapter (2.2) will give an overview about the main existing obstacles in particular for the interoperability and the cross-border use of ES. The third Chapter (2.3) will recapitulate the main past and present initiatives at the national and the European level to overcome these obstacles. In the fourth Chapter (2.4), we will outline the main existing proposals to improve the interoperability of ES and to facilitate their (cross-border) use. Finally, in a concluding Chapter (2.5), we will evaluate the recommendations outlined in Chapter 2.4 and present our opinion on the steps that should be taken to create an ES system that works at the European level.

2.1. Current state of play of eSignature Directive

The eSignature Directive has established a legal framework for the use of electronic signatures and certification services. Regulations are limited to an essential minimum in order to leave room for technical development potentialities.

While all member states have implemented the general principles of the Directive, there are differences in the legal implementation and interpretation of specific definitions or provisions. Currently, electronic signatures are mainly applied in the eGovernment and the eBusiness sector.

2.1.1 eSignature Directive – main issues

The Directive aimed, on the one hand, to conform to the challenge of advancing interoperable structures and standards and intended on the other hand to provide a basis for free flow of ES services and products. To reach this aim, the Directive only formulated a minimum of regulation with regard to technical and organisational matters.

2.1.1.1. Legal definition of electronic signatures

The Directive determines three levels of ES with ascending requirements: the "electronic signature", the "advanced electronic signature" (AES) and the "qualified electronic signature" (QES) which is not explicitly termed but outlined by the legal effects of Art. 5.

[1] COM (1998)297 final

[2] "ES" in this document shall not mean only the lowest level of ES (see below 2.1.1.1), but shall comprise all levels of ES (including AES and QES).

[3] Study on Standardisation Aspects of eSignature, 2007, p. 11.

ES are 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 broad definition does not implicate any security aspects, whereas AES have to meet further requirements of being uniquely linked to the signatory, capable of identifying the signatory, created using means that the signatory can maintain under his sole control and being linked to the data to which it relates in such a way that any subsequent change of the data is detectable. Without further specification of organisational or technical aspects, the Directive does not attach any legal effects to AES.

QES furthermore have to be based on a qualified certificate (QC), which is provided by a certification service provider (CSP), and have to be created by a secure signature creation device (SSCD). Solely QES deploy the legal effect of being put on a par with handwritten signatures (Art. 5). Mainly focusing on QES, the Directive posts a variety of requirements for components of the QES system: QCs must comply with the specifications of Annex I and have to be provided by a CSP that conforms to the requirements of Annex II. Annex III finally posts requirements for SSCD.

2.1.1.2. Legal and technical scope of the Directive

The regulations of the Directive allow scopes for certification services and technical standards with intent to limit the regulations to an essential minimum and to leave room for technical development potentialities. [4] Legal aspects, mainly accreditation and supervision of CSP as well as the "public sector clause", are addressed in Chapter 2.1.2.

Even if the definition of AES and QES is technology-neutral, it refers mainly to using Public Key Infrastructure (PKI) technology. [5] The principle of PKI is based on asymmetric cryptography in which a user holds a pair of keys, one private and one public key that are connected through a mathematical one-way function to assure that the private key cannot be deducted from the public key.[6] The ES is created through the private key (e.g. smart cards) by encrypting a digest of the original message (hash-value). The attached signature can be decrypted by the commonly accessible public key. The positive comparison between the hash-value of the document and the decrypted hash-value thereby ascertains the integrity of the document.[7]

Technical and organisational aspects of the mainly focused QES are regulated broadly but on a high level through the Annexes.[8] According to Annex II f), CSP, for example, must employ "trustworthy systems and products" to issue QC. The Commission is given the authority (Art. 3.5) to reference standards for ES products that fulfil the requirements of Annex II f) and Annex III concerning QES.

The Directive does not contain regulations for electronic identification (eIdentification/eID).[9] The definition of AES (Art. 2.2) only states the capability of identifying the signatory; likewise, Annex II simply defines the duty of CSP to verify by appropriate means the identity of the person to which a QC is issued.

[4] See Considerations 8, 28 of the eSignature Directive.

[5] ELSIGN Study, 2003, p.30.

[6] BSI, 2006, p. 21.

[7] NTC, 2004, p. 17.

[8] EFVS Study, CSM – Final Report, 2010, p. 13.

[9] See Chapter 2.3.2.6 below on European initiatives in the eID sector.

2.1.2 Legal implementation of eSignature Directive

While all member states have implemented the general principles of the Directive[10], quite a number of differences in the legal implementation and interpretation of specific definitions or provisions can be identified. Focusing on a number of selected provisions, Chapter 2.1.2 will outline relevant differences in the transposition of the Directive.

2.1.2.1. Electronic Signatures

Austria as the first member state to transform the Directive into national law defined a "secure ES" which referred to a QES. The 2008 regulatory reform aimed to align Austrian law more closely to the Directive and introduced the concept of AES. In some MS, however, there is still some divergence between the concepts used in the legal framework, e.g. the AES defined as being based on a QC, and the concept of secure ES still being used. Slovak law even limits its definition of ES to digital signatures (based on asymmetric cryptography).[11]

Some national Electronic Signature Acts do not address all types of ES. For example, Estonian law only regulates AES and generally established the legal effects of Art.5 of the Directive. In contrast, Latvian and Danish law only cover QES.[12]

Beyond this, a fourth type of ES, the AES based on a QC but created without a SSCD, has emerged and seems to be significantly used in practice. While the legal effects attributed to QES[13] do not apply to AES based on a QC, this signature type also benefits from the legal obligation of the member states to mutually recognise QC.[14]

2.1.2.2. Legal effect of electronic signatures

The legal recognition of ES is essential to advance their acceptance and use. The legal effects of Art. 5.1 for QES have been implemented in the national law of all member states.[15] QES have the same legal value as handwritten signatures and are admitted as evidence in legal proceedings.

The Directive does not award the same legal value to other types of ES. Nevertheless, the legal framework in most member states requires a handwritten signature only for a limited number of legal actions. Many actions do not rely on a signature at all and can be easily replicated in an electronic context with more basic ES types.[16] The non-discrimination rule of Art. 5.2 states that the acceptance of ES of whatever type cannot be denied in legal proceedings merely because it is in electronic form. Some member states have implemented legal equivalence of "lower-level" ES with QES (e.g. Italy, Estonia).[17] As regards the existing case law in the member states, a study from 2007[18] stated that the legal value of ES is being mainly decided on a case-by-case basis emphasizing their security level and does not necessarily distinct between the types of ES defined in the Directive.[19]

[10] EC, Operation of eSignature Directive, 2006, p. 4; Ramboll Management, 2006, p. 1.

[11] Study on Mutual Recognition of eSignatures, 2009, 2009, p. 63, 64f.

[12] Study on Mutual Recognition of eSignatures, 2009, p. 66.

[13] See below Chapter 2.1.2.2.

[14] CROBIES Study, 2010, HD, p. 7.

[15] ELSIGN Study, 2003, p. 68 f.; Ramboll Management, 2006, p. 1.

[16] EFVS Study, Analysis and Assessment of the Solutions Report, 2009, p. 58.

[17] ELSIGN Study, 2003, p. 77.

[18] Study on Standardisation Aspects of eSignatures, 2007, p. 19f.

[19] ELSIGN Study, 2003, p. 82.

2.1.2.3. Qualified Certificate (QC)

Use of an ES shows that a document has been signed with a certain private key and that it has not been changed after signature (integrity). However, a further mechanism is necessary to show that the used private key is attributable to a certain signatory (personal authentication). This is realized by issuance of a certificate (which links the name of the owner of the private key with the public key) by a CSP ("trusted third party") who thereby asserts that the public key is linked to a certain signatory.[20] A certificate is qualified if it contains the specifications listed in Annex I to the Directive and is provided by a CSP who fulfils the requirements laid down in Annex II. In particular, CSP may issue QC only after having verified the identity of a person "by appropriate means in accordance with national law"[21], definition of which is left up to the member states. However, in order to receive a QC, personal appearance is necessary in all member states except for the use of OCES[22] signatures for the public sector in Denmark. Since the Directive defines the signatory in Art. 2.3 as "a person", it is unclear if QCs can only be issued to natural persons (which is the case in most MS) or also to legal persons (which is possible e.g. in Spain, Portugal, Hungary, Latvia and Romania).[23]

2.1.2.4. Secure Signature Creation Devices (SSCD) and Conformity Assessment

Annex III of the Directive appoints the requirements for SSCD. On the basis of Art. 3.5, the Commission has specified types of SSCD that conform to these requirements.[24] Art. 3.4 provides that the conformity of SSCD with Annex III shall be determined by *appropriate* public or private bodies designated by member states. Commission Decision 2000/709/EC laid down minimum criteria of expertise, independence and professionalism of 'Designated Bodies' to be taken into account by member states in order to prevent manipulation or misuse.[25] However, the Directive does not contain a direct obligation for each member state to designate a suitable body. This is why in 2010 only 12 member states had a 'Designated Body' in the sense of Art. 3.4.[26] It is also unclear whether a formal conformity assessment by a Designated Body is mandatory or not[27]. Therefore, different types of compliance statements for SSCD recognition have emerged[28], which causes legal barriers for cross-border use of SSCD.[29]

2.1.2.5. Certification Service Provider (CSP)

A CSP is defined in Art. 2.10 as "an entity or a legal or natural person who issues certificates or provides other services related to ES". This broad definition with the intention to facilitate free market access of CSP and to imply ancillary services like time-stamping or long-term archiving (see below 2.1.3.1) that are not explicitly regulated by the Directive has led to an unclear market situation (see below 2.2.1).

The minimum liability regulations for CSP laid down in Art. 6 of the Directive are crucial to enable a trust framework for QES and AES based on QC. The user has to rely on the designation of a certificate issued by a CSP being "qualified" and to conform with the

[20] BSI, 2006, p. 46f.; Signature Perfect, 2008, p. 42.

[21] See Annex II d) of the Directive.

[22] "OCES" is the danish abbreviation for Public Certificates for Electronic Services ("Offentlig Certifikat for Elektronisk Services"), the Danish national digital signature standard.

[23] Study on Mutual Recognition of eSignatures, 2009, p. 89, 91.

[24] Commission Decision 2003/511/EC, see Chapter 2.3.2.2 below.

[25] ELSIGN Study, 2003, p. 47. For further details see Chapter 2.3.2.3 below.

[26] CROBIES Study, WP 4, p. 14f.

[27] Settling this discussion will require further action, see EFVS Study, CSM – Final Report, 2010, p. 24.

[28] CROBIES Study, WP 4, p. 12f.

[29] See Chapter 2.2.1. below.

Directive's provisions. Therefore CSP are liable for the accuracy of QC in the outline of Art. 6.1 under the precondition of negligence which is presumed unless the CSP proves that he has not acted negligently. A limitation of liability is possible if denoted in the certificate.[30] Yet it is not entirely clear if these liability rules also apply to the signatory.[31]

2.1.2.6. Supervision of CSP

Suitable supervision of CSP is currently a purely national competence.[32] Art. 3.3 of the Directive obliges member states to establish an appropriate supervision system for CSP established on their territory, without any further specifications on how supervision should be organised. Member states may decide how they ensure the supervision of compliance with the provisions laid down in the Directive.[33] This scope is limited by the prohibition of prior authorisation in Art. 3.1 and basic market rules (e.g. freedom of establishment). The member states have to proceed cautiously to strike a balance between consumer and business needs. Most member states have implemented a mandatory notification for CSP issuing QC to the public to a supervisory body before starting service[34] which is in line with the Directive.[35] However, the supervision systems differ and therefore lack mutual recognition between member states.[36]

2.1.2.7. Voluntary Accreditation of CSP

To prevent different national accreditation systems for CSP as a feared barrier to the use of electronic communications and electronic commerce, the Directive strictly prohibits prior authorisation of CSP (Art. 3.1) but allows voluntary accreditation as an incentive for service providers to offer higher quality and to flexibly meet a changing technical environment (Art. 3.2).[37] These voluntary accreditation schemes aim at enhanced levels of CSP service provision and offer member states to establish additional quality requirements which can further ensure the trustworthiness of specific ES solutions.[38] In practice national accreditation schemes do not exist in all member states and are sometimes organised by the private sector (e.g. in the UK).[39] Where established, these schemes vary notably and are not comparable from one member state to the next.[40]

2.1.2.8. Public Sector clause (Art. 3.7 eSignature Directive)

Art. 3.7 allows member states to impose additional requirements for the use of ES in public sector applications. However, such requirements must be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Several member states have not defined additional rules for ES applications in the public sector. Other member states have introduced specific eGovernment Acts that ascertain citizens to communicate with public administrations electronically or allow public administrations to use ES towards citizens. Some member states additionally encourage the use of ES by certain regulations, e.g. the right to reply to an electronically signed communication (Bulgaria) or the right to access electronic copies (Spain).[41] Some require the use of QES in eGovernment applications.

[30] ELSIGN Study, 2003, p. 55f.

[31] EFVS Study, CSM – Final Report, 2010, p. 14.

[32] EFVS Study, CSM – Final Report, 2010, p. 8.

[33] See Consideration 13 of the eSignature Directive. This leads to.

[34] Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 92.

[35] ELSIGN Study, 2003, p. 40.

[36] See Chapter 2.2.1 below.

[37] CROBIES Study, 2010, WP 1, p. 7.

[38] EFVS Study, CSM – Final Report, 2010, p. 13.

[39] Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 92.

[40] Regarding the issue of obligatory accreditation schemes see Chapters 2.1.2.8 and 2.2.1 below.

[41] Study on Mutual Recognition of eSignatures, 2009, p. 83.

Example: the German approach[42]

With regard to the topic of ES in eGovernment applications, it is worth noting that when electronic signatures procedures are used or offered, only qualified electronic signatures are used. This applies for the federal Government, states and municipalities and can be traced to the German legal system (so-called written form requirement).

Beyond this, in various member states accreditation is obligatory in order to access the "market" for eGovernment applications. There is a discussion about whether such obligatory accreditation schemes are in line with Art. 3.7 of the Directive[43] which is unlikely since they may cause an obstacle for cross-border use.[44] The Commission already stated that the limitation on accredited CSP in the public sector restrains the legal effects of QES[45] since the non-discrimination rule of Art. 5.2 also applies to the public sector.

2.1.3 Current practical application of eSignatures and related services

The following chapter intends to give an overview of the current practical application of ES, in particular of the services in the field of ES that have emerged on the market (see 2.1.3.2) and the main application areas of ES existing in practice at present (see 2.1.3.2).

2.1.3.1. Main services in the field of eSignatures

First of all, CSP services in the narrow sense imply the issuance of non-qualified and qualified certificates, the latter of which is regulated more broadly by the Directive.

Besides these basic services, a broader spectrum of CSP services has emerged in practice. These services include

- services ancillary to or supporting ES, such as time-stamping, (long term) archiving, signature policy services and signature validation services,
- services employing ES such as electronic registered mail services, and finally
- services from identification service providers and authentication service providers.[46]

(1) For example, **time stamps** issued by a CSP can be used to document the moment in time before which or in which an ES was created.[47] They offer a reliable way to determine whether an ES was valid at the time of signing/verifying or at the time the validation must relate to.[48] Such documentation may in particular become relevant if a QC on which an ES is based has been revoked after creation, but before verification of the ES. To create respective evidence, a QES should always be complemented by a time stamp shortly after creation. Some national laws have implemented regulations on time-stamping and other CSP services or even define qualified time-stamping (e.g. Czech Republic and Germany).[49] For example, qualified time stamps issued by a CSP fulfilling the requirements of the German Signature Act promise a high evidentiary value before a German court.[50]

[42] Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 33.

[43] Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 92.

[44] See below Chapter 2.2.1.

[45] Deutscher Bundestag, Drucksache 14/5324, p. 24.

[46] CROBIES Study, 2010, HD, p. 16.

[47] The moment of creation of a QES is the relevant moment in time for its verification under German law, see BSI, 2006, p. 66.

[48] EFVS Study, CSM – Final Report, 2010, p. 18.

[49] Study on Mutual Recognition of eSignatures, 2009, p. 65.

[50] BSI, 2006, p. 85.

(2) In many application areas it is (mostly due to legal obligations) necessary to retain or store documents for a long period of time. In any case, documents must be retained as long as their content may have a contractual or other legal effect. However, cryptographic mechanisms lose their security qualification in the course of time due to the technical progress. An ES which today is accepted as sufficiently forgery-safe may become easily forgeable tomorrow. Therefore, in order to preserve the evidentiary value of QES in the long run, it must be assured that before the anticipated adequateness of the algorithms and parameters used for the creation of the QES expires, the data must be resigned with a new QES based on new, adequate algorithms or corresponding parameters, which should be complemented with a qualified time stamp.[51] These and similar **long term archiving services** ensure that the ES and the signed document can be validated over a longer period of time.[52] Some member states have implemented rules on long time storage of electronically signed documents.[53]

(3) Beyond this, **signature policy services**, meaning services issuing signature policies or supporting their design become more and more important for providers of ES applications in particular in the eGovernment sector. Such services are used to determine the exact conditions under which an ES must be created and verified before it can be considered as valid in a given context or under a specific application.[54]

(4) Due to several issues on the different levels of the existing European ES framework (see below 2.2), there is also a current need for parties receiving ES to use **signature validation services** taking over or assisting them with the validation of a received ES. In practice, the verification of an ES requires not only the verification of its mathematical correctness as such, but also of the authenticity and integrity of the certificate.[55] This may include the verification of the CSP's signature, the type (qualified or non-qualified) and the validity of the certificate (i.e. not revoked or expired) at the point relevant in time, and may also require the retracing of a "verification path", i.e. a chain of certificates up to a trustable (root) certification authority.[56] Furthermore, the correctness of the certificate for the respective purpose of use[57], and – where applicable – of the certificate policy under which the certificate was issued must be verified.[58] Finally, an assessment of the "quality", trustworthiness and the legal value of the ES is necessary.[59] It should be noted that a validation process may rely on the provision of several ancillary services[60] as defined above which are sometimes offered by validation service providers as a single point of contact.[61]

(5) An example for a new, increasingly discussed type of services in the context of which also ES can be used are **electronic registered mail services**. Some member states have adopted legal frameworks for electronic and hybrid registered mail, e.g. Belgium[62] and Germany.[63]

[51] BSI, 2006, p. 88f.

[52] EFVS Study, CSM – Final Report, 2010, p. 18.

[53] Study on Mutual Recognition of eSignatures, 2009, p. 65.

[54] EFVS Study, CSM – Final Report, 2010, p. 18.

[55] EFVS Study, CSM – Final Report, 2010, p. 17.

[56] BSI, 2006, p. 64.

[57] A certificate must be admitted for the respective purpose(s) of use. The purposes of use mentioned in the certificate must correspond with the purpose of the digital signature to be verified, see BSI, 2006, p. 65, 68f., 82.

[58] BSI, 2006, p. 64f.

[59] EFVS Study, Analysis & Assessment Report, 2009, p. 9f. Further details on the requirements of a successful validation and a description and structure of an ideal signature validation solution can be found in EFVS Study, CSM – Final Report, 2010, p. 17.

[60] CROBIES Study, 2010, HD, p. 8 ; EFVS Study, CSM – Final Report, 2010, p. 14.

[61] EFVS Study, CSM – Final Report, 2010, p. 18.

[62] www.timelex.eu/nl/blog/p/detail/new-legal-framework-for-electronic-and-hybrid-registered-mail-adopted-in-belgium

(6) Several providers also offer **identification and authentication services**[64] e.g. to verify the identity of a person and establish the validity of a message and its originator.

2.1.3.2. Main current applications of electronic signatures

In most member states, there are numerous applications that rely on ES.

In particular, **eGovernment** services towards enterprises and citizens are a domain strongly benefitting from ES.[65] eGovernment applications are interactive[66] public services using electronic means which are offered entirely or partially by or on the authority of a public administration for the mutual benefit of this administration and the end user [meaning citizens ("A2C"), legal persons ("A2B") and/or other administrations ("A2A")].[67] Already in 2007, a variety of approximately 130 eGovernment applications in different member states could be identified, 90 of which rely on ES.[68] A study from 2009[69] surveyed the main areas of ES practice in 32 European countries and identified 19 countries offering **eProcurement** applications, 16 offering **eHealth** applications and 13 offering **eJustice** applications. Besides these, applications are established in the area of taxation and in the social area. It is worth noting that there are more and more applications for citizens and legal persons developed within member states that have deployed eID cards to the mass.[70]

Positive example: Austrian Citizen Card (Bürgerkarte)

A positive example is Austria which offers a great number of eGovernment applications for citizens and legal persons using the "Bürgerkarte"[71], an electronic identity (eID) card enabling them inter alia to register a business online or issue in an electronic form applications for pensions, child benefit, subsidies (e.g. for house building), applications and notifications relating to building law, applications for birth and marriage certificates or for certified copies from register of births and marriages, or to use many other services.[72]

[63] In Germany, the so-called "DE-Mail Act" (www.gesetze-im-internet.de/bundesrecht/de-mail-g/gesamt.pdf) has entered into force on May 3rd, 2011. Germany thereby implements the requirement of Artt. 6ff. of the Services Directive demanding that public authorities must accept electronic communication as a reliable medium and ensure that the relevant procedures may be completed by electronic means, see http://dipbt.bundestag.de/dip21/btd/17/036/1703630.pdf, p. 21, 44f. However, giving more details on registered electronic mail services would go beyond the scope of this Study.

[64] EFVS Study, CSM – Final Report, 2010, p. 29, 35; CROBIES Study, 2010, HD, p. 16 footnote 15.

[65] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 52; EC, Operation of eSignature Directive, 2006, p. 6; Ramboll Management, 2006, p. 1.

[66] Interactivity requires that a transaction between the parties must be involved (and not only one-way communication by a public administration (such as the publication of standardised forms on a website).

[67] See Preliminary Study on Mutual Recognition of eSignature, 2007, p. 8.

[68] The remaining 37 ones mainly use electronic certificates to achieve strong authentication but not for signature of documents in the sense of Art. 2.1, see Preliminary Study on Mutual Recognition of eSignature, 2007, p. 47, 62.

[69] Study on Mutual Recognition of eSignatures, 2009, p. 96ff.

[70] Study on Standardisation Aspects of eSignature, 2007, p. 56. Examples for existing eGovernment applications can be found in Preliminary Study on Mutual Recognition of eSignatures, 2007 (see in particular p. 74 ff.).

[71] See also Chapter 2.3.1.2 below.

[72] For more details see www.buergerkarte.at/anwendungen.de.php

ES are also used in different **eBusiness** related applications. Main relevant business fields for ES are electronic banking (**eBanking**)[73] and electronic invoicing (**eInvoicing**).

The banking sector has been mentioned as a specific sector showing a major interest in ES.[74] Although a few years ago, the banks were using proprietary security systems, a trend toward the use of ES could be observed. However, many authentication systems for personal eBanking services still rely on one-time passwords and tokens, being the simplest form of ES. Many eBanking applications only use these technologies for user authentication but electronic signing of transactions is increasing. For corporate eBanking it is more common to use smart cards which are considered to provide a higher level of security.[75]

Beyond this, a great number of well developed and integrated solutions offering eInvoicing facilities exist today. There are several positive examples for large eInvoicing platforms including the one of Portugal Telecom Group, Certipost and Isabel in Belgium or Certum[76] in Poland.[77] eInvoicing is ruled by the EU VAT Directive 2006/112/EC[78], amended by Directive 2010/45/EU, obligating the member states to simplify eInvoicing.[79] Art. 233 lists QES as an example of technologies that ensure the authenticity and content of an electronic invoice.

Furthermore, numerous professional organisations in Europe have identified the benefits of using ES, in particular notaries, accountants and advocates. For example, the Belgian and French notaries have a professional PKI card (SSCD) bearing a QC, which is called REAL card.[80]

In contrast, ES are still rather rarely used in the **eCommerce sector**. Directive 2000/31/EC on electronic commerce governs a range of matters, e.g. electronic contracts, but does not refer to ES. Indeed, it provides that member states must ensure that their legal system allows the conclusion of contracts by electronic means, subject to some exceptions (Art. 9).

However, several providers offer online signature services which allow their customers to sign documents electronically with a legal value (mostly QES) and send them via classical email. Examples are *Certipost*[81] in Belgium, *Digidoc*[82] in Estonia and *Safelayer*[83] in Spain.[84]

[73] See already EC, Operation of eSignature Directive, 2006, p. 6.

[74] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 53.

[75] EC, Operation of eSignature Directive, 2006, p. 4.

[76] http://www.certum.eu

[77] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 61.

[78] Following the issuance of the eSignature Directive, Directive 77/388/EEC was amended through Council Directive 2001/115/EC (followed by a few other Directives) which was then incorporated into a revised VAT Directive 2006/112/EC and amended by Directive 2010/45/EU. See also Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 40, 61.

[79] Art. 232 provides that the use of electronic invoices shall be subject to acceptance by the recipient, leaving it up to each taxable person to determine the way to ensure the authenticity of the origin, integrity of the content and legibility of the invoice.

[80] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 62. For European initiatives in the field of eJustice see Chapter 2.3.2.5 below.

[81] www.e-signing.be

[82] http://digidoc.sk.ee/entry_splash.html

[83] www.safelayer.com

[84] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 62.

Positive Example: Certipost e-signing service (Belgium)

For example, the Belgian Trust Service Provider Certipost offers a service that enables users to sign electronically with a qualified electronic signature (and thus with legal value equivalent to handwritten signature) any type of file or document (e.g. contracts, forms, subscriptions) with a Certipost digital certificate or electronic identity card. To assure the signer of the compliance of its signature with the legal requirements, Certipost creates a signature zip file archive containing three files: (1) the original signed document, (2) a technical file containing the signature itself, the certificate and the necessary information on the certificate and a time stamp to prove that the information has not been changed after signature, and (3) a PDF file giving some explanation about the archive. This zip file can then be sent via e-mail to the recipient together with an explanation. The receiver may likewise use the services offered by Certipost to easily verify whether the electronic signature is valid and – if appropriate - to countersign the document.

2.2. Existing obstacles for interoperability and (cross-border) use of electronic signatures

The main obstacles for the interoperability and (cross-border) use of electronic signatures are the following:

- *A fragmentation of markets resulting from the current diversity of national systems and the emergence of isolated applications for electronic signatures and a lack of cross-border recognition of electronic signatures;*
- *Interpretation discrepancies regarding the eSignature Directive and the fact that the Directive focuses only on qualified electronic signatures and the issuance of (qualified) certificates and lacks regulations e.g. on other certification services ancillary to electronic signatures;*
- *From a technical perspective, a lack of clear, common and accepted standards;*
- *A lack of trust in electronic signatures originating from other member states;*
- *Low use of electronic signatures due to complexity, high costs and lack of attractive applications.*

A legal and technical analysis of the practical usage of ES shows that there is a considerable number of issues that currently limit the interoperability and (cross-border) use of ES[85], especially since a broader spectrum of CSP services has emerged. Chapter 2.2 will provide an overview about the main identified obstacles within the framework offered by the eSignature Directive, grouped into barriers on the legal and administrative level (2.2.1), on the technical level (2.2.2) and on the trust level (2.2.3).

[85] EC, Action Plan on eSignatures and eID, 2008, p.4.

2.2.1 Legal and administrative barriers

(1) First, the wide scope of discretion in transformation of the Directive into national law has led to a **diversity of national systems** and evolvement of **isolated applications.**[86]

(2) Secondly, the primary objective of the eSignature Directive to promote cross-border legal recognition of ES has not been achieved (yet), as there is currently a **lack or at least an incompleteness of cross-border recognition of ES**. [87] A barrier for mutual recognition of QES arises e.g. from the fact that in a few countries QC can be issued not only to natural but also to legal persons. A member state that does not acknowledge the concept of a QC created directly by a company may however not consider this ES legally valid. The Directive is insofar unclear and requires clarification.[88]

(3) Beyond this, the Directive partly **lacks clear definitions** (e.g. "authentication" within the definition of ES is not defined")[89]. Such open wording and the lack of or different understanding of the ES system and definitions has resulted in discrepancies in the interpretation of the Directive[90] and **unclear and incoherent case law in the member states** on the legal effect[91] of ES.[92]

(4) Above all, the **current European ES legal framework** is widely considered **too narrow**[93], as it is in principle **limited to QES** and one specific type of CSP, namely a **CSP issuing QC**, which is currently de facto the main area of focus of the Directive and its detailed requirements and annexes. Only the QES (Art. 5.1) and the provision of QC are fully and clearly defined and regulated through specific requirements. Therefore, only CSP issuing QC to the public are regarded to be covered by the Directive in sufficient detail.[94]

In contrast, there is a **lack of common and specific requirements** at EU level with regard to the **provision of other CSP services employing ES or ancillary to ES,** such as time-stamping, (long term) archiving, or signature validation.[95] This is crucial as some of these services are intrinsically required in order to implement PKI based digital signatures which are currently the sole technical solution to implement AES and thus QES.[96] Likewise, the complex validation process for ES may rely on the provision of ancillary services.[97] The Directive only briefly touches on other CSP services[98], but does not clearly regulate them in terms of requirements or by referencing related standards.[99]

[86] Datev eG, Stellungnahme zur Evaluierung der Richtlinie 1999/93/EG, 19.08.2003, p. 2.

[87] CROBIES Study, 2010, HD, p. 7.

[88] Study on Mutual Recognition of eSignatures, 2009, p. 86ff., 90.

[89] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 105.

[90] Ramboll Management, 2006, p. 1.

[91] See above Chapter 2.1.2.2.

[92] For more details see Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 24.

[93] CROBIES Study, 2010, HD, p. 8f.; EFVS Study, CSM – Final Report, 2010, p. 14ff.

[94] EFVS Study, CSM – Final Report, 2010, p. 29, 24.

[95] For definitions and explanations of such services see Chapter 2.1.3.2 above.

[96] See also Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 104.

[97] CROBIES Study, 2010, HD, p. 8; EFVS Study, CSM – Final Report, 2010, p. 14.

[98] Recital 9 of the Directive notes that "ES will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using ES; the definition of such products and services should not be limited to the issuance and management of certificates, but *should also encompass any other service and product using, or ancillary to, ES, such as registration services, timestamping services, directory services, computing services or consultancy services related to ES*". Art. 2.11 defines a CSP as "an entity or a legal or natural person who issues certificates *or provides other services related to ES*". Art. 2.12 defines an ES product as "hardware or software, or relevant components thereof, which are intended to be used by a CSP for the provision of ES services *or are intended to be used for the creation or verification of ES*".

[99] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 105.

For example, the concept of a validation service provider (VSP) and the criteria for ES verification services[100] are entirely undefined, which entails that their services are not comparable at EU level and that specific requirements cannot be determined uniformly.[101] The absence of regulations for time based ES services (time-stamping, electronic archiving) also renders a reliable long term validation extremely difficult.[102] The result is that VSP have to design their own solutions and can currently only operate on a local and not on a cross-border level.[103]

Furthermore, the Directive does not fix the **obligations and liabilities of providers of other types of CSP services than issuing QC to the public**.[104] The specific liability rules in Art. 6 only apply to CSP issuing QC.[105] The current impossibility to obtain sufficient guarantees with regard to responsibility and liability[106] for the reliability and value of ES, backed by an entity willing to take responsibility and liability for making assertions related to this point is seen as a major reason why ES from other member states are not easily accepted.[107]

The absence of a coherent legal framework and sufficient guarantees also makes it very difficult to determine **the trustworthiness of CSP.** The Directive does not contain clear provisions regarding the mutual recognition between different CSP.[108] As it allows member states to decide what they consider an appropriate supervision system[109] without stipulating common minimum requirements, the **supervision systems of CSP issuing QC differ quite widely** between member states, which is detrimental for their mutual recognition.[110] For example, the existing VSP have to establish own criteria to determine whether a CSP covered by the validation service is indeed trustworthy. This leads to market fragmentation and impairs the provision of cross-border validation services, at least with respect to ES which are not based on QC.[111] Beyond this, there is the danger that CSP establish their business in member states with the lowest supervision requirements, which could foster the belief that their ES are of a lower "quality".[112]

Finally, some member states have already established national laws and regulations on the provision of ancillary CSP services. For instance, Italy, Germany and Hungary have national laws on the provision of time-stamping services in particular when supporting (Q)ES.[113] Divergences in such national laws/initiatives may rapidly create or are already creating undesired additional barriers to the interoperable and cross-border use of ES.[114]

[100] EC, Operation of eSignature Directive, 2006, p. 7.

[101] EFVS Study, CSM – Final Report, 2010, p. 23.

[102] EFVS Study, CSM – Final Report, 2010, p. 8. Beyond this, there are no complete and common European standards nor an adequate trust framework, see below 2.2.2 and 2.2.3.

[103] EFVS Study, CSM – Final Report, 2010, p. 27. In practice, validation service providers often define their own policies which then have to be contractually accepted by the users of the validation solution.

[104] EFVS Study, CSM – Final Report, 2010, p. 23, 29.

[105] At least there is much uncertainty as regards the application of the Directive's provisions on liability in relation to signature verification services, see EFVS Study, Analysis & Assessment Report, 2009, p. 46.

[106] EFVS Study, Analysis & Assessment Report, 2009, p. 52.

[107] EFVS Study, CSM – Final Report, 2010, p. 24; Analysis & Assessment of the Solutions Report, 2009, p. 52.

[108] EC, Operation of eSignature Directive, 2006, p. 7.

[109] See Chapter 2.1.2.6 above.

[110] EFVS Study, CSM – Final Report, 2010, p. 15f. See however the initiatives listed in Chapter 2.3.2.3.

[111] EFVS Study, CSM – Final Report, 2010, p. 23.

[112] See also Chapter 2.2.3 below.

[113] EFVS Study, CSM – Final Report, 2010, p. 29.

[114] CROBIES Study, 2010, HD, p. 13; Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 105. For example, only the implementation of a different time stamp token for each divergent national regulation could

(5) Beyond this, the current **"mapping" between legal requirements** contained in the eSignature Directive **and the existing technical standards** is considered **insufficient**. Art. 3.5 allows the Commission to establish and publish reference numbers of generally recognised standards for ES products. However, the (rebuttable) presumption of compliance with legal requirements is limited to ES products meeting the standards published for Annex II(f) and Annex III (which have been referenced via Commission Decision 2003/511/EC[115]). Though there are currently more than 30 other European ES standardisation deliverables available which also cover other CSP services than issuing QC, transparent binding legal consequences outside CSP issuing QC or SSCD are missing.[116]

(6) As regards **AES** and other ES which are not based on QC, challenges in practice are even greater, as there are currently more legal, technical and organisational constraints connected to AES than to QES.[117]

Art. 2.2 of the Directive defines **AES** in a generic way, which has led member states to use very diverse technical solutions with different security levels.[118] There are numerous ways to technically implement AES, while the equivalence and levels of AES are unclear.[119] AES do not benefit from a clear legal value or a clear legal distinction from low security implementation.[120] The cross-border acceptance of ES applies only to the qualified level, as Art. 4.2 establishes the free circulation of ES products which comply with the Directive (meaning in practice complying with the requirements for QES as laid down in the Annexes).[121] Member states have more discretion as to which AES solution to accept (or not), depending on the specific requirements of a given application. Moreover, even if an AES fulfills these requirements, the variety of available technical solutions may render the practical acceptance of an AES difficult.[122] Interoperability for non-qualified ES solutions is therefore difficult to achieve, which refrains the use of AES.[123]

Beyond this, the legal qualification of certificates and thus of the **signature type** created with this certificate is currently extremely complicated. From the legal perspective of the Directive, a signature certificate is either qualified or not qualified; likewise, an ES can be either qualified or nonqualified. Therefore, existing key validation solutions use only this distinction and cannot make any judgments on the quality of ES that do not use QC (or on nonqualified certificates). This can be seen as being out of phase with market realities.[124]

Furthermore, the Directive does not provide a conclusive **trust framework for AES**. Art. 3.3 requires only CSP issuing QC to the public to be supervised. Member states may additionally establish voluntary accreditation schemes, which may apply also to CSP providing AES solutions. However, those accreditation schemes, where they exist, differ and are not comparable between member states as they can be freely defined at the national level.[125]

ensure a long term ES equivalent to hand written signature valid in the whole Community, see EFVS Study, CSM – Final Report, 2010, p. 29.

[115] See Chapter 2.3.2.2 below.

[116] CROBIES Study, 2010, HD, p. 14; EFVS Study, CSM – Final Report, 2010, p. 14.

[117] EC, Action Plan on eSignatures and eID, 2008, p. 8.

[118] EC, Action Plan on eSignatures and eID, 2008, p. 8f.

[119] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 106.

[120] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 75.

[121] EC, Action Plan on eSignatures and eID, 2008, p 6.

[122] EC, Action Plan on eSignatures and eID, 2008, p. 8f.

[123] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 106.

[124] EFVS Study, CSM – Final Report, 2010, p. 24.

[125] EFVS Study, CSM – Final Report, 2010, p. 9, 13.

Therefore, the validation of a non-national ES solution (in particular the validation of AES and the necessary assessment of its legal value or security level in a given application) often requires **case-by-case assessment** and treatment of the ES received. Specifically for non-qualified ES solutions where no clear criteria for the determination of security levels exist[126], this is an impossible task from a practical perspective, as it would require application owners to verify the procedures and guarantees for the issuance and management of foreign ES and see if they meet the requirements of their specific applications.

(7) Although the Directive provides a set of requirements for SSCD, there are several **legal uncertainties relating to the conformity assessments** for these devices. Art. 3.4 states that determination of conformity with the requirements in Annex III made by the "Designated Body" of a member state shall be recognised by all member states. However, as the Directive does not contain a direct obligation for member states to designate a suitable body and does not stipulate whether a formal assessment by a Designated Body is mandatory, different types of compliance statements for SSCD recognition have emerged.[127] In particular, it is unclear whether conformity declarations made by other entities are acceptable or must be rejected.[128] Beyond this, due to the different requirements for the certification of SSCD products, it is currently impossible to get a certification which covers all member states.[129] Furthermore, publicly available lists of SSCD benefitting from a determination of conformity are rarely available[130], not harmonised or difficult to find.[131]

(8) Beyond this, the following legal issues affecting in particular **eGovernment applications,** being the largest channel of transactions using ES[132], have been identified:

As a consequence of the principle of subsidiarity[133], ES solutions in eGovernment applications are often designed with a **purely national perspective**. Most member states who have adopted ES in their applications have either not taken into account ES created by signatories from other member states, or do not consider occasional use of the application by users from other member states as a priority. The regulatory, technical and organisational framework is typically organised from a national perspective. In particular in the public sector, member states often require **different types of ES** for similar applications.[134] Typically, national rules regarding the use of an ES application specify that only one or more specific ES solutions are acceptable, which are often available only to users residing within this member state. This practice excludes any other ES solutions regardless of their reliability and security requirements. The design of such solutions is the result of a policy decision which is usually based on valid pragmatic considerations[135], but practically makes ES interoperability impossible.[136] Beyond this, the use of (A)ES typically depends on the reliable identification of the signatory and is thus closely linked to the

[126] Preliminary Study on Mutual Recognition of eSignatures, 2007, p.107.

[127] See Chapter 2.1.2.4 above.

[128] CROBIES Study, WP 4, p. 15; see also EFVS Study, CSM – Final Report, 2010, p. 24.

[129] A product that has passed the certification in a MS will not work in another MS and vice versa ; see Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 76.

[130] Only a few of these bodies provide such publicly available lists, e.g. Austria, France, Germany or Italy.

[131] CROBIES Study, WP 4, p. 20f.

[132] EC, Action Plan on eSignatures and eID, 2008, p. 4f.

[133] Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 104.

[134] EFVS Study, Analysis & Assessment Report, 2009, p. 51; Preliminary Study on Mutual Recognition of eSignatures, p. 103ff.

[135] In particular the non-existence of an interoperable validation and assessment mechanism for non-national ES.

[136] Preliminary Study on Mutual Recognition of eSignatures, 2007, p.109.

national identity management schemes organised by each member state in a completely independent way. Often, solutions require certificates issued by local CSP or even an establishment or a legal representation on the territory of the member states.[137] Some national eGovernment applications accept only ES based on certificates which contain a **specific national** unique number or other **identifier**. The processing of these identifiers is sometimes strictly regulated (e.g. reserved for designated authorities or service providers).[138] It is questionable whether such specific national rules can be interpreted as valid "additional requirements" for ES used in the public sector within the meaning of Art. 3.7 of the eSignature Directive.

Example: the Danish approach[139]**:**

According to a Study from 2007, "only persons with a Danish Central Personal Register (CPR) number can have an OCES[140] personal digital signature, because the registration and identification process is based on a CPR register. For the same reason only companies registered in the Danish central business register can have an OCES employee- and/or company certificate."

Moreover, many member states only accept certificates issued by CSP which are supervised or accredited by their own national body.[141] As this could be construed as "**de facto" requirement equivalent to a prior authorisation**[142], this practice is possibly violating Art. 3.1 of the Directive.[143]

According to a Study which assessed different eGovernment applications in the member states, none of the assessed applications was found to be fully interoperable, as none of them accepted an ES generated by a non-national certificate.[144]

Finally, as the **decentralisation of certain competences** is a legal reality in many member states, usage of ES in eGovernment applications is not only regulated and organised on a national level but often on a regional or local level.[145]

2.2.2 Technical barriers

Also from a technical perspective, the use of different ES leads to interoperability problems which make cross-border use of ES quite complicated at present. In particular, it may be technically impossible to verify a document that is signed in another member state. The main reason for this is the **current lack of common, accepted and actually used standards**[146], which has lead to different technical implementations of the Directive.[147]

[137] Preliminary Study on Mutual Recognition of eSignatures, 2007, p.110; Ramboll Management, 2006, p. 4.

[138] EFVS Study, Analysis & Assessment Report, 2009, p. 50, 52.

[139] Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 37.

[140] See footnote 22.

[141] Preliminary Study on Mutual Recogn. of eSignatures, 2007, p. 93; EFVS Study, Analysis & Assessment Report, 2009, p.52.

[142] EFVS Study, Analysis & Assessment Report, 2009, p. 52.

[143] It could only be regarded as compliant if these restrictions would constitute valid "additional requirements" for ES used in the public sector within the meaning of Art. 3.7 of the Directive. See Study on Mutual Recognition of eSignatures, 2009, p. 95.

[144] See Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 92, 93, 95 for further details.

[145] Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 108.

[146] See inter alia EC, Legal barriers in eBusiness, 2004, p. 8, 15. The Commission issued in 2004 a Working Paper on legal barriers in e-business. The legal problems reported by the consulted enterprises affected all parts of

Standards are necessary to help the stakeholders comply with laws, meet their business needs and convince others that developed solutions are correctly implemented.[148] However, the standardisation work initiated after the adoption of the Directive[149] has resulted in a European ES standardisation framework which is **too complex and not applicable in practice**. In particular, there are too many different standards but still some gaps remain.[150] For ancillary CSP services, an European standardisation framework is entirely missing. Existing standards are not "business practice" oriented but mere "academic standards" that often not reflect the real business and market needs[151], are outdated or even contain mistakes. Beyond this, the standardisation deliverables are not self-explanatory and **sufficient guidelines and implementation samples are missing**. Finally, the standards are not world-wide and not even EN standards, but mere CEN, TR and TS which are easier to issue but have an unclear legal value. [152] For all these reasons, application providers are reluctant to implement the existing standards and rather tend to employ national standards even if existing European standards are known to them.[153]

First of all, signatories in member states currently use **different formats of AES** to sign documents electronically.[154] This creates obstacles for interoperable use of ES if the ES has to be verifiable in multiple member states[155], in particular if the signed documents need to be exchanged from an application to another[156], and also significantly complicates the situation for VSP.[157]

Beyond this, digital certificate implementations in the member states differ and not all CSP use the same extensions and give the same meaning to certificate fields. Therefore, especially at cross-border level, it is **very complicated** in practice **to identify the type of an ES** originating from another member state, in particular to establish whether the signature is an AES, whether it is based on a **QC** and whether the device that was used by the signatory can be considered an **SSCD**, so that the ES can be qualified as a QES.[158] All this information should in principle be retrieved from the ES itself and from the content of the QC. At present, however, it is difficult to obtain this information because of differences in the actual content of QC, varying legal requirements for QC profiles, the use of different standards and practices[159], the wide degree of interpretation of those standards and last

electronic transactions, with a large number related to ES (30%). Many referred to missing standards or technically impracticable solutions for the usage of ES, or the lack of common standards in the area of ES which has resulted in different technical implementations of the Directive.

[147] EC, Legal barriers in eBusiness, 2004, p. 15.

[148] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 94f. and Executive Summary, p. 5.

[149] See Chapter 2.3.2.2 for further details.

[150] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 92ff.; EC, Legal barriers in eBusiness, 2004, p. 8.

[151] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 90ff.

[152] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 92, 93f., 89f.; Ramboll Management, 2006, p. 4.

[153] See however Study on Standardisation Aspects of eSignature, 2007, ExS, p. 5, according to which a majority of the survey respondents stated that they are using EU standards.

[154] See recital (3) of Decision 2011/130/EU.

[155] EFVS Study, CSM – Final Report, 2010, p. 24.

[156] Study on Mutual Recognition of eSignatures, 2009, p. 165; EFVS Study, Analysis & Assessment Report, 2009, p. 50f.

[157] EFVS Study, CSM – Final Report, 2010, p. 24.

[158] EFVS Study, CSM – Final Report, 2010, p. 24; EFVS Study, Analysis & Assessment Report, 2009, p. 50.

[159] EC, Action Plan on eSignatures and eID, 2008, p.7; CROBIES Study, 2010, HD, p. 8; Ramboll Management, 2006, p. 4.

but not least the multitude of formats and algorithms that are in use.[160] All this creates additional burdens for the receiving party, which may have to individually assess each non-national ES.[161]

Likewise, **differences in the semantic interpretation of certificate fields** make it difficult to verify the semantics behind authorisations included in QC[162], e.g. to check whether an ES was created by a person acting on its own behalf or on behalf of a legal entity.

Furthermore, the **incompatible use of national unique identifiers** already mentioned under 2.2.1 also has a technical impact: If the expected identifier is not found in the certificate, applications simply stop their processing and reject the signature request, which clearly impedes cross-border interoperability.[163]

Another issue is that currently not all eGovernment applications support all **types of certificate validation protocols**. While specific standards are available, implementation still differs significantly between VSP across Europe.[164] This can result in the problem that an application supporting only a certain protocol cannot verify the validity of a certificate issued by a CSP which has deployed another protocol.

The existence of a huge number of European CSP using different standards also creates additional **management problems** in particular for VSP, such as the challenges to manage a relationship with all these CSP in order to be able to validate their trustworthiness, and/or the need to maintain specific semantic interpretation of fields for each supported CSP to be able to validate all certificates.[165]

Finally, as regards **eBanking**[166], several barriers for the use of QES by the banks have been identified, in particular in connection with eID cards.[167]

All in all, the existing inappropriate standardisation framework contributes to the current lack of technical interoperability at national and at cross-border level. This has resulted in many "isolated" islands of ES applications where certificates can only be used for one single application.[168] Therefore, the technical framework needs to be significantly rationalised.[169]

2.2.3 Trust related barriers

As a consequence of the existing legal and technical inadequacies of the current European ES framework and the different national practices resulting therefrom, the main obstacles for the cross-border use of ES in practice lie in the **lack of trust in ES** originating from other member states and in the **difficulties linked to validating** these ES.[170]

[160] CROBIES Study, 2010, WP 2-1, p. 5; EFVS Study, CSM – Final Report, 2010, p. 17 and Analysis & Assessment Report, 2009, p. 9.

[161] EC, Action Plan on eSignatures and eID, 2008, p.7; see also CROBIES Study, 2010, HD, p. 8.

[162] EFVS Study, CSM – Final Report, 2010, p. 25; EFVS Study, Analysis & Assessment Report, 2009, p. 49f.

[163] EFVS Study, Analysis & Assessment Report, 2009, p. 50.

[164] EFVS Study, Analysis & Assessment Report, 2009, p. 51; EFVS Study, CSM – Final Report, 2010, p. 25.

[165] EFVS Study, Analysis & Assessment Report, 2009, p. 49, 50.

[166] See above chapter 2.1.3.2.

[167] These include the lack of cross-border PKI interoperability, the lack of control on the issuance of eID cards deployed to the citizens by public authorities and other liability issues and the co-existence of European ES standards and the Banking sector's standards that all need to be followed, see Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 57ff., 60.

[168] EC, Operation of eSignature Directive, 2006, p. 7; Roßnagel, 2008, p. 119.

[169] EFVS Study, CSM – Final Report, 2010, p. 15, 32. See also Chapter 2.4.1.1 below.

[170] EC, Action Plan on eSignatures and eID, 2008, p. 7. This view is shared by CROBIES Study, 2010, HD, p. 7f.

As already stated above[171], in order to validate an ES originating from another member state, a receiving party must not only be able to perform a technical validation of the ES and the certificate, but also needs to assess the "quality", i.e. **the trustworthiness and legal reliability of the ES,** which is currently extremely difficult.[172]

For CSP issuing QC, the Directive has established at least a basic trust infrastructure by defining specific requirements and introducing mandatory supervision at the national level. [173] However, only an effective supervision and the availability of appropriate information on such supervision[174] can ensure reliability of QC and create an adequate level of trust.[175] As regards CSP providing other (ancillary) services to ES, there is currently no trust infrastructure at all.[176] The lack of trustworthiness criteria requires parties who wish to rely on such services to determine the trustworthiness of a CSP based on self-established criteria on a case by case basis, which is a barrier to cross-border interoperability.[177]

Beyond this, member states have adopted radically divergent approaches in terms of security requirements and trust.

Example: Registration for OCES[178]-signature in Denmark

For example, Denmark does not require registration based on in persona appearance for the so-called OCES-signature, which is commonly used in Danish eGovernment applications. The resulting signature is explicitly not considered a qualified electronic signature, so that it is not covered by the Directive's equivalence provisions. Even if this process would meet the Directive's requirements imposed on qualified certificates (and in particular Annex II lit. d), other member states may be reluctant to accept the resulting ES as adequate.[179]

2.2.4 Other practical and commercial issues

Focusing on the existence of interoperability barriers on the cross-border level, it should not be overlooked that already within most member states, ES are still not widely used in all areas.

First of all, **not all contractors accept ES yet.** Therefore, parties will still have to verify with their contractor whether it will accept the presentation of electronic documents signed with ES, and under which conditions.[180]

[171] See above 2.1.3.1 (signature validation services).

[172] Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 106.

[173] EFVS Study, CSM – Final Report, 2010, p. 25.

[174] CROBIES Study, 2010, WP 1, p. 8 f.

[175] The existing supervision schemes also lack effectivity and need improvement, see 2.2.1. The need for information on super-vision has to a certain extent been met by the approach to establish "Trusted Lists" (TL) of CSP (see Chapter 2.3.2.3 for details).

[176] See Chapter 2.2.1.

[177] A receiving party wishing to outsource the validation of an ES received to a VSP must at least assess the trustworthiness of this provider. The VSP, in turn, needs to assess the trustworthiness of all involved CSP used/covered by his service. See EFVS Study, CSM – Final Report, 2010, p. 25f.

[178] See footnote 22.

[179] Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 112.

[180] Without a common infrastructure allowing the counterparty to verify the validity of an ES, contractual parties will refuse to rely on electronic communication, ELDOC Study, 2006, Final Report, p. 61 and p. 65 for credit arrangements with banks.

Beyond this, while widely regulated, **QES are often not used in practice**.[181] Simpler ES solutions with lesser guarantees but affordable security measures are often fully suitable and much cheaper to acquire.[182] The security level of QES is sometimes judged "too high" compared to the real business needs, the costs[183] and efforts to reach such level and the added value compared to AES which also have a legal effect that cannot be denied.[184] Many organisations would therefore like to opt for a lower level of ES for which interoperability is however even more difficult to achieve.[185] Other **reasons for not using ES** are the absence of real business need for the use, the difficulty of implementation and the conviction of the market not being mature enough.[186]

Furthermore, the current **de-facto necessity to engage** a trusted third party (VSP) creates additional issues[187] in terms of costs, time and trust. Beyond this, the **archiving** of electronically signed documents is considered too complex, uncertain and costly[188]; applications providing comprehensive solutions for electronic archives are still rare.[189]

Moreover, there is **no real consistency and mapping between** the existing legal, standardisation and trust **framework**. Beyond this, there is a **lack of information and marketing activities for ES** and a lack of promotion regarding their cross-border use.[190] Users are also often not aware of the risks of unprotected electronic transactions and inadequate electronic evidence.[191]

Finally, a number of **other commercial issues** identified for Germany[192] currently restrains the use of ES:

First of all, a nationwide supply of the population with the **necessary infrastructure** for the use of ES is still missing. The dissemination of signature cards has so far fallen short of expectations.[193]

Beyond this, there is a **lack of attractive ES applications with clearly identifiable benefit** in particular for private users of ES.[194] Presently, ES are virtually not marketed in the private customer segment. The conclusion of online contracts using QES is virtually not offered. Many providers only offer branch-specific ES solutions and target mainly business clients or public authorities as customers.[195]

Costs for the use of ES (in particular QES) are still too high, especially for private users. Their willingness to pay and the current market prices for ES diverge while potential providers of ES applications are not ready to bear the set-up costs for their clients.[196]

[181] See also Ramboll Management, 2006, p. 2.

[182] See also EFVS Study, Analysis & Assessment Report, 2009, p. 40.

[183] The QES level of signature requires a quite costly implementation.

[184] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 75.

[185] See above Chapter 2.2.1.

[186] Study on Standardisation Aspects of eSignature, 2007, ExS, p. 5.

[187] ELDOC Study, 2006, Final Report, p. 85.

[188] Legal obligations to keep documents for as long as over 30 years require costly and cumbersome technology and procedures to ensure readability and verification for such period of time, see EC, Operation of eSignature Directive, 2006, p. 8.

[189] EC, Operation of eSignature Directive, 2006, p. 10.

[190] Roßnagel, 2008, p. 70, for Germany; EFVS Study, CSM – Final Report, 2010, p. 16.

[191] Roßnagel, 2008, p. 71, 81, for Germany.

[192] Though these issues have been identified for Germany, we assume, however, that the situation in other MS is similar.

[193] Roßnagel, 2008, p. 154.

[194] Roßnagel, 2008, p. 60, 63, 67, 71, 85; EC, Operation of eSignature Directive, 2006, p. 10.

[195] Roßnagel, 2008, p. 51, 47, 67, 100.

[196] Roßnagel, 2008, p. 47, 61, 86.

Also, CSP hardly make any competing product and price offers or design introductory offers for private customers to test QES technology.[197] The actual CSP business models put private users at disadvantage, who have to bear the costs for the creation of the ES, while mainly the public authorities or business companies profit by the solution.[198] The cost-benefit ratio for the private user is very low[199], in particular as there is currently no solution available which could be used for all application areas of ES.[200] Providers so far have little incentive to develop multi-application ES and prefer to offer solutions for their own services instead of focusing on interoperability.[201] Unless this is changed, the number of users will remain low. This in turn will restrain other users to join the solution, which then risks to be economically unprofitable and socially unaccepted.[202]

The existence of eGovernment ES applications alone will not sufficiently leverage the use of ES, as individuals generally do not have to consult public authorities very often.[203] Thus additional attractive ES applications are necessary.

2.3. Existing Initiatives to overcome the identified obstacles

In order to overcome the existing obstacles, member states have undertaken own standardisation initiatives or have introduced electronic identity cards with optional electronic signature functionality.

At European level, the Commission has launched different studies and pilot projects including PEPPOL and SPOCS and has undertaken several other initiatives in different sectors to increase interoperability of and enhance trust in electronic signatures. In particular, the Commission has adopted several Decisions addressing specific aspects of electronic signatures, submitted the Standardisation Mandate M/460 to the European Standardisation organisations and announced a revision of the eSignature Directive for 2011.

The issues listed in Chapter 2.2 show that even if most of the basic elements of an European ES framework are currently in place, the situation is quite far from an ideal solution of sound, consistent and efficient frameworks fully supporting the ES market and its stakeholders.[204] In order to overcome the identified obstacles, member states and notably the Commission have initiated a number of initiatives at national and European level.

[197] Roßnagel, 2008, p. 69, 70, 73.

[198] They do not only have an own financial benefit but also profit from the integrity of the document and the authenticity of the signatory caused by the QES and from the fact that they can further process the data electronically. See Roßnagel, 2003, p. 2.

[199] Roßnagel, 2008, p. 65 ff., 72.

[200] Instead, they have to cope with a variety of isolated applications, see already chapter 2.2.2 above.

[201] EC, Operation of eSignature Directive, 2006, p. 10.

[202] Roßnagel, 2003, p. 2.

[203] Insofar, convenience and time saving when using eGovernment services are no relevant aspects, Roßnagel, 2008, p. 64, 88.

[204] EFVS Study, CSM – Final Report, 2010, p. 16.

2.3.1 Initiatives at Member State level

2.3.1.1. National initiatives on the standardisation level

In the recent years, technical standardisation has taken place mainly at national level.

EESSI (European Electronic Signatures Standardisation Initiative) has worked on common interoperability standards[205] but most of the member states have developed national standards for ES in order to promote interoperability.[206] This has often been done by or with the collaboration of national consortia and working groups[207] in which Members exchange their know-how. For example, the Common PKI (formerly "ISIS MTT[208]") specification in **Germany** aims at creating technical interoperability between ES products.[209]

Germany: Common PKI specification

The Common PKI (Public Key Infrastructure) specification describes a profile of standards for ES, encryption and public key infrastructures which is officially recommended by the German Government and supported by the leading German product developers and solution providers for eBusiness and eGovernment.

Common PKI was created by T7.e.V.[210] in cooperation with TeleTrust Deutschland e.V.[211] supported by the German Federal Ministry of Economics and Labour. It is not only accepted in Germany, but more and more attracts interest also on the international level.[212] Also international companies including Microsoft and Entrust have obtained the so-called Common PKI compliance label testifying conformity with the Common PKI specification.[213]

Beyond this, there are also national initiatives facilitating validation and other services. One example is the so-called "European Bridge-CA (EBCA)".[214]

[205] See Chapter 2.3.2.2 below.

[206] EC, Standardisation Mandate M/460, 2009, p. 4.

[207] For example, in Germany, the "Electronic Signature Alliance" (Signaturbündnis), an alliance of providers of infrastructures for ES and encryption and providers of electronic services (eGovernment and eBusiness) created in 2003 by several German Federal Ministries and enterprises has published in 2005 a technical standard building a basis for the interoperability between different ES applications (in particular signature card solutions) independent of the concrete application or manufacturer.

[208] Industrial Signature Interoperability and Mailtrust Specification. The industry standard ISIS stipulates common formats for certificates and for directory services used in connection with services within the scope of the German Digital Signature Act, see www.datev.de/portal/ShowPage.do?pid=dpi&nid=79369

[209] European Commission, Operation of Directive 1999/93/EC on a Community Framework for ES, 2006, p. 7.

[210] *T7 e.V.* is a consortium of TSP and CSP issuing chip cards and certificates for QES founded in 1999. Its tasks are to represent the interests of the German TSP and to foster the possibilities and user-friendliness of QES application, see www.t7ev.org/ueber-t7/ueber-t7.html

[211] *TeleTrusT* is a competence network for the promotion of IT Security and trustworthiness of electronic processes. Founded in 1989, it represents today more than 100 members including manufacturers, research institutes, providers of ES applications, public authorities and users of IT security technology including ES, see www.teletrust.de/en/teletrust/ziele-und-nutzen

[212] The last published version is version 2.0 of 20/01/2009, testbed of 10/01/2011, see www.t7ev.org/index.php?id=44

[213] www.datev.de/portal/ShowPage.do?pid=dpi&nid=79369

[214] The "European Bridge-CA (EBCA)" operated by the German industry association *TeleTrusT Deutschland e.V.* (see footnote 212) connects the PKI of each participating organisation, thereby enabling secure and authenticated communication between enterprises and public authorities. Existing certificates can be used beyond local "identity islands", which allows business processes to span across different organisations. Subject to the conclusion of a

2.3.1.2. eID cards with (optional) electronic signature functionality

In an attempt to increase the uptake of ES, many MS have adopted eCard/eSignature strategies[215] and/or introduced eID[216] cards with (optional) ES functionality which are being promoted through government and private sector initiatives.[217] In October 2009, eleven out of 27 member states were already deploying government supported eID cards.[218] In addition, ten further member states having paper ID cards[219] and 3 of 4 member states who do not issue identity cards at all[220] had announced eID card plans for the future or are already deploying eID cards in the meantime, e.g. Germany.[221] Thus, eID cards have or will become increasingly common in the next few years.[222] Most of the member states deploying eID cards offer several electronic services which the citizens can access.[223] However, e.g in Germany, only 10% of the ID cards are renewed per year which raises fears that the potential signature functionality will diffuse only slowly. Beyond this, the mere issuance of eID cards with optional ES functionality to the mass does not necessarily implicate that this functionality is indeed actively used by the owner. Therefore, attractive applications which increase the demand for eID cards are necessary.[224]

Positive example of eID card: Austrian Citizen Card (Bürgerkarte)[225]

A positive example of an electronic identity card (eID card) is the Austrian Citizen Card, which is based on an open concept as many different supporting media (chip cards such as signature cards, student ID, bank cards, health insurance card, eCard) and also mobile phones[226] can be used as citizen card. It can be assumed that nearly 100% of the population possess at least one such card with signature functionality. This open concept allows also the integration of foreign signature cards, e.g. since February 2006 of Belgian, Estonian, Finnish and Italian ID cards.

single contract with EBCA, its members benefit i.a. from directory and validation services without having to set up agreements with each of the EBCA partners. The independence of the EBCA is guaranteed by a steering committee equally made up of representatives from commerce, administration and science. For more information see www.teletrust.de/en/european-bridge-ca and https://www.bsi.bund.de/ContentBSI/EN/Topics/otherTopics/publickeyinfra/EuropeanBridgeCA/index_htm.html.

[215] For example, the German Government has adopted in 2005 the so-called "eCard strategy" to foster the use of QES. This strategy, technically based on the so-called "eCard API framework", envisages inter alia the introduction of different chip cards including an e-health card, an eID-card (the ePA), an electronic passport and projects such as ELSTER (electronic tax return) and ELENA (jobcard). Further information can be found in Kowalski, Die eCard Strategie der Bundesregierung.

[216] eID gives individuals using electronic procedures the assurance that no unauthorised use is made of their identity and personal data. Likewise, it enables administrations to make sure that the individuals are the persons they claim to be and have the rights that they claim to have (e.g. to receive the requested service), EC, Action Plan on eSignatures and eID, 2008, p. 10.

[217] ELDOC Study, 2006, Final report, p. 10; Study on Standardisation Aspects of eSignature, Final Report, p. 53.

[218] Austria, Luxemburg, the Netherlands, Sweden (issued by private CSP with a public sector mandate); Belgium, Estonia, Finland, Italy, Lithuania, Portugal, Spain (issued by public bodies), Study on eID Interoperability for PEGS, 2009, WP 1, p. 5.

[219] Romania (2011), France (2012), Czech Republic, Hungary, the Netherlands, Cyprus, Malta, Poland, Slovakia, Slovenia.

[220] Ireland, Latvia and the UK – but not Denmark.

[221] Germany is issuing an eID card – the so-called ePA (Elektronischer Personalausweis) since November 2010.

[222] Study on eID Interoperability for PEGS, 2009, WP 1, p. 5.

[223] For more information on such applications see the Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 74ff.

[224] Roßnagel, 2008, p. 153.

[225] www.buergerkarte.at/index_en.html. See already Chapter 2.1.3.2 above.

[226] www.digitales.oesterreich.gv.at/site/6470/default.aspx; Study on Mutual Recognition of eSignatures 2009, p. 43.

Use of the functionality requires a central activation and issuance of a certificate (opt-in solution).[227] Citizen cards therefore constitute not only a secure method for eID, but may also be used to electronically sign documents with QES created with the chipcard or mobile qualified electronic signature created with a mobile phone which is used as citizen card with the same effect as a handwritten signature.[228] The citizen card concept actually covers an increasing multitude of potential application domains[229], in particular applications in the eGovernment sector, access to personal information, secure eBanking and electronic signing and verification of pdf documents; the necessary software is available free of charge.[230]

Positive example: Estonia

In Estonia, since 2005 more than 50% of the population possesses an electronic identity card (eID card) with signature functionality. Since 2003, a cheap ID-Card-Starter-Kit is being offered (card reader and CD with the necessary Software). About 75% of the Estonians handle their banking activities online; nearly 80% also file their tax return electronically. Mobile signatures can be used at relatively low cost. Votes can be cast online at local elections. All in all, Estonia has achieved considerable success with electronic signatures231 and is also one of the few countries where eGovernment services partly support electronic signature solutions from other member states. For example, the Estonian Company Registration Portal is usable also to holders of a Portuguese, Belgian or Finnish ID-card or to holders of a Lithuanian Mobile-ID. Similarly, electronic signatures from an Estonian certification service provider also active in the Lithuanian market are also accepted in some Lithuanian eGovernment applications. These examples show that it is at least conceptually possible for certification service providers to develop their services across several countries. However, it must be noted that these examples relate to neighbouring countries which have certain similarities in their cultural and legal attitudes towards electronic signatures which do not exist between all member states.[232]

2.3.2 Initiatives at European Level

The current EU framework offers horizontal and sectoral instruments to facilitate and enhance the use of ES.[233] In the last years, the Commission[234] has adopted a number of Decisions and undertaken different other initiatives to identify interoperability problems

[227] Roßnagel, 2008, p. 161.

[228] www.digitales.oesterreich.gv.at/site/6476/default.aspx#a12.

[229] Study on Mutual Recognition of eSignatures 2009, p. 33. For further information see www.buergerkarte.at/anwendungen.en.php and www.digitales.oesterreich.gv.at/site/6476/default.aspx and Chapter 2.1.3.2 above.

[230] www.digitales.oesterreich.gv.at/site/6470/default.aspx.

[231] Roßnagel, 2008, p. 162ff.

[232] Study on Mutual Recognition of eSignatures 2008, p. 146, 147.

[233] EC, Action Plan on eSignatures and eID, 2008, p. 3.

[234] DG DIGIT.

related to ES and to improve the interoperability between ES solutions at the European level, building on the legal framework created by the eSignature Directive. These initiatives can be subdivided into general or cross-border initiatives (2.3.2.1), initiatives on the standardisation level (2.3.2.2), on the trust level (2.3.2.3), ITC PSP pilot projects (2.3.2.4) and European sector-specific initiatives relating to ES (2.3.2.5). To gain an overview, the more general initiatives affecting all levels are briefly outlined under 2.3.2.1, while details on specific actions and Commission Decisions affecting a specific level will be given in the relevant subsection below. Finally, for the sake of completeness, we will take a quick glance at initiatives in the eID sector (see below 2.3.2.6).

2.3.2.1. General or cross-level initiatives

The Commission issued in 2004 a **Working Paper on legal barriers in e-business**[235] which illustrated legal problems reported by the consulted enterprises also relating to ES.[236]

In a **Report on the Operation of the eSignature Directive**[237], the Commission concluded in 2006 that its objectives had been largely fulfilled and that no clear need for its revision had emerged. However, the Commission acknowledged problems with the mutual recognition and cross-border interoperability of ES and committed to address the legal, technical and standardisation related causes of these issues.

As regards the **eGovernment** sector, the **IDABC Programme**[238] has been working on identifying, supporting and promoting the development and establishment of pan-European eGovernment services and the underlying interoperable communications networks.[239] Under this programme, the Commission launched the **Study on Mutual Recognition of eSignatures**[240], which analysed the requirements for ES interoperability for different eGovernment applications and services. It consisted of a preliminary study (2007)[241] and of an update of the Country Profiles in October 2009.[242]

In 2008, the Commission issued an **"Action Plan on eSignatures and eIdentification to facilitate the provision of cross-border public services in the Single Market"**.[243] The Action Plan focused on a number of practical, organisational and technical issues causing a lack of cross-border interoperability for ES which in particular affects **eGovernment** services. The Action Plan sets out specific actions on ES and eIdentification, aiming at the creation of a comprehensive and pragmatic framework to achieve interoperable ES and eID in order to simplify access of enterprises and citizens to cross-border electronic public services.[244] It assumed that the cross-border use of QES and AES based on QC could be improved very quickly because of their clear legal status

[235] EC, Legal barriers in eBusiness, 2004.

[236] Regarding the issues reported by the enterprises see already above Chapter 2.2.2.

[237] EC, Operation of eSignature Directive, 2006, p. 9f.

[238] European Community Programme for the **I**nteroperable **D**elivery of pan-European eGovernment services to public **A**dministrations, **B**usinesses and **C**itizens. For a final evaluation of the IDABC programme see Deloitte, 2009.

[239] Study on Mutual Recognition of eSignatures, 2009, p. 19.

[240] EC Action Plan on eSignatures and eID, main undertakings, under 5.

[241] Preliminary Study on Mutual Recognition of eSignatures, 2007. This Study collected and analysed information on ES approaches in eGovernment applications in the MS and determined interoperability barriers and potential solutions.

[242] Study on Mutual Recognition of eSignatures, 2009. These updated Country profiles were published by the Commission in order to improve information on the AES currently being used in eGovernment applications, see EC, Action Plan on eSignatures and eID, 2008, p. 9.

[243] EC, Action Plan on eSignatures and eID, 2008.

[244] EC, Action Plan on eSignatures and eID, 2008, p. 4.

under the Directive and the already existing substantial work in the field of standardisation. Although the Action Plan focused mainly on eGovernment applications, the Commission expected that the means to be put in place could also be used in B2B and B2C transactions[245].

In support of this Action Plan, the Commission launched the **CROBIES Study**[246] to analyse the requirements and establish a general strategy for cross-border use of QES and AES based on QC *within* the existing legal framework set by the Directive.[247] However, the CROBIES study concluded that a recast of the existing legal, standardisation and trust frameworks related to ES, supported by appropriate promotional and educational efforts, is essential to improve interoperability and cross-border use of ES.[248] Nevertheless, it focused in five working packages (WP) also on several "quick-win" actions that could improve some very specific aspects of the interoperability, cross-border use and mutual recognition of QES and AES based on QC *within* the current legal framework.[249] As far as the Study relies on the existing legal framework, its impact is substantial mainly with respect to ES based on QC and less for other types of AES.[250]

In 2010, the Commission released a **Digital Agenda for Europe**[251], being Europe's strategy for a flourishing digital economy by 2020.[252] It consists of seven action areas, two of which relate to eAuthentication and eIdentification. The Commission acknowledged that despite the existing key single market legislation, online transactions are still too complicated and fragmented markets limit the demands for cross-border transactions. Therefore, it announces as a "Key Action 3" under the "1st pillar a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems.[253] In addition, under the 7th pillar, the Commission has requested member states to make eGovernment Services fully interoperable, extend the function of the Points of Single Contact within the meaning of the Services Directive and agree by 2011 on a common list of key cross-border public services that correspond to well defined needs, and to make available these key services online by 2015."[254]

Furthermore, initiated by IDABC[255], the Commission launched the **EFVS Study** to examine the existing issues from the perspective of signature validation at the European level[256] and to assess the legal, operational and technical feasibility of a European scale

[245] EC, Action Plan on eSignatures and eID, 2008, p. 5, 12.

[246] Study on Cross-Border Interoperability of ES (CROBIES Study, 2010).

[247] The study addresses ES operability in general, but specifically in the context of cross-border use. Its objective is to remove barriers to cross-border interoperability of QES and AES based on QC and to prepare the actions required to enhance trust and facilitate the cross-border validation of ES, see EC, Action Plan on eSignatures and eID, 2008, p. 7. For details on the recommendations given by the CROBIES Study see below 2.4.1.1.

[248] CROBIES Study, 2010, HD, p. 8.

[249] For details see CROBIES Study, 2010, HD, p. 9f. and Chapter 2.4.4.1. (2) below.

[250] EFVS Study, CSM – Final Report, 2010, p. 9.

[251] EC, A Digital Agenda for Europe, 2010. The Digital Agenda is one of the seven flagship initiatives of the Europe 2020 Strategy, the EU's growth strategy for the coming decade (see EC, Europe 2020).

[252] See European Commission Information Society, Digital Agenda for Europe. This strategy is set out to define the key enabling role that the use of Information and Communication Technologies (ITC) will have to play if Europe wants to succeed in its ambitions for 2020, see EC, A Digital Agenda for Europe, 2010, p. 3.

[253] EC, A Digital Agenda for Europe, 2010, p. 34, 11 (under the first pillar "A vibrant digital single market).

[254] EC, A Digital Agenda for Europe, 2010, p. 31ff.

[255] See footnote 239.

[256] EFVS Study, CSM – Final Report, 2010, p. 9.

ES verification functionality[257] based on a federated model of national VSP.[258] The Study consists of 3 Reports and 22 solution profiles. The **First report**[259] analysed selected existing ES verification solutions with a focus on AES used in eGovernment applications[260] in order to determine if further European initiatives are necessary to facilitate cross-border verification and to assess whether the reviewed solutions could provide valuable insights on organisational questions or even serve as examples at EU level.[261] The **Second report**[262] examined the consequences and presented proposals for a common European certificate validation solution, an organisational structure and a legal framework. However, the **Final report** of March 2010[263] concluded that in the current environment of missing legal regulations for VSP, inappropriate standards and a trust framework on an ad hoc basis it is virtually impossible to design comprehensive and durable validation solutions with a general EU level impact. Therefore, the Study stated the need for a broader perspective and proposed a comprehensive revision of the existing legal, technical and trust framework.[264]

In 18 February 2011, the Commission has launched a **public consultation on ES and eIdentification**. The consultation seeks feedback on citizens' and businesses' expectations of EU rules on ES, eID and authentication (including additional trustbuilding services), the ICT sector's view on how ES could be tailored to face the forthcoming challenges triggered by technological progress, the common principles to guide the mutual recognition of eID and eAuthentication and the potential contribution of research and innovation to the development of new eID and ES authentication. The results of this consultation which ran until 15 April 2011 will feed into the Commission's review of the eSignature Directive and the preparation of the initiative on the mutual recognition of eID and eAuthentication announced under the Digital Agenda.[265]

Finally, the Commission is also working on an ES Service Infrastructure (**ESSI**) to facilitate the introduction of ES in its own internal and external exchanges.[266]

2.3.2.2. European standardisation initiatives

Following the adoption of the eSignature Directive, standards have been developed by CEN (European Committee for Standardisation) and ETSI (European Telecommunications Standards Institute) within the **EESSI** (European Electronic Signatures Standardisation Initiative).[267] EESSI delivered CWA, TS and TR on a variety of ES related topics.[268]

[257] See www.epractice.eu/en/library/315483.

[258] The creation of such a cross border validation model had also been proposed by the Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 112, as a useful first step to overcome the technical difficulty of validating a certificate.

[259] EFVS Study, Analysis & Assessment Report, 2009.

[260] See EFVS Study, Common Solution Model Report, 2009, p. 9.

[261] Europe's Information Society Thematic Portal, Main undertakings under the Action Plan, under 6.

[262] EFVS Study, Common Solution Model Report, 2009, p. 9f.

[263] EFVS Study, CSM – Final Report, 2010, p. 27.

[264] EFVS Study, CSM – Final Report, 2010, p. 27ff.; EC Action Plan on eSignatures and eID, main undertakings, under 6. Further details on the recommendations of the EFVS Study will be given in Chapter 2.4.4.1 below.

[265] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/198 Regarding this initiative, see below Chapter 2.3.2.6.

[266] EC, Action Plan on eSignatures and eID, 2008, p. 5, footnote 8.

[267] Mandates M 279 in 1998 and M 290 in 1999 to CEN, CENELEC and ETSI in support of a European legal framework for ES (1999 until 2004). For information on EESSI see www.ictsb.org/Working_Groups/EESSI/index.htm.

[268] EC, Standardisation Mandate M/460, 2009, p. 3.

This initiative resulted in a set of legally recognised European standards: Based on the results of the EESSI, the Commission adopted the **Commission Decision 2003/511/EC** which – in accordance with Art. 3.5 of the Directive – established a list of three generally recognised standards for ES products[269] which – when they are complied with – grant presumption of compliance with the requirements laid down in Annex II (f) and Annex III to the Directive.[270] However, these standards are not formal standards in the sense of EN; their value is different from real EN documents and they are often not regarded as real standards by the market.[271] Nevertheless, standardisation work continued and resulted in the existing complex set of ETSI and CEN standardisation deliverables for ES and ancillary services.[272] Meanwhile, these standards have become obsolete and must be updated together with the Decision 2003/511/EC.

As a follow-up to Decision 2003/511/EC, the Commission launched a **Study on the Standardisation Aspects of eSignature** which analysed the use made by enterprises, market players and other stakeholders of the standards referenced by the Decision and other related standards and assessed whether the business model chosen by the Directive is still relevant given the recent technological developments.[273] The Study concluded that the current European set of standards related to ES is too complex to use[274] due to the multiplicity of standards[275], the lack of business orientation and usage guidelines and the difficulty of access, and formulated a number of recommendations to mitigate this.[276]

Likewise, the **Action Plan**[277] adopted by the Commission also announced relevant actions on the standardisation level, in particular to update or possibly extend the Commission Decision 2003/511/EC to other ES products than profiles of QC and of SSCD and to establish guidelines and guidance helping to implement ES in an interoperable way.

Furthermore, also the **CROBIES Study**[278] investigated "quick-win" solutions on the technical level addressing some specific issues regarding cross-border recognition of SSCD (WP 4) and common formats for QC and QES (WP 3).[279]

The Commission also launched the **Study on electronic documents and electronic Delivery**[280] focusing specifically on the availability and use of eDocuments in the context of Art. 8 of the Services Directive. The Study recommended to move towards a consensus between member states on a signature format to be used universally for all authentic eDocuments issued by public administrations, as many member states had indicated that they are reluctant to invest in eDocuments due to the lack of a common approach regarding ES between member states.[281]

[269] (1) Security requirements to be matched by a CSP issuing QC, CWA 14167-1, (2) security requirements for the hardware used by the provider, CWA 14167-2 and (3) security requirements of SSCD used by the signatory, CWA 14169.

[270] EC, Action Plan on eSignatures and eID, 2008, p.8; CROBIES Study, 2010, HD, p. 14.

[271] Study on Standardisation Aspects of eSignature, 2007, ExS, p. 13.

[272] For further details see Chapter 2.2.2 and EC, Standardisation Mandate M/460, 2009, p. 3f.

[273] Study on Standardisation Aspects of eSignature, 2007, ExS, p. 3f. See also Art. 2 of Decision 2003/511/EC.

[274] Study on Standardisation Aspects of eSignature, 2007, ExS, p. 13 f; EC, Standardisation Mandate M/460, 2009, p. 2.

[275] These include established official EU or international standards and less formal consensus specifications, e.g. CWA, TS, TR.

[276] Study on Standardisation Aspects of eSignature, 2007, ExS, p. 17ff. For further details see Chapter 2.4.1.2 below.

[277] EC, Action Plan on eSignatures and eID, 2008, p. 8.

[278] See already Chapter 2.3.2.1 above.

[279] For further details on WP 4 see Chapter 2.4.2 and for further details on WP 3 see Chapter 2.4.1.1.(2) below (footnote **Error! Bookmark not defined.**).

[280] Study on electronic documents and electronic delivery, 2009.

[281] Study on electronic documents and electronic delivery, 2009, p. 23, 28.

To address the issues identified by the aforementioned Studies[282] and based on the input from the CROBIES Study, the Commission has submitted in January 2010 a four-year **Standardisation Mandate M/460**[283] to the European Standardisation Organisations CEN, CENELEC and ETSI. The aim of this mandate is to enhance the current too complex set of standards into a rationalised European ES standardisation framework[284] in order to achieve interoperability of ES at intra-community level. Its main object is to rationalise the existing standardisation framework around the various types of CSP services, the creation and verification of ES and secure user devices[285] and to include helpful implementation guidelines. The tasks to be carried out include quick updates of relevant CWA to enable a rapid update of Decision 2003/511/EC and its possible extension to other ES products in order to address the commitments made in the Action Plan.[286] Work under this mandate has started in 2011 and the rationalised framework is expected to be delivered in 2014.[287]

In addition, the Commission has adopted the **Decision 2011/130/EU** in the context of Art. 8 of the Services Directive. This Directive obliges the member states to ensure that service providers are able to complete electronically and at a distance, through the "Points of Single Contact", all procedures and formalities necessary to provide a service activity.[288] Decision 2011/130/EU therefore stipulates the **use of common signature formats** to ensure that the Points of Single Contact will be able to handle and verify ES from other member states.[289] In particular, it defines a number of AES reference formats that need to be supported technically by the receiving member state in order to allow greater automation and improve the cross-border interoperability of electronic procedures.[290] This Decision which shall apply from 1 August 2011[291] constitutes a further step at European level to facilitate the verification of ES, provided that they are used in documents that service providers may need to submit via the Points of Single Contact.[292]

2.3.2.3. European initiatives in order to overcome the lack of trust

On the trust level, in particular the following European initiatives should be noted:

In order to rule and enhance **trust in the use of SSCD** and on the basis of Art. 3.4 of the Directive, the Commission has, through **Decision 2000/709/EC**, established minimum criteria to which member states must refer to determine how a public or private body can

[282] Study on Standardisation Aspects of eSignature, 2007, and CROBIES Study, 2010.

[283] EC, Standardisation Mandate M/460, 2009, p. 2.

[284] A possible schematic structure of such rationalised framework can be found in EC, Standardisation Mandate M/460, p. 6.

[285] EFVS Study, CSM – Final Report, 2010, p. 36.

[286] EC, Action Plan on eSignatures and eID, 2008, p. 8.

[287] Europe's Information Society Thematic Portal, Main undertakings under the Action Plan, under 2.

[288] This implies the possibility for cross-border identification of service providers and authentication of the data submitted (EC, Action Plan on eSignatures and eID, 2008, p. 3f).

[289] In other words, its objective is to facilitate the verification of ES used in documents signed electronically by competent authorities that service providers may need to submit via the Points of Single Contact, see recital (5) of Decision 2011/130/EU.

[290] Art. 1 provides that the MS shall put in place the necessary technical means allowing them to process electronic documents that service providers submit through the Points of Single Contact as foreseen by Art. 8 of the Services Directive, which are signed by competent authorities of another MS with an XML or a CMS or a PDF AES in specified formats that complies with the technical specifications set out in the Annex. Likewise, the Decision obligates MS whose competent authorities use other ES formats to notify to the Commission existing validation possibilities that allow other MS to easily validate the received ES online, unless the required information is already included in the document, in the ES or in the electronic document carrier. See also www.epractice.eu/en/library/315483.

[291] See recital (2) of Decision 2011/130/EU.

[292] This Decision was considered necessary given the fact that Decision 2009/767/EC facilitating the cross-border use of AES supported by a QC (see below 2.3.2.3) does not deal with formats of ES in documents which have to be submitted electronically.

be designated to determine the conformity of SSCD with the requirements laid down in Annex III.[293] According to this Decision, the "Designated Bodies" are free to establish conformity assessments according to their own criteria but must be transparent in their respective practices and are liable for their activities. However, under this Decision, the question whether SSCD conformity assessments are legally required still remains unclarified.[294]

A major, often mentioned requirement and widely expected step was the **establishment of so-called "Trusted Lists" (TL)** of supervised/accredited CSP. The need for TL comes from the fact that in practice several difficulties[295] linked to the (cross-border) use of QES and AES based on QC still persist and need to be solved, including the lack of trust on ES originating from other member states.[296] The Commission had already announced the creation of a TL of (supervised) qualified CSP at European level as an action under the Action Plan[297] in order to facilitate the validation process of ES based on QC and enhance trust in the cross-border use of ES. Consequently, the **CROBIES Study** presented in WP 2 a "Trusted List" concept for the provision of information on the supervision/accreditation status of CSP services.[298] The realisation of these lists (at least for CSP issuing QC) was finally pushed in the context of the implementation of Art. 8 of the Services Directive[299], being the main driver for their realisation: Based on the input of the CROBIES Study, the Commission adopted **Commission Decision 2009/767/EC** which obligated the member states in particular to establish, maintain and publish, in accordance with the technical specifications set out in the annex, a 'trusted list' (TL) containing the minimum information related to the CSP issuing QC to the public who are supervised/accredited by them. Each list shall be based on a proposed Common Template and shall indicate in particular the relevant services offered and the supervision and/or accreditation status[300] of each CSP issuing QC. The purpose of these TL is to make available the information necessary to validate the ES in a trustworthy form through other means, where this information is not appropriately provided in the certificate.[301] To facilitate access to the TL created by each member state, the Commission has created a compiled central list of links to the national lists.[302]

Decision 2009/767/EC was **updated** by **Commission Decision 2010/425/EU** to facilitate the automated use of TLs[303] and to further enhance trust in them. This Decision, which has applied since 1 December 2010, obligates the member states inter alia to establish and publish not only a human readable but also a machine processable form of their TL[304] in accordance with the specifications set out in the amended Annex, now incorporating inter alia the updated ETSI standards on TL.[305]

[293] In particular, the Decision stipulates that "Designated Bodies" must be sufficiently competent, personally and financially independent and not involved in the design, construction, marketing, maintenance of SSCD nor be a CSP. Likewise, the impartiality of their staff must be guaranteed and appropriate insurances obtained to cover its liabilities.

[294] CROBIES Study, WP 4, p. 11ff., 14. See already Chapter 2.2.1. above.

[295] See in particular Chapter 2.2.2 above.

[296] CROBIES Study, WP 2-1, p. 5.

[297] EC, Action Plan on eSignatures and eID, 2008, p. 8. See also already Chapter 2.3.2.1 above.

[298] CROBIES Study, 2010, HD, p. 10; CROBIES Study, 2010, WP 2-1, p. 5.

[299] Directive 2006/123/EC. The relevant obligations introduced by the Services Directive are briefly outlined in Chapter 2.3.2.2.

[300] A service is currently either supervised or accredited; beyond this, a supervision or accreditation status can be 'ongoing', 'in cessation', 'ceased', or even 'revoked'.

[301] CROBIES Study, WP 2-1, p. 5. See also recital (4) of Commission Decision 2009/767/EC.

[302] Europe's Information Society Thematic Portal, Main undertakings under the Action Plan, under 3.

[303] Decision 2009/767/EC obligated the MS only to publish at least a *human readable* form of their trusted list.

[304] Machine processable forms of TL must be signed electronically, see Art. 2 a of Decision 2009/767/EC as amended by Decision 2010/425/EU.

[305] TS102 231 (Provision of harmonised trust-service status information), updated in 2009, defining the technicalities of the common template for national "TL", see also EC Action Plan on eSignatures and eID, main undertakings, under 3.

However, the existing TLs currently **cover only CSP issuing QC** and therefore their benefit is limited to the facilitation of the validation of QES and AES based on QC. Insofar, a relying party can now determine the trustworthiness of the CSP by checking his supervision/accreditation status.[306] It is therefore assumed[307] that (at least) for issuers of QC, the European ES framework offers a suitable basis for building trust. This is however questionable as the basic information about the supervision/accreditation status does not, in our view, necessarily allow for an assessment of the quality of the (actual) performance of the supervision/accreditation in the respective member state and thus of the quality of the ES.

2.3.2.4. ITC pilots relating to electronic signatures – PEPPOL and SPOCS

Beyond this, the Commission and several member states have launched different pilot projects[308] as part of the ICT PSP Programme.[309]

For example, a federated approach to cross-border validation of ES is currently tested within **PEPPOL**[310], a large-scale cross-border eProcurement pilot project launched in 2008. From the general perspective of an ES user, the most interesting part of PEPPOL is its WP 1, which aims at a European interoperability of ES, in particular regarding the verification process.[311] In order to avoid multiple validation efforts in all member states which are the main obstacle to cross-border interoperability, it may be an option to delegate verification tasks to a centralised or distributed validation service mechanism.[312] WP 1 of PEPPOL addresses a specific cross-border ES validation tool or, to be more precise, a validation infrastructure for eProcurement applications. Inter alia, this infrastructure provides the receiver of signed documents a service to validate the signature certificates of digital signed data against configured CSP[313] whereas the sender can sign these documents with his national ES solutions. The validation service will be integrated in some national applications.[314] The project is currently in the roll-out phase (until 10/2011).[315] Although the EFVS Study did not preselect PEPPOL as a key solution because it operated as a mere pilot project without a functioning implementation at that time and was unlikely to implement a definitive liability model[316], the results of EFVS study should also feed into a further optimisation of PEPPOL.

The second large-scale Pilot is the **SPOCS**[317] Project launched in May 2009.[318] It aims at improving the competitiveness of European businesses and particularly small and medium-sized enterprises by enabling national and European businesses to benefit from available,

[306] EFVS Study, CSM – Final Report, 2010, p. 25.

[307] See e.g. EFVS Study, Analysis & Assessment Report, 2009, p. 40.

[308] PEPPOL – see below (1), SPOCS – see below (2) and STORK, which will be outlined further below, see Chapter (2.3.2.6).

[309] Information Communication Technologies Policy Support Programme, which is part of the competitiveness and Innovation Framework Programme (CIP), http://ec.europa.eu/cip. See also EC, Action Plan on eSignatures and eID, 2008, p. 9.

[310] **P**an-European **P**ublic **P**rocurement **O**n**L**ine, www.peppol.eu

[311] PEPPOL website, www.peppol.eu/work_in_progress/wp-1-esignature/current-status.

[312] EC, Action Plan on eSignatures and eID, 2008, p. 8f., which announced as an action the Creation of an European federated validation service, subject to the results of the EFVS feasibility study.

[313] PEPPOL website: www.peppol.eu/work_in_progress/wp-1-esignature/results/signature-validation-infrastructure-online.

[314] PEPPOL website, www.peppol.eu/work_in_progress/wp-1-esignature/current-status.

[315] PEPPOL website, www.peppol.eu/work_in_progress/wp-1-esignature/project-plan.

[316] EFVS Study, Analysis & Assessment Report, 2009, p. 15.

[317] **S**imple **P**rocedures **O**nline for **C**ross-border **S**ervices, www.eu-spocs.eu .

[318] This project has also been set up on the basis of the 2008 CIP ICT PSP Programme of Work.

efficient and interoperable electronic procedures. SPOCS is expected to build the next generation Points of Single Contact within the meaning of the Services Directive for businesses across Europe. It will provide seamless electronic procedures by building cross border interoperability based on existing systems and solutions. The project has presented several deliverables on specifications of a European interoperability layer for eGovernment services which are currently undergoing review from the European Commission.[319]

2.3.2.5. European sector-specific initiatives relating to electronic signatures

European work on ES and eID is particularly relevant in judicial matters, where the authentication of acts is essential.[320] Therefore, the Council of Bars and Law Societies of Europe (**CCBE**)[321] seeks to assist the development of a safe and practical electronic environment for legal professionals throughout Europe. In order to enable interoperable eCommunication for lawyers, CCBE has proposed a **European Framework System for electronic ID cards for lawyers**[322] with possibly optional ES functionality. With this system, the CCBE aims at supporting its member bars in the implementation of electronic ID card schemes and – at the same time – to make these schemes interoperable for lawyers throughout Europe.

Beyond this, an important step has been the adoption of the **Council eJustice Action Plan 2009-2013**[323] in November 2008 which aims at developing the use of information and communication technologies (ICT) at EU level in the field of justice. The plan stated that one of the essential conditions for the effective use of eJustice across national borders is the development of uniform standards or interfaces for the use of authentication technologies and the components of ES. It proposed to continue the examination of the various legal requirements and technologies used in the member states with the final aim of introducing a secure electronic exchange of documents between member states.[324]

Beyond this, several harmonisation initiatives in other specific sectors have been undertaken on the EU level, namely through the **EU Directives** on **eInvoicing**[325] and **eProcurement**[326], which have been or will be addressed in other chapters of this Study.

2.3.2.6. European Initiatives in the field of eID

In parallel to the initiatives regarding ES there are also several European initiatives in the field of eID[327], which are however outside the scope of this Study and will thus only be

[319] www.eu-spocs.eu/index.php?option=com_content&view=article&id=53&Itemid=76.

[320] Council, European eJustice Action Plan, recital 13.

[321] www.ccbe.org. The CCBE represents more than 700,000 European lawyers through its member bars and law societies of the EU and the EEA.

[322] www.ccbe.org/fileadmin/user_upload/NTCdocument/en_guidelines_framew1_1192450932.pdf.

[323] Council, European eJustice Action Plan, recital 1.

[324] Council, European eJustice Action Plan, recital 28. As a first step, the Action Plan announced the establishment of the European eJustice portal (see recital 1) which will provide access to the whole European e-Justice system, i.e. to European and national information websites and/or services. A basic version of this portal is now online (https://e-justice.europa.eu/home.do).

[325] See Chapter 2.1.3.2 above.

[326] See Chapter 3. below.

[327] As stated in 2.3.1.2 and 2.1.3.2, most MS already have eID systems in place for access to the electronic procedures of their public administrations. However, the technical means have been deployed without coordination between MS and therefore vary greatly, even if the trend today is towards the use of eID cards.

outlined briefly. With regard to cross-border eIdentification, there is still no Community instrument on which action at Community level could be based.[328]

The **i2010 eGovernment Action Plan**[329] and the **Action Plan**[330] consider interoperable electronic identity management (eIDM) as a prerequisite for cross-border access to public services. As in the case of ES, a horizontal solution is sought on which sectoral applications can rely and which would be based on mutual acceptance of each other's eIdentification mechanisms.[331] CEN has developed some standards for eID[332] which will probably be unavoidable for any EU cards schemes, but lack a serious concept of privacy and are therefore criticized.[333] Nevertheless, harmonisation initiatives continue and certainly appear to be promising.[334]

The Commission has launched a study on **eID interoperability for Pan-European eGovernment Services (PEGS)**[335] to keep up with developments in the use of eID in the member states; updated country **profiles** have been published in 2009.

Beyond this, the Commission is supporting a large scale ITC **pilot project named "STORK"**[336] to enable cross-border recognition of eID systems and easy access to public services in 18 European countries. By 2012, member states are invited to demonstrate solutions for the cross-border use of eID in the STORK pilot project. Depending on the results, the Commission will determine if and what additional actions might be required to enable an effective EU wide use of eID.[337] Complementary to and in support of this project, the Commission has announced to launch specific surveys on the use of eID in member states.

Finally, in the **Digital Agenda**[338], the Commission has also announced its intention to propose by 2012 a Council and Parliament Decision to ensure mutual recognition of eID and eAuthentication across the EU based on online 'authentication services' to be offered in all member states, and to support seamless cross-border eGovernment services in the single market through the CIP[339] and ISA[340] Programmes.

[328] EC, Action Plan on eSignatures and eID, 2008, p. 5.

[329] EC, i2010 eGovernment Action Plan.

[330] EC, Action Plan on eSignatures and eID, 2008, p. 10, 5.

[331] EC, Action Plan on eSignatures and eID, 2008, p. 10f.

[332] These include CWA (CEN Workshop Agreement) 15480 and CWA 15264-1.

[333] Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 54f.

[334] ELDOC Study, 2003, Final Report, p. 61.

[335] Study on eID Interoperability for PEGS, 2009.

[336] **S**ecure iden**T**ity acr**O**ss bo**R**ders lin**K**ed. The STORK pilot project (https://www.eid-stork.eu) aims to enable EU citizens to prove their identity and use national electronic eID systems (passwords, ID cards, mobile phones and others) throughout the EU, not just in their home country, see http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/198. The project considers a model of interoperable electronic identity mutually recognised in all MS, but allowing MS to keep their systems and practices in place (EC, Action Plan on eSignatures and eID, 2008, p. 11). In October 2010, 6 STORK pilot projects intending to offer secure cross-border eID services have been started. The specific areas are: cross-border authentication platform for electronic services, student mobility, change of address, electronic delivery of documents, safe use of internet by children. In 2008, 13 MS were involved plus Iceland, the project has 29 participants in total (private and public).

[337] EC, Action Plan on eSignatures and eID, 2008, p. 10ff.

[338] See EC, A Digital Agenda for Europe, p. 32 (seventh pillar).

[339] Competitiveness and Innovation Programme.

[340] Interoperability Solutions for European Public Administrations.

2.4. Proposed further actions

As most of the above-mentioned challenges continue to exist, two main strategies to improve interoperability and cross-border use of electronic signatures have been proposed:

- *A **large-scale approach** envisaging a comprehensive revision and extension of the eSignature Directive to all types of electronic signatures, the full range of related products and all types of certification services (including services ancillary to or using electronic signatures and identification and authentication services which are currently not regulated by the Directive). This should be accompanied by a respective recast of the existing standardisation and trust framework and appropriate promotional efforts.*
- *A **small-scale approach** intending to improve the Directive's business model without amending the Directive, but by referencing more standards via Commission Decisions. Instead of risking a difficult revision process, a non-binding Commission Document could help to support a common interpretation of the Directive and to clarify specific issues.*

Beyond this, other actions and supportive measures for electronic signatures including financial incentives have been proposed to stimulate the use of electronic signatures.

The adoption of the eSignature Directive had raised expectations that this legislation would provide a platform of trust in ES and related services in order to help the market for ES to take off.[341] However, while the Directive has introduced legal certainty with respect to the general admissibility of ES and their legal recognition[342], the market for ES has not developed as expected. This is mainly due to the above-mentioned challenges which may continue to cause a detrimental effect to a successful implementation of the Directive's primary objectives of promoting cross-border legal recognition of ES as well as ensuring a free circulation within the internal market of ES supporting products, equipments and services. Therefore, further action is necessary in order to address and overcome the existing obstacles. In this Chapter 2.4, we will outline the main existing proposals for further steps to create an ES system that works at European level, to improve the interoperability of ES and to facilitate their (cross-border) use.

2.4.1 Basic approaches recommended by existing Studies

Against the background of the insight that the current scope of the eSignature Directive and the present technical and trust framework does not meet the requirements and expectations of the present market, mainly the following two different strategies to improve interoperability of ES and facilitate their cross-border use are being discussed: a large-scale approach (including a comprehensive review of the eSignature Directive and its extension to ancillary and eID services, see 2.4.1.1) and a small-scale approach (proposing enhancements on the basis of the existing legal framework without seeing a fundamental need to amend the Directive, see 2.4.1.2).

[341] EC, Operation of eSignature Directive, 2006, p. 4f.

[342] EC, Operation of eSignature Directive, 2006, p. 9.

2.4.1.1 Large-scale approach: Comprehensive revision of the eSignature Directive

The first proposed strategy envisages a large-scale approach, meaning a comprehensive revision of the Directive combined with the ongoing standardisation work under the Mandate M/460[343] and further enhancements on the trust level, supported by appropriate promotional and educational efforts.[344] This approach has mainly been proposed by the recent **CROBIES**[345] and **EFVS**[346] **Studies**, which determined that a number of existing challenges cannot be resolved under the present legal, technical and trust ES framework as they are simply not under the scope of the current Directive.[347]

Therefore, the Studies concluded that improving interoperability and cross-border use of ES will only come to reality through a recast of the existing legal, standardisation and trust framework related to ES into a common broader, more comprehensive and fully consistent framework covering all types of CSP services and even fully addressing the identification, authentication and signature policy issues.[348] In their view, the establishment of such framework is a key success factor to convince the market and business stakeholders of the possible successful implementation of ES and an essential action to enhance mutual recognition and facilitate interoperability and (cross-border) use of ES beyond QES and AES based on QC and of eID and authentication services.[349] However, the Studies acknowledge the numerous positive aspects of the existing legal, technical and trust framework, in particular of the eSignature Directive[350], its national transpositions, the existing standardisation work and the national trust infrastructure at least for the use of certain types of ES.[351] Therefore, they do not propose to rebuild the framework from scratch or to replace it in a "big bang" action, but to fill in the existing blanks in a stepwise approach.[352]

(1) Legal framework

With regard to the legal framework, the EFVS and CROBIES Studies recommend extending the scope of the eSignature Directive and to recast it into a newer version that covers all types of ES, the whole range of products and services related to ES and applies to all types of CSP services, not limited to the issuance and management of QC to the public (as is currently the case).[353] In particular, they recommend to integrate specific requirements on the provision of other CSP services, focusing on key services ancillary to ES (including time-stamping, (long term) archiving, signature validation and signature policy issuance and their component services), but also encompassing services applying ES like e.g. electronic registered mail services, as well as identification and authentication services.[354]

[343] See above Chapter 2.3.2.2.

[344] CROBIES Study, 2010, HD, p. 8.

[345] CROBIES Study, 2010.

[346] EFVS Study, 2010.

[347] EFVS Study, CSM – Final Report, 2010, p. 27f.

[348] EFVS Study, CSM – Final Report, 2010, p. 3, 8, 16, 27.

[349] EFVS Study, CSM – Final Report, 2010, p. 11f., 29, 37.

[350] Recognised strengths are i.a. the principle of technological neutrality, a clear legal value for QES, the flexible standardisation approach to determine technical details outside of the Directive and give them legal value through a Commission Decision, the supervision and voluntary accreditation mechanisms and the liability rules, EFVS Study, CSM – Final Report, 2010, p. 13f., 30.

[351] Insofar, the Study considers the eSignature Directive as a "conceptually sound basic approach".

[352] EFVS Study, CSM – Final Report, 2010, p. 16.

[353] See Chapter 2.2.1.

[354] See CROBIES Study, 2010, HD, p. 16; EFVS Study, CSM – Final Report, 2010, p. 27ff. The EFVS Study takes the view that the EU could regulate this, since it is clearly an internal market issue: the current lack/inadequacies

The EFVS Study thus talks of a *"TSP Directive on a Community framework for electronic identification(ties), authentication and signatures (IAS)"*.[355]

The Studies recommend structuring the revised Directive around three main pillars:[356]

(i) a Common Section[357] acting as a general frame applicable to any CSP service, including

- definitions of the concept of a CSP service and of the specific CSP services to be covered[358],
- application of the principle of differentiation between qualified services (with a specific legal value) and non-qualified services (benefitting of non-discrimination rules) which the Directive stipulates only for ES to all CSP services, while encouraging also the definition of levels of other AES than QES[359],
- rules on supervision and voluntary accreditation, establishing obligatory supervision for all qualified services, while supervision must and accreditation may follow EU standards to ensure interoperability,
- an extension of Art. 3.5 of the Directive to enable the adoption of standards for all services via Commission Decisions, and
- General internal market rules; and

(ii) a Service specific section defining in particular

- the characteristics and requirements of each specific type of service in specific subsections, including definition of security/quality/policy levels and criteria associated to those services and the results (outputs) of those services,
- the specific legal effect and value (e.g. legal presumption) of the respective qualified service and its output, and
- the liability and internal market rules for each specific service (if they differ from the Common Section).[360]

(iii) Technical details such as the specific quality requirements which are reliant on standardisation should – like in the present version – however be addressed outside of the Directive, via Commission Decisions extending or replacing Decision 2003/511/EC.[361]

(2) Technical Framework

On the technical level, the CROBIES and EFVS Studies recommend creating a sound and stable standardisation framework, likewise covering the full range of ES and related products and services, and CSP services in the broader sense through international and

of the existing framework is causing market disruptions which would be hard to address conclusively without further European intervention (see p. 28).

[355] EFVS Study, CSM – Final Report, 2010, p. 34.

[356] EFVS Study, CSM – Final Report, 2010, p. 30ff.; CROBIES Study, 2010, HD, p. 17. For more details on the content and steps to tackle this revision see EFVS Study, CSM – Final Report, 2010, p. 30ff., 34 ff.; CROBIES Study, 2010, HD, p. 17, 19f.

[357] EFVS Study, CSM – Final Report, 2010, p. 30ff., 34 ff.; CROBIES Study, 2010, HD, p. 17, 19f.

[358] These include issuance of certificates, time-stamping, electronic archiving, validation, signature policy issuance, identification and authentication services and their component services, see EFVS Study, CSM – Final Report, 2010, p. 19f.

[359] The EFVS Study encourages also the definition of levels of other AES and associated security/quality/policy levels for the supporting digital certificates (without giving them equivalence to handwritten signatures, but to help relying parties to determine the reliability and acceptability of these ES for their purposes), EFVS Study, CSM – Final Report, 2010, p. 29, 31.

[360] For the proposed definitions of validation and validation authority see EFVS Study, CSM – Final Report, 2010, p. 30ff., 35ff.

[361] EFVS Study, CSM – Final Report, 2010, p. 31, 35.

recognised standards and including guidance and implementation guidelines.[362] In particular, they recommend to create **rationalised, generally recognised European ES standards (EESS)** in order to overcome the existing complex, outdated, incomplete, inaccurate and therefore inappropriate standardisation framework. This task is already being addressed under the Mandate M/460.[363] The EFVS Study recommends however that the Commission should further interact with the relevant standardisation bodies and make them aware of the broader perspective during their work. The Commission should also liaise with existing service providers regarding possible implementation measures on their side, and make sure that these efforts will support a recast legal framework as described above. The resulting EESS should be organised around three main cornerstones: the technical specifications (including policy requirements), the Conformity Assessment Guidance (on the basis of which supervision and accreditation system can be built), and the Implementation Support (aiming to facilitate their use by stakeholders).[364]

In addition, the clear mapping between functional legal requirements ruled by the Directive and the generally recognised standards created under Mandate M/460 should be ensured by Commission Decisions granting legal compliance for those ES products and services which are meeting the relevant requirements, in continuation of the existing approach of the eSignature Directive. This should be combined with clear Conformity Assessment Guidance to assess the compliance of such services to the relevant requirements.[365]

The **EFVS**[366] **and CROBIES Studies** recommend that in particular the following specific standardisation actions ("quick-win-tracks"[367]) should be part of the standardisation approach driven by Mandate M/460:

- Common definitions, specifications and policy requirements of the identification, authentication and ES and CSP products and services and of the various types and variants under which they may be operated;
- Commonly defined identification elements (e.g. subtype identifiers);
- Establishment of quality criteria for certificates, ES and other trust service tokens;[368]
- A rationalised profile for QC and non-QC;[369]
- A common identification profile for signatories and certificate holders. Improvement in the provision and registration policy requirements on certificate's subject identity is addressed in the **STORK** pilot and other studies and initiatives on this topic[370];

[362] CROBIES Study, 2010, HD, p. 16, 18, 20ff; EFVS Study, CSM – Final Report, 2010, p. 32f., 36f.

[363] See Chapter 2.3.2.2 above. For further details on the proposed architecture of the rationalised European ES standardisation frameworks see Mandate M/460, p. 6ff. and EFVS Study, CSM – Final Report, 2010, p. 32.

[364] EFVS Study, CSM – Final Report, 2010, p. 32, 36f., 39.

[365] EFVS Study, CSM – Final Report, 2010, p. 31f., 35.

[366] EFVS Study, CSM – Final Report, 2010, p. 32f., 36f.

[367] **CROBIES WP 5-1** addressing mainly standardisation and trust issues were meant to be "quick win" actions within the existing legal framework. However, great part of them is now being addressed (or at least recommended to be addressed) within Mandate M/460 and thus also part of the "large-scale approach" to establish a recast legal, standardisation and trust framework.

[368] In this context, **CROBIES WP 5-2** has proposed a Quality Classification Scheme for ES elements identifying a set of quality levels for major ES elements (signing device, certificate provision, cryptographic suite, ES application and independant assurance) with the aim to support ES stakeholders in specifying requirements on the quality of an ES implementation (e.g. in a signature policy context), to be considered for potential standardisation under Mandate M/460, see CROBIES Study, WP 5-2.

[369] In order to address the issues relating to differing contents of QC, varying legal requirements for QC profiles and use of different standards and the validation difficulties resulting from these (see Chapter 2.2.2), the **CROBIES WP 3** has proposed an interoperable QC profile by stipulating common minimum requirements and data to be contained in a QC. The Study recommends that this proposal should be taken into account in the context of the execution of Mandate M/460, in order to create a clear set of consistent and complete requirements related to certificate profiles, see CROBIES Study, WP 3, p. 10ff., 16.

- The formalisation of common policy requirements, building on previous ETSI initiatives. In particular, the recast of the ES standardisation framework for ES should also ensure a consistent approach with regard to requirements on algorithms and parameters eligible for ES.[371]
- Harmonised protocols (interface, access and input/output) for communication of TSP;
- Mapping of different certificate profiles against a European Standard[372], and
- A better coverage of all types of (secure) user devices.

Beyond this, the CROBIES Study has delivered in **WP 5-1** a draft proposal for guidelines and guidance for cross-border and interoperable implementation of ES. Recognising the need for such guidance[373], the Commission has determined that such implementation guidelines shall be part of the rationalised European ES standardisation framework and has forwarded the document to the ESOs[374] for consideration.[375]

(3) Trust Framework

Beyond this, the **EFVS**[376] and **CROBIES**[377] Studies recommend the creation of a sound and stable Trust Framework for the provision of all types of CSP services and the practical implementation of ES, e.g. through appropriate supervision, voluntary accreditation and certification of ES products and applications. In particular, they propose

- to extend the current model of supervision/voluntary accreditation schemes also to CSP providing other services using ES or ancillary to ES (on national basis or through private or sector specific initiatives), and to implement guidelines for service providers to streamline and facilitate supervision/accreditation process;[378]
- to extend/create and publish TL[379] for such other services or products containing information on the status of supervision and/or accreditation.[380] This could include the creation of further TL at the national level by supervisory and accreditation bodies, but also the creation of sector specific TL by other bodies including private sector parties, allowing relying parties to easily determine when a TSP respects a consistent set of requirements;[381] and
- to define appropriate conformity assessment guidance schemes and possibly also common EU level accreditation schemes.[382]

[370] CROBIES Study, WP 3, p. 4. For further details see the STORK pilot (referenced in Chapter 2.3.2.6 above).

[371] CROBIES Study, WP 5-3, p. 6. **CROBIES WP 5-3** proposes to maintain, establish, update, standardise and correctly reference so-called European "Algo lists" (meaning lists of algorithms and parameters eligible for ES serving as a valuable guidance tool). Such an "Algo" list already exists as a result of an ETSI initiative but there are uncertainties regarding its use, see CROBIES Study, WP 5-3, p. 3ff., 6ff. for details.

[372] EFVS Study, CSM – Final Report, 2010, p. 36f.

[373] EC, Action Plan on eSignatures and eID, 2008, p. 8; EC Action Plan on eSignatures and eID, main undertakings, under 4.

[374] European Standardisation Organisations.

[375] EC Action Plan on eSignatures and eID, main undertakings, under 4.

[376] EFVS Study, CSM – Final Report, 2010, p. 33, 37, 39.

[377] CROBIES Study, 2010, HD, p. 18f.

[378] **CROBIES WP 1** proposes a common model for supervision and accreditation of CSP issuing QC (which can be extended to other services ancillary to ES), see CROBIES Study, 2010, HD, p. 24f. and WP 1, p. 4 ff.

[379] With regard to Trusted Lists (TL) see above Chapter 2.3.2.3.

[380] The CROBIES and the EFVS Studies take the view that the existing national TL of supervised/accredited CAs (to the establishment of which the **CROBIES WP 2** had significantly contributed) should constitute a highly useful resource in addressing the issue that the identification of QES (in particular, the identification whether the ES received is based on QC and whether it has been created using a SSDC) is very complicated in practice, see EFVS Study, CSM – Final Report, 2010, p. 24.

[381] EFVS Study, CSM – Final Report, 2010, p. 18f.

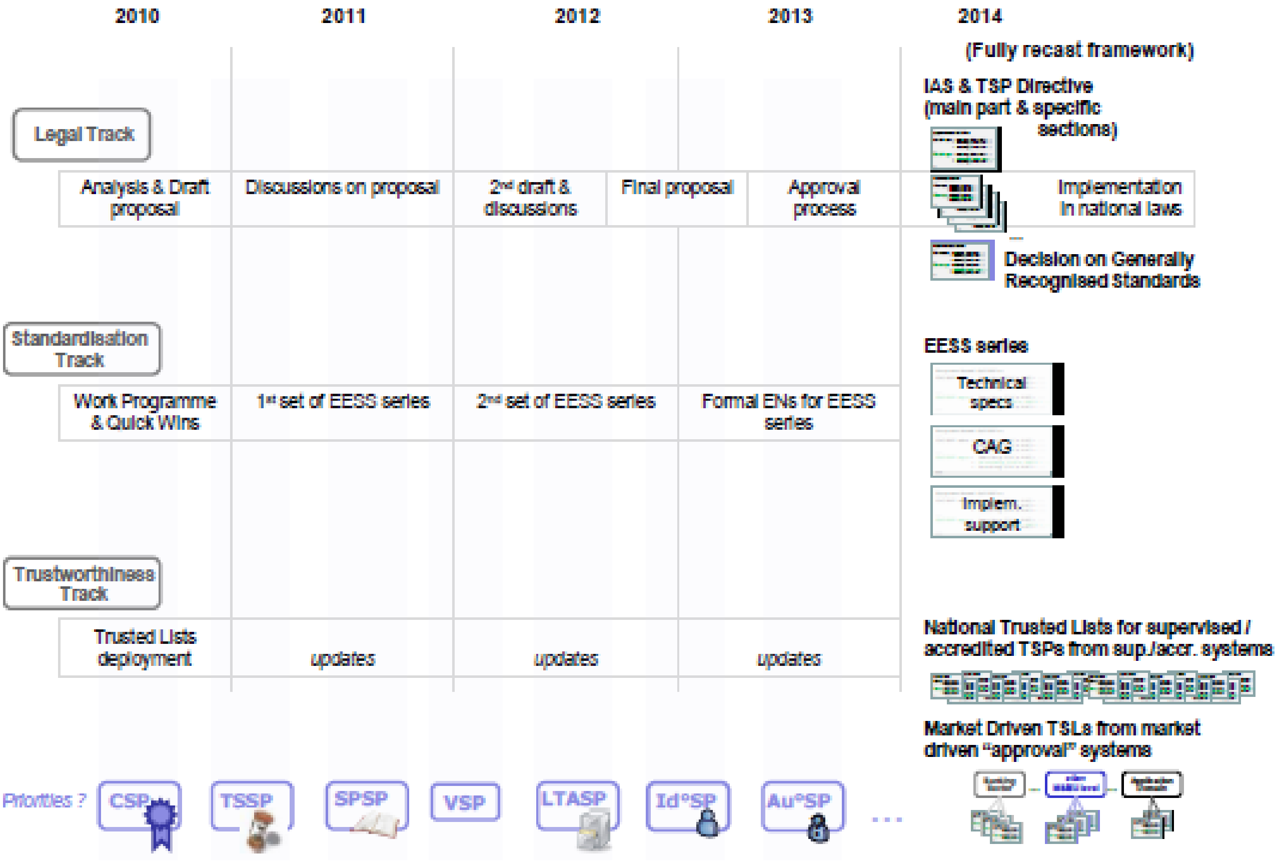
[382] EFVS Study, CSM – Final Report, 2010, p. 33.

(4) Proposed Roadmap

The Studies take the view that the envisaged framework, i.e.

- the revised "IAS & TSP Directive" covering also the legal aspects of ancillary services,
- the implementation of EESS series to allow interoperability, and
- the provision of the receiving party with the necessary trust service status information on CSP that are supervised or accredited at a national level through national TL and/or TL from market driven "approval" schemes)[383]

would be capable of handling the current ES validation challenges[384] and could create a real added value in other areas as well.[385] They expect to have a fully recast legal, technical and trust framework by 2014 (see the figure below). This might not be realistic though as the Commission will issue a draft proposal for a recast Directive at the earliest in 2011.[386]



Soruce: Figure copied from EFVS and CROBIES Study[387]

[383] EFVS Study, CSM – Final Report, 2010, p. 38.

[384] CROBIES Study, 2010, HD, p. 8.

[385] EFVS Study, CSM – Final Report, 2010, p. 27; CROBIES Study, 2010, HD, p. 8.

[386] The timeline appears all the more strict as the EFVS-Study recommends to collect and analyse MS national inputs on the draft proposals (involving local legal experts, MS regulatory bodies, MS national supervisory, accreditation and IT security bodies as well as other key stakeholders (e.g. academics, industry, CIP pilots, etc.), in order to prepare an updated draft proposal, see , Common Solution Model – Final Report, 2010, p. 36.

[387] EFVS Study, CSM – Final Report, 2010, p. 38 (Figure 4); CROBIES Study, 2010, HD, p. 30 (Figure 8).

2.4.1.2 Small-scale approach: No revision of the eSignature Directive

In contrast, the second proposed approach to address the existing challenges is a small-scale approach which disapproves of a revision of the eSignature Directive as such. This approach has inter alia been proposed by the **Study on the Standardisation Aspects of eSignature**[388], whose authors see clear possibilities to significantly improve the Directive's business model and its success without amending the Directive.

More precisely, the authors expressly opted against the incorporation of specific internal market rules for other (ancillary) certification services such as archival or time stamping services into the Directive and do not see a necessity to extend the legal compliance presumption of Art. 3.5 to other requirements than Annex II (f) and Annex III. In their view, opening the Directive for review would trigger cumbersome and time consuming procedures and would risk the re-opening of lengthy discussions between the member states on the issue of authentication and ES as well as a perturbation of the market due to the changes and time to reassess existing products.[389] As the Study had come to the conclusion that the Directive's business model linking the publication of some standards to a legal presumption of conformity with some legal requirements has reasonably well functioned for those standardisation deliverables that have been referenced by Decision 2003/511/EC, the authors recommended instead that this business model should be fully implemented and expanded.[390] However, the Study acknowledges that without amending Art. 3.5 of the Directive, it is not possible to establish a presumption of compliance with legal requirements by publishing references to generally recognised standards other than standards relating to Annex II (f) and Annex III.[391]

The "small-scale approach" is thus limited to the reshaping, review and rationalisation of the existing standards into a business-oriented ES standardisation framework based on real EN, and, as a second step, the referencing of those standardisation deliverables via Commission Decisions based on Art. 3.5 of the Directive, updating or complementing Decision 2003/511/EC, together with appropriate marketing and promotion efforts.[392]

Similarly, also the **ELSIGN Study**[393] recommended not to amend the eSignature Directive, or at least to consider such amendments as an ultimate solution only to be used when all other measures are deemed to be insufficient. Its authors also raised concerns that amending the Directive would be a long and cumbersome operation that should be avoided if possible, given the fact that the Directive constitutes a compromise reached only after long and difficult negotiations between 15 member states all of whom had very divergent

[388] Study on Standardisation Aspects of eSignature, 2007. See already Chapter 2.3.2.2 above.

[389] Study on Standardisation Aspects of eSignature, 2007, ExS, p. 17.

[390] The authors take the view that Art. 3.5, sentence 1, of the eSignature Directive ("*The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities*") authorises the Commission to publish references to generally recognised standards relating to all types of ES products for the provision of all ES services, i.e. also to standards other than those ensuring compliance with Annex II (f) and Annex III. In their opinion, this first sentence can be read without linking it to the second phrase. While the authors recognise that the publication of reference numbers under Art. 5.3 of the Directive is limited to ES products, they consider the definition of "ES product" (which is broader than CSP trustworthy systems, Annex II (f), and SSCD, Annex III) to be wide enough to cover all market needs when implementing ES. Therefore, they believe that there is no fundamental need to amend the Directive or the basic principle of its business model.

[391] Therefore, they recommend that whenever publishing other standards under Art. 3.5, the Commission should explicitly state that legal compliance is insofar not presumed, see Study on Standardisation Aspects of eSignature, 2007, ExS, p. 15.

[392] The Study also recommended a number of "quick-win" actions. For more details on all recommendations see Study on Standardisation Aspects of eSignature, 2007, ExS, p. 17ff.

[393] See ELSIGN Study, 2003. Please note, however, that this study from 2003 is in our view no longer fully representative.

views on these issues. The study considered the text of the Directive adequate enough to serve its purpose in the near future but acknowledged that it needs re-interpretation and clarification. Therefore, it recommended that the Commission should issue a non-binding document to support a more "community-focused" interpretation of the Directive, combined with realistic accompanying measures which could be implemented in the short term.[394]

2.4.2 Other proposed actions and supportive measures for electronic signatures

Besides the recommendations discussed within the above-mentioned approaches (Chapter 2.4.1), also the following actions and supportive measures for ES are being proposed:

(1) Actions to overcome uncertainties regarding SSCD conformity assessments

Though opting for the "large-scale approach", the **CROBIES Study** has formulated in **WP 4** (Framework for SSCD cross-border recognition) additional recommendations for a homogeneous interpretation of the Directive at the European level as a "quick win" action within the existing legal framework[395], which could be realized via an update of Decision 2000/709/EC, CWA 14169 and Decision 2003/511/EC. These recommendations intend to overcome the legal uncertainties[396] relating to the conformity assessments of SSCD[397] and comprise i.a. the clarification of the legal validity and value of conformity assessments and the introduction of requirements for each member state to have a Designated Body in place, notify it to the Commission (who will then publish a list of Designated Bodies), publish (and possibly update) harmonised lists of approved SSCDs and use common templates[398] for the notification and the publication.[399] Furthermore, WP 4 proposed to establish conformity assessment guidelines, and to create (within Mandate M/460) real SSCD standards to overcome the uncertainties around the existing standards.[400]

(2) Actions to overcome eGovernment national perspective issues

Above, we have outlined some interoperability barriers that affect primarily ES applications in the eGovernment sector which are often designed with a mere national perspective (e.g. the existence of different national identity management schemes, use of national identifiers).[401] According to the Study on Mutual Recognition of ES, solutions overcoming these issues have to be developed in the framework of eID interoperability. The Study proposes that the mutual recognition or harmonisation of eID schemes should be progressed[402], which will most probably include legislative amendments in some member states. Beyond this, interoperability issues resulting from national characteristics are often the consequence of the design decision of the eGovernment applications owner and can only be solved if these owners modify the design of the concerned application and eliminate such restrictions.[403]

[394] ELSIGN Study, 2003, p. 9. For more details on the different recommendations please see the text of the Study.

[395] Although opting for the large-scale approach, the CROBIES Study has additionally proposed in WP 1-5 several "quick win actions" within the existing legal framework, to be undertaken as transitional measures until the realisation of a recast framework enabling MS from a technical and practical perspective to accept and validate non-national ES. However, great part of them affects the technical or trust level and is already being addressed (or at least recommended to be adressed) within the standardisation approach under Mandate M/460 [see above Chapters 2.3.2.2 and 2.4.1.1. (2)] or on the trust level, and is therefore already part of the above proposed overall large-scale approach, see CROBIES Study, 2010, HD, p. 9ff.

[396] See Chapter 2.2.1 above.

[397] CROBIES Study, 2010, WP 4, p. 21., 61ff, 72, and HD, p. 26.

[398] Annex 1 of CROBIES WP 4 contains a proposal for such common templates, inspired by the Decisions 2009/767/EC and 2010/425/EU on TL.

[399] CROBIES Study, 2010, WP 4, p. 21., 72. For details on the recommendations see CROBIES Study, 2010, WP 4, p. 61ff.

[400] CROBIES Study, 2010, WP 4, p. 79 and HD, p. 26.

[401] See Chapter 2.1.1. above

[402] For further recommendations see Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 110f.

[403] EFVS Study, Analysis & Assessment Report, 2009, p. 52.

With regard to the potential abuse of the public sector clause (Art. 3.7) of the Directive, the Study[404] recommends to request member states to offer ES solutions with cross-border legal validity instead of introducing requirements restricting the free movement of services by limiting public sector applications e.g. to certain CSP or to eID cards issued by their own authorities. Member states should also be reminded of their notification duties regarding additional requirements imposed in application of Art. 3.7, which would help to get an accurate overview of accepted ES solutions and CSP abroad.[405] The Study also recommends to remind member states that a possible national decentralisation of competences does not absolve a member state of its obligations under the Directive and to make eGovernment application owners aware of the existing issues.[406]

(3) Promotion and awareness rising

Beyond this, most Studies recommend an appropriate education, promotion and awareness rising around ES and the (recast) European ES framework to convince the market and business stakeholders of the possible return on investment of ES securing their eProcesses.[407] Likewise, appropriate marketing campaigns for ES are being suggested.[408]

(4) Other economic supportive measures for ES

Finally, in order to foster the still hesitant and low use of ES in particular by private persons or small and medium sized enterprises[409], some authors consider price reductions and a subsidisation strategy necessary to reach the critical mass of users and recommend the provision of incentives for investments.[410] They point out that the distribution of SSCD alone is not sufficient to enable a widespread use of ES.[411] Likewise, they encourage the creation of alternative business models (e.g. based on cost sharing)[412] and the creation of ES applications which are attractive for ES users[413] and could thus also increase the demand for eID cards.[414] Possible financial incentives to use ES could e.g. be the introduction of tax deductibility for ES infrastructure, tax reductions for citizens who file their tax return electronically using QES, discounts or other benefits to customers ordering products using QES and other financial benefits for acquirers of ES solutions.[415] In specific areas, even the introduction of a legal obligation to use QES (like in the emissions trading in Germany[416]) is being considered.[417]

[404] Preliminary Study on Mutual Recognition of eSignatures, 2007, p.104 f., 106.

[405] Preliminary Study on Mutual Recognition of eSignatures, 2007, p.104 f., 106. In contrast, given the complexity of the issue and the lack of a common technical solution allowing MS from a practical perspective to accept and validate non-national ES, the study does not consider infringement proceedings for non-compliance with the eSignature Directive appropriate.

[406] Preliminary Study on Mutual Recognition of eSignatures, 2007, p. 108f., 106.

[407] EFVS Study, CSM – Final Report, 2010, p. 11.

[408] Roßnagel, 2008, p. 164, 138.

[409] See above 2.2.4.

[410] Roßnagel, 2003, p. 62, p. 2.

[411] Roßnagel, 2008, p. 154.

[412] Roßnagel, 2008, p. 123.

[413] Proposed applications are e.g. the replacement of PIN/TAN or login/password authentification by more secure authentification methods based on QES (for example in ebay), signature of electronic transaction orders with QES, electronic business processes, electronic correspondence with courts, access to official registers (see Roßnagel, 2008, p. 98f., 102f., 114ff.).

[414] Roßnagel, 2008, p. 67, 71, 85f., 100.

[415] Roßnagel, 2008, p. 144, 93, 145, 105.

[416] For more details see www.epractice.eu/en/cases/dehstew.

[417] Roßnagel, 2008, p. 141.

(5) Use of other types of ES

Others propose to foster the use of other types of ES, e.g. of mobile signatures[418] or of a specific type of AES which is based on the signatory's handwritten signature issued e.g. on a signature tablet as a cheaper and more practicable solution compared to QES. The digitalised profile of this handwritten signature is encrypted, included in the hash value of the signature and thus linked to the data to which it relates. While the legal effect of QES does not apply to this type of AES, its supporters nevertheless consider it a probative evidence as in case of need, the signatory can be retroactively identified before court as the creator of the handwritten signature by an authorised script expert.[419]

2.5. Evaluation and conclusions

In our view, the large-scale approach aiming at the creation of a sound legal basis for all certification services through a revision and extension of the eSignature Directive is the preferable strategy.

Mandate M/460 should be continued to establish a rationalised standardisation framework accompanied by appropriate guidelines. European standards should be established and linked with the legal requirements of the revised Directive via Commission Decisions.

An appropriate trust infrastructure based on liabilities, supervision and voluntary accreditation should be established for all types of certification services.

Existing pilot projects and sector specific harmonisation initiatives should be continued but well aligned with the revised Directive and other initiatives. In addition, further harmonisation in the field of electronic identification and economic supportive measures (e.g. financial incentives) to encourage the use of electronic signatures and the development of attractive electronic signature applications are necessary.

The explanations in Chapter 2.4. show that there is already a number of detailed, comprehensive and promising recommendations on how interoperability and cross-border use of ES, but also the use of ES in general can be improved. In this final Chapter 2.5, we will evaluate the recommendations outlined above and give our opinion on the steps which should be taken to create an ES system that works at European level.

As regards the two approaches discussed above, we believe that in spite of the possibly long-term discussions which are to be expected, the more comprehensive **large-scale approach** is preferable for the following reasons:

On the legal side, we believe that a thorough revision of the eSignature Directive is indeed recommendable, as it is in our view crucial to have a clear and sound legal basis for the use of ES and all relevant types of certification (CSP) services, which will also facilitate further enhancements on the standardisation and trust level. The Directive should be amended and extended to define and rule also services ancillary to ES or employing ES.

[418] Roßnagel, 2008, p. 245ff.

[419] Signature Perfect, 2008, p. 48.

Beyond this, unclear definitions and wordings in the current version should be optimised in order to address the existing interpretation issues. Furthermore, adequate liability rules for all certification services should be defined. In order to ensure a clear mapping of legal and technical requirements, Art. 3.5 should be extended in order to establish a basis to reference future standards to be created within mandate M/460 (or future mandates) via Commission Decisions. This should be combined with the definition of legal presumptions when meeting these standards. However, it is not fully clear to us how the proposal of the EFVS and CROBIES Studies to also introduce regulations on eIdentification and eAuthentication services and the announcement of the Commission in the Digital Agenda to provide "a legal framework for cross-border recognition and interoperability of secure eAuthentication systems"[420] have to be interpreted. In particular, it is unclear to what extent and in what detail rules on eIdentification and eAuthorisation should be included in the recast Directive and how this will relate to the announced Decision to ensure mutual recognition of eIdentification and eAuthentication across the EU based on online authentication services[421]. In any case, it should be well considered whether it is recommendable to fully regulate eIdentification and eAuthorisation in this Directive, or whether this risks to be an overkill which could entail even more cumbersome discussions.

In order to address eGovernment national perspective issues, initiatives have to be taken also in the eIdentification sector. Likewise, the limits of Art. 3.7 of the Directive regarding additional requirements for the use of ES in the public sector should be clarified.

On the technical level, in our view the appropriate and necessary actions have already been started by the Commission initiating Mandate M/460 with the aim to create a full set of rationalised common European standards. It should be made sure that these standards reflect the market needs and cover all relevant products and services regulated by the Directive. European Norms should be established and linked with the legal requirements of the revised Directive via Commission Decisions. Such recast standardisation framework should be capable to overcome the existing uncertainties and implementation of the respective standards would ensure interoperability. In order to facilitate interoperability, this mandate should inter alia cover the establishment of common standards for the use of ES formats also beyond the use of ES in documents that service providers may need to submit through Points of Single Contact within the scope of the Services Directive (for which Decision 2011/130/EU stipulates a number of formats that member states technically have to support).[422] However, once such a recast standardisation framework has been put in place, it is equally important to ensure that the standards are actually being implemented and find acceptance in the market. In this context, it is crucial to make available appropriate guidelines for the implementation and use of such standards, which are planned to be formulated under Mandate M/460. Beyond this, an appropriate promotion of European Standards and related guidelines is necessary to ensure interoperability in the area of ES.[423]

As regards the trust level, the ideal future trust framework should in our view cover all certification (CSP) services covered by the extended Directive. In particular, following the proposals of the EFVS and CROBIES Studies, an appropriate trust infrastructure should be created also for certification service providers offering other services than issuing qualified

[420] EC, A Digital Agenda for Europe, p. 11. See also Chapter 2.3.2.1 above.

[421] See EC, A Digital Agenda for Europe, p. 32 (Key Action 16). See also Chapter 2.3.2.6 above.

[422] As regards the interoperability issues due to the use of multiple ES formats across Europe see above Chapter 2.2.2. For further details on Decision 2011/ 130/EU see above Chapter 2.3.2.2.

[423] See already EC, Legal barriers in eBusiness, 2004, p. 15.

certificates, i.a. by establishing supervision and voluntary accreditation schemes and by publishing respective Trusted Lists also for these services.

Beyond this, in parallel to and until the realisation of a recast legal, standardisation and trust framework, the existing CIP[424] **pilots PEPPOL, SPOCS and STORK should be continued.** A number of the building blocks required to realize the ideal framework for ES is already being developed or examined in different contexts within these pilots.[425] While the functional specifications of PEPPOL WP 1 are specifically targeted at cross-border public procurement, it is believed that the solution will be applicable also to other application areas in need of ES interoperability. This will allow use of the solution not only for procurement processes, but in general as a service for any request certificate validation that may arise in a cross-European context and thus for every business process with signed documents.[426] Until the full realisation of the recast framework, the pilots will give valuable insight on existing barriers which in turn can be taken into account for the actual standardisation and rationalisation work. Beyond this, the recommended recasting of the framework supports the long term sustainability of the outcomes of the pilot projects, as these outputs could be integrated in a more general and consolidated form into the future framework.[427] Therefore, even once a fully recast framework exists, we take the view that these pilots will not be useless as they can then provide services which parties receiving ES may optionally use to simplify matters instead of having to use them as a matter of necessity.

Beyond this, sector specific harmonisation initiatives should continue but should be well coordinated with the other initiatives to foster ES and be aligned with the revised Directive.

In addition to these actions intending to enhance interoperability of ES and facilitate their cross-border use, it is in our view equally important to foster and promote use of ES in general. The reason is simply that if ES are not used on a national level, they will neither be used on a cross-border level so that the best measures to enhance cross-border use will have little value. In particular, the proposed (financial) incentives for potential application owners to invest in ES solutions and create attractive applications for the mass market on the one hand and for ES users to invest in the use of ES and the necessary infrastructure on the other hand should be considered. Likewise, use of modern or cheaper and more practical types of ES such as mobile signatures should be fostered.

If the recommended measures are taken, we see good chances that the usage and interoperability of ES and related products and services can be significantly improved once a more comprehensive and consistent legal, technical and trust framework has been established.

[424] Competitiveness and Innovation Framework Programme 2007-2013.

[425] EFVS Study, CSM – Final Report, 2010, p. 39.

[426] See the PEPPOL websites, www.peppol.eu/work_in_progress/wp-1-esignature/results/deliverable-1.2/d1.2-trans-national-verification-solution-s-prototype-documentation; www.peppol.eu/work_in_progress/wp-1-esignature/results/deliverable-1.1/first-deliverable-of-wp1-has-been-released and www.peppol.eu/work_in_progress/wp-1-esignature/current-status.

[427] See also EFVS Study, CSM – Final Report, 2010, p. 39, according to which such integration will support to solve the problem that the results under the CIP pilots might be very promising for pilot purposes, but their usage in practice in the long term required a consolidation process in which the outputs would be formalised.

3. ePROCUREMENT

Public Procurement represents a very important part of the EU economy. Public authorities in the EU buy goods and services to the amount of 19% of GDP each year.[428] Considering this, there is a major interest to improve efficiency, transparency and competitiveness as well as to reduce costs. Using eProcurement could have an enormous impact and improve the way government procurement operates. Many studies have pointed out that the digitalization and automation of administrative processes hold much, if not most, of the imminent productivity improvement potential.[429]

To support the introduction of eProcurement on a large scale Commission launched in 2004 an eProcurement Action Plan[430] and introduced several provisions in the new public procurement Directives 2004/17/EC and 2004/18/EC. In 2005, EU-Ministers declared in Manchester that *"by 2010 at least 50% of public procurement above the EU public procurement threshold will be carried out electronically"*.[431]

Considering the state of play today as presented in the 2010 Green Paper on eProcurement[432] the use of eProcurement remains far behind the expectations, especially with regard to cross-border eProcurement. The Commission estimates that less than 5 % of total procurement budgets in the first-mover states is awarded through electronic budget[433] (except Portugal – see below). Cross-border eProcurement seems nonexistent.

The following analysis gives an overview of eProcurement in Europe today and tries to find out the main obstacles to the broader use of eProcurement, especially as far as cross-border participation is concerned. Finally it will be stressed which kind of identification and authentication solutions should be chosen and which further steps have to be taken to improve the uptake of eProcurement.

3.1. Overview of eProcurement

Making all phases of a public procurement electronically available would bring many advantages, especially more transparency, more efficiency and a cost reduction.

Since 2004 many efforts have been made on national as well as on European level. Nevertheless the results are far behind the expectations. Especially cross-border eProcurement is virtually non existent.

The Commission´s 2010 Green Paper on eProcurement and the related documents give a comprehensive overview of the whole subject.

For a better understanding of the problems which are encountered by eProcurement it is necessary to first describe eProcurement and to give an overview of the actual state of play in the member states.

[428] eProcurement – E-Banking Snapshot 36, dbresearch, February 2011.

[429] Referred to in EC, Report on eInvoicing, 2009, p. 1.

[430] EC, Action Plan for EPP, 2004.

[431] The Manchester ministerial declaration of 2005.

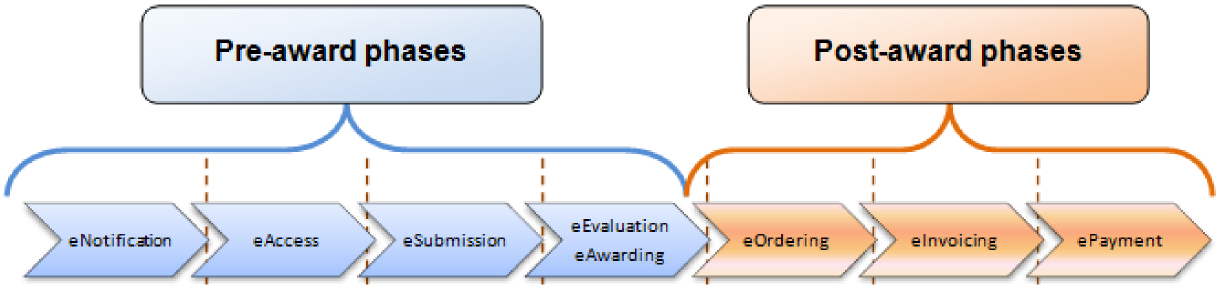
[432] EC, Green Paper on expanding the use of eProcurement, 2010.

[433] EC, Evaluation of the 2004 Action Plan for EPP, p. 9.

3.1.1 What is eProcurement?

eProcurement refers to the use of an internet-based electronic system which automates and integrates any part of the procurement process.[434]

A public procurement commonly consists of different phases: publication of tender notices, access to tender documents, evaluation, award, invoicing and payment. All these phases could be provided electronically. In this case, one can speak of a "straight-through eProcurement". But it is not always necessary or even advisable to provide all phases electronically. Especially the evaluation phase will continue to require human intervention when qualitative criteria have to be assessed.



Map 1: Example for eProcurement phases as defined in the Siemens-time.lex study[435]

The Commission assumes in its evaluation for the green paper that the minimum requirement for a system to be defined as providing eProcurement is the electronic provision of the publication of tender notices, access to tender documents and submission of tenders.[436]

Because of the sensitivity of the government data and the legal nature of tenders, orders and payments, security of data is critical in an eProcurement system. The system must have mechanisms for identifying and authenticating the users.[437]

3.1.2 The 2010 Green Paper on eProcurement

On October 18, 2010 the EU Commission published the Green Paper on expanding the use of eProcurement in the EU.[438] It represents a first step towards a Commission White Paper outlining steps that the Commission will take to establish an inter-connected eProcurement infrastructure, as foreseen in the Commission's Digital Agenda.[439]

The Green Paper gives a summary of the state of eProcurement today and the challenges that prevent the successful transition to eProcurement. Finally it suggests several further steps to be taken on EU level to promote the uptake of eProcurement.

In the Green Paper, the Commission has set out a series of questions for a market consultation whose results will be published in 2011.

[434] Vaidya, Callender, Sajeev in: *Handbook of Public Procurement*,p. 477.

[435] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 139.

[436] EC, Evaluation of the 2004 Action Plan for EPP, p. 6.

[437] Vaidya, Callender, Sajeev in: *International Handbook of Public Procurement*, p. 482.

[438] EC, Green Paper on expanding the use of eProcurement, 2010

[439] EC, A Digital Agenda for Europe, 2010, page 32.

The figures and other evidence presented in the Green Paper are based on a Commission Staff Working Document on the Evaluation of the 2004 Action Plan for Electronic Public Procurement.[440] Within the Action Plan, the Commission was tasked, by the end of 2007, to start to "*review and report on the results achieved and to propose, if need be, …. corrective action or additional measures*".[441] This evaluation was supported by an external study by Siemens-time.lex : "Study on the evaluation of the Action Plan for the implementation of the legal framework for electronic procurement". This study provided most of the information presented in the staff working document.

3.1.3 Advantages and Disadvantages of eProcurement

As eProcurement is still not in use on a broad scale it is merely impossible to demonstrate the advantages (or disadvantages) on the basis of reliable figures. However, the Green Paper assumes that eProcurement has the following advantages[442]:

- Accessibility: searching for tender opportunities online is much quicker and cheaper than screening paper-based publications. eProcurement has the potential to reduce distance barriers, especially when cross-border participation is at stake, and encourage greater participation and potentially enlarging markets.
- Transparency: the procurement process is more open, well-documented and communicated. More transparency means usually less corruption, therefore eProcurement could also play a important role in fighting procurement-related corruption.
- Efficiency: The amount of time spent on administrative tasks is reduced allowing contracting authority personnel to concentrate on more strategic issues. Opportunity to rationalize and review the procurement process.
- Cost reduction as a result of transactional and process efficiencies.

In addition eProcurement could attract better offers due to faster invoice / payment processing and is environment friendly, as it is a paperless process.

A very recent study from Germany´s Deutsche Bank assumes that a full switch to eProcurement may save between EUR 50 and 75 bn on public procurement in the EU per year, considering only the operational savings and the price reduction in the bids.[443]

Practice case

Austria: Bundesbeschaffung GmbH (Federal Procurement Company)

The Bundesbeschaffung GmbH (BBG) centralises purchases through an eProcurement system. Since its establishment in 2001 the BBG bought products and services with an accumulated volume of 4.2 Billion Euro and saved a total amount of 705 Million Euro, which means an averaged saving rate of 13.4 percent. The systems serve 12,000+ users. In 2008 the BBG reported procurements of 830 Million Euro and savings of 17.64 percent (178 Million Euro).

(**Source:** Siemens-Time.lex, Country Profiles – Austria)

[440] EC, Evaluation of the 2004 Action Plan for EPP

[441] EC, Action Plan for EPP, 2004, page 10.

[442] EC, Green Paper on expanding the use of eProcurement, 2010, p. 4.

[443] Deutsche Bank, 2011 - Chart 3.

As to disadvantages one can say that in theory no real disadvantage exists. The negative aspects one can identify at the moment are mostly due to inappropriate implementation and use of eProcurement. The Siemens-time.lex study for example shows as possible negative impacts:

- less competition: an excessive use of framework agreements could result in less competition, negating the expected cost benefit of increased efficiency;
- less value for money: an inappropriate use of automated evaluation could lead to suboptimal results, with economic operators focusing more on elements that can be automatically evaluated (such as price) and less on subjective but equally important characteristics such as quality;
- possible marginalisation of SMEs and/or foreign economic operators.[444]

3.1.4 eProcurement in Europe today

Since 2004 some notable successes have been achieved at national level. But eProcurement remains a fragmented landscape and very little has been made towards cross-border use. Overall there seems to be a big gap between the possibilities in place and the usage in practice.

3.1.4.1 At national level

With the exception of Greece all member states have at least rudimentary eProcurement systems. But there are very big differences between these systems in terms of phases and tools on offer, the entities that can use them and how they are used.[445]

(1) Existing infrastructures

The Siemens-time.lex study has identified 129 eProcurement sites in 30 countries[446], noting that the list is not comprehensive, especially due to the eProcurement landscape in decentralised member states. Local or regional contracting authorities have a much larger range of procurement solutions available to them, including by implementing solutions developed by private sector service providers.[447] As an example, the study counted only 1 site when one solution has been implemented by several contracting authorities. That would mean that a far bigger number of eProcurement sites exist in practice.

The study reported on:

- 26 platforms (solution that a service provider develops and runs for subscribing procurement organisations, managed by private parties without a specific public sector mandate);
- 22 CPB´s framework platform (system supporting the provision of goods and services to public offices under framework agreements signed by a Central Purchasing Body such as the Austrian Bundesbeschaffung GmbH (see above);
- 81 portal sites (web-based solution offering a single entry point to a number of procurement platforms managed by a public body or with a mandate from a public body; portals are either for their own use, or for use by other contracting authorities);

[444] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 16.

[445] EC, Evaluation of the 2004 Action Plan for EPP, p. 61.

[446] Compared to 36 sites identified in 2004 – EC, Evaluation of the 2004 Action Plan for EPP, p. 41.

[447] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 135.

- The scope of the sites can vary widely: some of the sites functions are open eProcurement sites (available to any contracting authority), while others are only available to contracting authorities at the national/federal level, at the regional level, at the local level, or within a specific sector.[448]

(2) Availability of phases

Whereas most of the countries do not offer "straight through eProcurement", notification by electronic means is widespread (all member states are using at least TED, the EU-wide notification tool). The use of evaluation and award-phases is very low, as well as the post-award phases.

Table 1: Overview of the phases, based on Staff Working Document, page 44

Availability of phases	Countries (27 EU MS, 3 EEA MSt and 2 Accession countries)
Full pre-award	Belgium, Denmark, Germany, Ireland, Spain, France, Italy, Cyprus, Lithuania, Hungary, Malta, Austria, Portugal, Romania, Slovenia, Slovakia, Sweden, United Kingdom, Norway
Full pre-award except eEvaluation and e-Award	Czech Republic, Estonia, Latvia, Netherlands, Poland, Finland
Only eNotification and eAccess	Bulgaria, Luxembourg, Croatia, Turkey
No pre-award or very limited	Greece, Liechtenstein, Iceland
Full post-award	Finland, United Kingdom, Norway
Full post-award except e Payment	Czech Republic, Denmark, Spain, Sweden
No post-award or very limited	Bulgaria, Estonia, Greece, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Slovakia, Slovenia, Iceland, Liechtenstein, Croatia, Turkey

(3) Transposition of tools offered by the Directives

The 2004 EU Public Procurement Directives offer some tools designed to achieve a more effective and efficient procurement: Dynamic Purchasing Systems (DPS)[449], eAuctions[450], framework agreements[451] and buyer profiles.[452] The member states are not required to implement these tools in their legal framework.

[448] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 135.

[449] Art. 1.6 Directive 2004/18/EC.

[450] Art. 1.7 Directive 2004/18/EC.

[451] Art. 1.5, 32 Directive 2004/18/EC.

[452] Art. 35.1, Annex VIII 2 b Directive 2004/18/EC.

Whereas only DPS and eAuctions are explicitly related to eProcurement, electronically managed framework agreements also play an important role as they have the potential to include more economic operators and to serve more contracting authorities, leading to more efficient purchases.[453]

Most of the member states have implemented these tools. as far as framework agreements are concerned, even all member states transposed some provisions.

Practice case

Portugal: VORTAL

Portugal made eProcurement mandatory for all public contracts – even below EU Thresholds) in November 2009. In the first year of adoption 75 % of all public procurement were made electronically. Contracting authorities using Vortal´s platform saved, on average, 10 to 20 % on price reduction through increase in competition (suppliers tend to submit more proposals if there is an easy process of submission and tend to be more aggressive if they know that there is a larger spectrum of competition), and 60 % of time spent on administrative tasks (eTendering process automatisation).

(**Source:** eProcurement Meeting Vienna, March 24, 2011)

Table 2: Overview of the tools' transposition, based on the Staff Working Document, pages 32-34

	Legally supported	Not legally supported
eAuction	26 countries (including 22 MS)	6 countries
DPS	27 (including 22 MS)	5
Buyer profiles	20 (including 18 MS)	12

(4) Use in practice

As already mentioned above, the differences between the member states seem to be bigger with regard to the use in practise than regarding the legal implementation.

On the one hand, many countries introduced a more restrictive policy than the EU legislation, making some elements in their eProcurement systems mandatory. For example eSignatures are made mandatory in 19 of the 32 examined countries.[454] As seen above, Austria made the use of the BBG-Platform mandatory for certain contracting authorities, whereas the most advanced State is Portugal, making mandatory the whole pre-award phases for all contracting authorities.

On the other hand, many tools and phases that are legally possible are either not available or not used in practice. As reported in the Siemens-time.lex study, only five member states have not yet implemented the relevant provisions for DPS but only one French eProcurement

[453] EC, Evaluation of the 2004 Action Plan for EPP, p. 33.
[454] EC, Evaluation of the 2004 Action Plan for EPP, p. 39.

site - the "place de marché interministérielle – www.marches-publics.gouv.fr" - is known to have built-in support for DPS.[455] However, it seems that DPS starts to have a slightly better uptake in practice than assumed in the study. A TED-research end of March 2011 showed 15 current DPS-notices, spread over 10 countries (1 DK, 3 UK, 2 F, 1 CZ, 2 NO, 1 E, 1 P, 1 N, 2 LT, 1 MK). For example, North Lincolnshire Council (UK) has established a Dynamic Purchasing System for long-term taxi services (www.northlincs.gov.uk/NorthLincs/CouncilandDemocracy/finances/Procurement/DPS.htm).

It also seems that the economic operators are starting to adopt eProcurement more and more: According to the Deutsche Bank research-study, the overall share of firms using eProcurement in the EU increased by 2 pp. during the last year. In some countries already almost a third of all economic operators used eProcurement last year (Ireland, Lithuania).[456]

3.1.4.2 At European level

To promote eProcurement and to achieve a better cross-border use the EU is financing and/or supporting a number of initiatives.

- PEPPOL (Pan-European Public Procurement Online) aims to implement common standards enabling EU-wide public eProcurement. Existing national systems of electronic public procurement will be linked so that all participants can enjoy the full benefits of a single European market. PEPPOL is operated under the Commission`s Competitiveness and Innovation Framework Programme's ICT Policy Support Programme - www.peppol.eu 12 countries participating.
- PEPPOL project has packaged, and is currently implementing, an integrated set of standards and agreements that collectively address many of the challenges identified by the Green Paper.[457]
- CEN/ISSS (Information Society Standardization System) Workshop on Business Interoperability Interfaces in Public Procurement (WS/BII2) - www.ds.dk/en-GB/Sectors/ICT/Bii/Sider/default.aspx: The objectives of the Workshop are to provide a basic framework for technical interoperability in pan-European electronic transactions. CEN/ISSS Workshops aim to arrive at a European consensus on an issue that can be published as a CEN Workshop Agreement (CWA). These deliverables may take the form of best practice agreements, codes of conduct or pre-standards, with the formal backing of CEN, one of the three European Standardization Organizations. The workshop is part of the PEPPOL-project.
- Open ePRIOR is an Open Source eProcurement platform for all Public Authorities wishing to pilot eProcurement, including its cross-border aspects, using the Profiles of CEN/ISSS WS/BII. Open ePRIOR (electronic Procurement, Invoicing and Ordering) has been developed by the Directorate General for Informatics (DIGIT) of the Commission in the context of the IDABC eInvoicing and e-Ordering project (www.epractice.eu/cases/ePRIOR).
- eCertis - http://ec.europa.eu/markt/ecertis/login.do: information system provided by the EU-Commission that helps identify the different certificates and attestations frequently requested in procurement procedures across the 27 member states,

[455] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 84.

[456] Deutsche Bank, 2011 – Chart 7.

[457] see Chapter 2.3.2.4 above.

two Candidate Countries (Turkey and Croatia) and the three EEA countries (Iceland, Liechtenstein and Norway). eCertis is not only related to eProcurement, as it can be helpful for all kind of procurement, also paper-based. Nevertheless, it has an important impact for cross-border procurement (not to be confounded with "eCertificates/eAttestations" which mean fully electronically provided certificates).

- eTEN Procure - www.eten-procure.com: The eTEN Procure project aims at enabling electronic bids for public procurement procedure through safe and intuitive web services for SMEs, across 6 pilot regions in the EU (Bourgogne, Piedmont, Central Bohemia, Uddevalla, Brittany, Guadeloupe). As the project links all the regional systems together, it creates the first interregional network of shared eProcurement platforms, providing cross-border eProcurement solutions. The virtual public marketplace is now fully operational and ready to be implemented in new EU regions. The platform is built with an open-source licence, enabling any other organisation to take it, adapt it and deploy it.

  The project is funded by the European Union via the eTEN programme. eTEN is a European Union programme designed to contribute to the deployment of trans-European eServices in the public interest.

- www.ePractice.eu is a portal created by the Commission which offers a new service for the professional community of eGovernment, eInclusion and eHealth practitioners. It is an interactive initiative that empowers its users to discuss and influence open government, policy-making and the way in which public administrations operate and deliver services. With a large knowledge base of real-life case studies submitted by ePractice members from across Europe, ePractice.eu serves as a point of reference for all users.

3.2. Identified obstacles at national and European Level

The main obstacles towards a better implementation of eProcurement are the lack of standards and the language barrier. The phases with the greatest implementation problems are the submission phase, also due to the authentication and identification matter, as well as the post-award phases.

The multitude of technical solutions in place leads to a market fragmentation that complicates the task of economic operators who seek to participate in multiple systems. In a cross-border context the technical problems are topped by the language problems, but also by administrative obstacles.

The obstacles that can be identified are mostly due to the lack of standards: too many different technical solutions are in place, some only in use in one small contracting authority (individual island solutions). This market fragmentation complicates the task of economic operators who seek to participate in multiple systems, in particular when it comes to cross-border participation. The economic operators encounter practical, technical and administrative obstacles.

Practice case

Germany: XVergabe

Due to the federal system a lot of different island solutions with different technologies are in place in Germany. This is considered to be the reason for the low use of eProcurement in Germany (less than 5% of all procurements are fully electronically processed). To solve this problem a governmental project involving the main eProcurement solution providers was set up to build a common interface between bid-client and eTendering platforms and to standardise forms. The interface should be available beginning of 2012.

(**Source:** www.Xvergabe.org)

Considering the different phases of eProcurement the identified obstacles are as follows:

3.2.1 Notification and access to tender documents

3.2.1.1 Notification

Notification can be defined as the publication of relevant information on public procurements, either as formal national or European-wide notices or as any other way of communication.

The use of electronic means in this phase is widespread. Above the thresholds usage of the standardised TED forms is mandatory, but the notifications can still be sent by fax, even if the Directive contains some incentives to use electronic means, as the shortened publication delay. Nevertheless, in 2009 94% of the notices for tenders above the EU-thresholds were sent electronically.[458]

However, even if there do not appear to be any significant obstacle for the use of electronic notifications it has to mentioned that there is very little data with regard to procurements below the EU thresholds.[459]

3.2.1.2 Access to tender documents

Access to tender documents refers to the ability to obtain any tender documents and specifications. In eProcurement, this should be made available by electronic means, either via email, by publishing the information on one or more websites or by a direct link to a ZIP file hosted on the contracting authority's system.[460] When published on a website the access can vary due to registration requirements.

Access to tender documents by electronic means seems to have reached nearly universal availability, with the exception of the countries where no advanced eProcurement infrastructure could yet be identified (Greece, Liechtenstein).[461]

Thus, it seems that no real obstacles exist. However, some barriers remain:

Considering cross-border use, the main obstacle is the language barrier. While this problem is not particular to eProcurement, it is none the less a practical challenge to be recognized towards the uptake of cross border eProcurement. Based on an examination of 129 key sites, 39 provided at least some information in languages other than the national language(s).

[458] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 150.
[459] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 154.
[460] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 156.
[461] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 163.

In each of these 39 cases, English is among the supported languages. However, only 13 of these 39 were ranked as being comprehensive, that is providing enough information to permit full usage of the site on the basis of the translation.[462]

A second problem is the practical accessibility of the core functionalities of each site. When the site only disseminates information in a relatively straightforward manner (e.g. by allowing visitors to search for procurement opportunities and download the relevant documents), then no restrictions need to apply: the site can be freely used without any need for registration of the visitors. More complex processes (including e.g. customized search functions based on the user's profile and preferences) will normally require the user to create a profile on the site. This may be as simple as filling out a web form and receiving a username and password (like on most consumer grade eCommerce websites), or it may require the use of smart cards or software certificates issued by a trusted third party.

These requirements can result in accessibility barriers.[463]

3.2.2 Submission

The submission – the actual tendering phase – seems to be a key phase for the successful adoption of any eProcurement system. It is the most complex of the pre-award-phases due to the bilateral dimension of the phase. For the submission phase the Directive defines a set of minimum requirements: the integrity and confidentiality of submitted tenders has to be ensured, tenders have to be inaccessible to everybody until applicable deadlines have expired, and time and date of the receipt of tenders have to be determined in a reliable manner. Depending on the evaluation of risk, the public procurement system may require the use of AES, logging facilities, time stamping services, identification and authorisation management systems etc[464] (see also below 3.3).

The electronically based submission can have a variety of form: sending an offer via an asynchronous, email-type communication channel (e.g. PEPPOL), uploading a non-standardized offer via an eProcurement platform, with or without signature, complemented with standardised forms or not, or uploading a standardized offer.

According to the Siemens-time.lex study, eSubmission is available in 93% of the member states, even if it is hard to measure whether eSubmission is used in practice. One problem could be that in the vast majority of countries (50 %) the permissibility of eSubmission is entirely dependent on a decision of the contracting authority. Only in some countries (Austria, Portugal and Sweden) eSubmission has already become mandatory for some procurement.[465]

3.2.2.1 Accessibility barriers

According to the Siemens-time.lex study, language support remains an important barrier also for eSubmission. In addition the many island-solutions implicate that the economic operator has to learn for each solution how this special submission-tool works. Unfortunately the instructions provided by the contracting authority are rarely clear and accessible enough.[466]

[462] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 75/76.

[463] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 137.

[464] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 169.

[465] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 175.

[466] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 179.

Especially for SMEs which may not participate frequently in procurements, eSubmission may require a disproportionate initial investment. For each eSubmission solution they have to decide whether it is economically interesting to invest the time, effort and resources to fulfil all technical requirements and learn how to use them.[467]

3.2.2.2 Interoperability barriers

The biggest interoperability barrier for eSubmission is the identification and authentication process.

eSubmission currently relies on two possible options in order to ensure that economic operators are sufficiently identified and that the integrity and authenticity of their communications is guaranteed: either they require the use of username/password authentication following prior registration, or they use authentication systems supported by cryptography, e.g. using smart cards (so called Public Key Cryptography, or PKI).[468]

In practical terms, username/password based systems (as used mainly in Ireland and the UK) currently pose no interoperability challenges other than the completion of the registration process (which may be complicated due to language barriers or the need to provide information which is only available at the national level). PKI systems, in contrast, are currently almost universally unable to accept foreign solutions, meaning that foreign economic operators will be unable to use eSubmission unless they can obtain a PKI solution issued in the country in which they wish to submit an offer.[469]

For further details, especially related to ES see below 3.3.

Another issue that still needs to be tackled is the certification of submission time. Depending of the submission method (see above) there is a need for an external time stamping service. At the moment this poses a cross-border obstacle as an interoperable EU-wide time stamping service does not exist.[470]

3.2.3 Evaluation and award

The pre-award phases end with the evaluation and award phases. Evaluation refers to the determination of the validity of the bids and to the comparative evaluation of all admissible bids. The award can be defined as the communication of the outcome to the bidders.

Part of the evaluation phase is also the (simultaneous) opening of the bids, which can successfully be supported electronically. During all the phases it has to be ensured that the integrity and the confidentiality of the bids are preserved.

3.2.3.1 Status and remaining barriers

According to the Siemens-time.lex study there are eEvaluation / eAwarding functionalities on one or more platforms in a narrow majority of countries (17 out of 32).[471]

However, as in many cases a fully automated evaluation is impossible due to the presence of subjective elements, the electronic evaluation is often reduced to a decision support tool. The same applies to the electronic awarding, which is largely a matter of assisting the contracting authority in managing its communication.[472]

[467] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 179.

[468] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 23.

[469] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 24.

[470] EC, Evaluation of the 2004 Action Plan for EPP, p. 113.

[471] Study on the evaluation of the Action Plan for electronic procurement, 2010, page 184: AT, BE, CY, DK, FR, DE, HU, EI, IT, LT, MT, NO, PT, RO, SK, SE and UK.

[472] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 183.

All in all, there do not appear to be significant obstacles in these phases. The limited usage in practice could be due to the lack of systematic eProcurement infrastructure which can still be observed in most of the countries.

3.2.3.2 eAttestation / eCertificates

One important aspect in the evaluation phase is the assessment of the admissibility of the bid. Therefore the economic operator has to submit a number of documents and/or declarations such as extracts from judicial reports, tax/social security certificates etc. To achieve a fully electronic submission and evaluation, the economic operator should have the possibility to get these documents electronically and the contracting authority should accept and validate them, especially if they were issued in another member state. This is far from being achieved.

According to the Siemens-time.lex study, the main approach used by the surveyed countries to handle the problems related to attestations is to install electronic procedures that eliminate or reduce the need for attestations, either in a paper or electronic form. The use of real eAttestation in public procurements is virtually non-existent.[473]

Separate official eAttestations, issued electronically and signed electronically were reported only in 4 countries and there the systems were still in a pilot stage.[474] Furthermore, there is presently no commonly accepted solution for the cross-border validation of e-Attestations.[475]

Thus, only three types of more or less "electronic" attestations are in use: self-declaration form using the signature solution required by the eProc system, direct information exchange between administrations and declarations of compliance from trusted third parties in a pre-qualification system. However, these models cannot be considered as real electronic attestations and are difficult to extend to foreign users. If the declaration form requires an ES, the economic operator will have the same problems as already mentioned before. An exchange between administrations only works at national level, as the data is very sensitive. Finally the prequalification systems seem to favour local tenderers.[476]

Nonetheless, a step towards eAttestation is being made in the context of the large scale eProcurement pilot project PEPPOL. The second work package of this pilot project is working on the development of a so-called Virtual Company Dossier. Essentially, the Virtual Company Dossier is a standardized package of electronic evidence that can thereafter be submitted to any European contracting authority, in a way that would allow the contracting authority to easily determine the completeness and validity of the Dossier.[477]

The main challenges with respect to eAttestations can be summarized as follows:

- Language barriers;
- Legal uncertainty – whether a foreign attestation actually matches the requirements imposed by law;
- Cross-border validation due to different document and signature characteristics.

However, all these obstacles for a cross-border use seem also to exist in a paper environment (except for the signature problem).

[473] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 256.

[474] eCertificates Study, 2008 – Final Report, p. 7.

[475] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 245.

[476] eCertificates Study, 2008 – Final Report, p. 8.

[477] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 251.

3.2.4 Post-award phases

As seen above (3.1.1) the procurement process does not end with the award phase. After the conclusion of the contract, there may be further steps which could be automated and which are referred to as "post-award-phases".

Electronic implementation of post-award phases is important to unlock the full appeal of eProcurement. Only the consistent integration of electronic means can significantly improve efficiencies.[478]

3.2.4.1 eInvoicing (and payment)

Electronic invoicing - eInvoicing - is the electronic transfer of invoicing information (billing and payment) between business partners (supplier and buyer).[479]

While eInvoicing is already an accepted and rapidly growing practice, there are, however, a number of barriers standing in the way of wider adoption especially by smaller businesses and particularly when it comes to cross-border eInvoicing.[480] Thus, only 6 countries (CZ, DK, NO, FIN, SE, ES) reported using eInvoicing in their eProcurement systems.[481] In this context it has to be noted that the Council Directive 2006/112/EC on the common system of value added tax requires member states, as of 1 January 2013, to adhere to the principle of equal treatment between paper and eInvoices.

To improve implementation of eInvoicing a lot of mostly EU-funded initiatives have been started since the Action Plan 2004[482]. Most of the work is related to standardisation (within CEN, IDABC[483] and OASIS[484], notably). Furthermore, the PEPPOL project includes work packages examining eInvoicing, and actual implementation work for the Commission is being undertaken via the ePRIOR project. In addition, the Expert Group on Electronic Invoicing published its final report in 2009, which lead in December 2010 to a Communication from the Commission entitled *Reaping the benefits of electronic invoicing for Europe*.[485] Following the recommendations of the Communication, the Commission set up the European Multi-Stakeholder Forum on Electronic Invoicing (eInvoicing) on Dec. 2, 2010.[486] Finally, there is a multitude of national, sector specific and transnational standardisation initiatives.

All in all, one of the main problems is the great number of available standards in the field of eInvoicing. Therefore, cross-border interoperability is presently very limited.[487] In addition, the legal uncertainty due to the diversity between and within national legislations in Europe remains a major obstacle.[488] However, some effort has been made to correct the legal challenges.[489]

[478] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 186.

[479] http://ec.europa.eu/internal_market/payments/einvoicing/index_en.htm, see Chapter 2.1.3.2 above.

[480] EC, Report on eInvoicing, 2009, p. 4.

[481] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 200.

[482] For further details see Study on the evaluation of the Action Plan, p. 195 – 199.

[483] **I**nteroperable **D**elivery of European eGovernment Services to public **A**dministrations, **B**usinesses and **C**itizen, http://ec.europa.eu/idabc. For a final evaluation of the IDABC programme see Deloitte, 2009.

[484] **O**rganization for the **A**dvancement of **S**tructured **I**nformation **S**tandards, http://www.oasis-open.org/.

[485] EC, Reaping the benefits of electronic invoicing for Europe, 2010.

[486] Decision C(2010)8467.

[487] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 204.

[488] See PEPPOL eInvoicing Pilot Specifications.

[489] Council Directive 2010/45/EU of 13 July 2010 amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing.

Practice case

Denmark: eInvoicing

Denmark adopted a regulation on February 1, 2005 mandating the private sector to send all invoices to the public sector in via electronic means. In addition Denmark adopted a common message standard known as OIOUBL. The impact is significant: over one million e-Invoices were exchanged by over 200.000 companies; time saving is estimated at 12 to 20 minutes per invoice, resulting in potential yearly cost saving of EUR 500.000.000. SMEs can use an eInvoicing portal to facilitate the creation of e-Invoices or they can use the services of scanning agencies.

(**Source:** Siemens-time.lex study, page 202)

With respect to electronic payments, relevant steps towards a real cross-border use have been made since the Action plan 2004. The Payment Services Directive[490] and the resulting Single Euro Payments Area (SEPA)[491] will eliminate most of the barriers for electronic payments.[492] The Single Euro Payments Area (SEPA) is an initiative of the European banking industry that will make all electronic payments across the euro area – e.g. by credit card, debit card, bank transfer or direct debit – as easy as domestic payments within one country are now. However, only a very few number of countries (4) reported e-Payments to be part of (one of) their eProcurement systems.[493] This may be due to the fact that an ePayment solution without the implementation of eInvoicing is not very attractive as it makes an automated processing impossible.[494]

3.2.4.2 Ordering

Electronic ordering is a precondition for the effective use of DPS or framework agreements: all economic operators receive the same order and submit a response using the same technical format. The contracting authorities will be enabled to fully automate the procurement process, e.g. if the evaluation is only based on quantitative criteria.

17 countries (including 16 member states) reported having implemented an eProcurement system allowing the use of eOrdering.[495] This is a significant progress. However, as already mentioned for eInvoicing, cross-border interoperability is currently very limited, due to the multitude of existing standards.

eOrdering is also addressed by a number of initiatives (CEN, PEPPOL etc.), mostly working on standardisation.

3.2.5 eProcurement tools

In addition to the different phases, it is interesting to see how some of the key eProcurement tools have been implemented and which obstacles can be observed.

[490] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.

[491] http://ec.europa.eu/internal_market/payments/sepa/index_en.htm.

[492] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 192.

[493] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 200.

[494] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 204.

[495] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 200.

As ES will be addressed below (see 3.3), this chapter only considers Framework agreements and Dynamic Purchasing System.

Though eAuctions are one of the more interesting procurement mechanisms enabled through the use of electronic means, this tool will not be examined in detail in the following chapter. As seen above eAuctions have been legally implemented in most of the countries. But in many cases there is still a lack of appropriate infrastructure and some barriers remain. According to the Siemens-time.lex study[496], eAuctions can only be productively used in procurements where it is possible to define clear assessment criteria that can serve as a basis of comparison between bids, and in markets where the auction is reasonably likely to result in multiple bids that can compete on equal terms.

3.2.5.1 Framework agreements

Framework agreements are defined in the Directive as "an agreement between one or more contracting authorities and one or more economic operators, the purpose of which is to establish the terms governing contracts to be awarded during a given period, in particular with regard to price and, where appropriate, the quantity envisaged".[497] Framework agreements are not an eProcurement tool as such. They can be used both in traditional (paper based) procurement and eProcurement, but through eProcurement they can be used more systematically and at a larger scale. This means ultimately more competition, reduced prices, better quality of the goods and services provided and increased overall efficiency.[498]

It seems that there is a strong relation between framework agreements and eProcurement. In a number of countries eProcurement relies on framework agreements, with key examples being the partially mandatory regimes in Sweden and Austria, and the extensive supporting infrastructures (typically via central purchasing bodies) established in these and other countries, including Belgium, Denmark, Finland, Italy, Norway, and the UK. Framework agreements will increasingly go 'online' (see e.g. current activities in Cyprus and Lithuania), and will more and more interact with other tools such as eCatalogues.[499]

However,some obstacles remain. Framework agreements are closed environments, and thus improve efficiency at the expense of competition. According to the data collected by the Siemens-time.lex study a majority of 60% of framework agreements is concluded with only one economic operator, which means there is no competition at all on the ordering level.[500] It should be noted, however, that this is not a specific problem for electronically based framework agreements.

3.2.5.2 Dynamic Purchasing System (DPS)

A DPS can be defined as fully electronically and open framework agreement for "commonly used purchases".[501] Contrary to the latter, new economic operators can join a DPS after its establishment by submitting an indicative tender which meets the requirement of the DPS.

As seen above almost all the member states have implemented the legal framework or intend to do so. However it seems that the uptake in practice is not the same. According to the findings of the Siemens-time.lex study, DPS are rarely used and, contrary to framework agreements, they do not take an important role in national procurement strategies yet.[502]

[496] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 276.
[497] Art. 1.5 and 1.4 of respectively Directives 2004/18/EC and 2004/17/EC.
[498] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 211.
[499] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 223.
[500] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 225.
[501] Art. 33 of Directives 2004/18/EC.
[502] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 239.

Some reasons for the limited usage of DPS could notably be:

- The relatively high complexity (and thus costs) of implementing fully electronic public procurements;
- The challenges in defining the specifications for 'commonly used purchases' in a way that is attractive for economic operators and sustainable over the duration of the DPS;
- The economic challenge in ensuring sufficient participation of economic operators;
- The time-restricted nature of a DPS, which may put it in competition with more permanent solutions (like eProcurement websites managed by central purchasing bodies).[503]

3.2.6 Other obstacles

One aspect, which also could be a challenge in practice, is the human factor: Although technology is available on the market and can be used to build sophisticated and fully automated procurement solutions, it is the ability of the human beings involved in the development and use of the solution that determines success.[504] According to the CGEC (2002), the two major obstacles to increasing support among users are their level of technological awareness and acceptance and their willingness to change long-established internal business processes.[505]

Furthermore, eProcurement implementation is expensive, demanding upon staff, and time consuming, so that it may take several years for contracting authorities to fully reap the strategic and operational advantages.[506]

3.3. Authentication and identification solutions proportionate to the risks encountered in eProcurement

The identification and authentication process is a key element for eProcurement. Nevertheless it seems that cross-border interoperability is far from being achieved in this area (see also Chapter 2). Especially for eProcurement a number of solutions have been developed, but most of them do not enable cross-border use.

We recommend encouraging the use of username/password-based models as commonly used electronic signature in eProcurement. These models are less complex and costly than qualified electronic signatures and do not pose any (cross-border) interoperability barriers. However, they should be backed by a security token to ensure that the documents being submitted are protected against tampering.

[503] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 240.

[504] Vaidya, Callender, Sajeev in : *International Handbook of Public Procurement*, p. 525.

[505] Consortium for Global Electronic Commerce (CGEC), 2002: *Measuring and Improving Value of EProcurement Initiatives*, University of Wisconsin-Madison.

[506] Vaidya, Callender, Sajeev in: *International Handbook of Public Procurement*, p. 486.

The Commission staff working paper states that "the lack of interoperable ES (of any type) is probably the greatest blocking factor to EU-wide eProcurement and eGovernment services in general".[507]

In the following we will examine the challenges eProcurement has to face in that matter and give an overview about the existing options/solutions in the member states. We will conclude with an assessment of the risks and our recommendations.

3.3.1 Definition and scope

First of all it is necessary to define the terms "identification" and "authentication". They are mostly used together, but they are not identical and a clear distinction is often lacking.

Commonly spoken, identification is the process by which the identity of a user is established and authentication is the process by which a service confirms the claim of a user to use a specific identity by the use of credentials.[508] The question of authenticity is thus linked primarily to the source of the information: to what extent is it certain that specific information originates from a specific entity?[509]

Whereas some authentication solutions such as AES and QES should be by definition capable of identifying the signatory[510], the simple ES do not cover identification. Moreover and in contrast to ES, the concept of electronic identity has not been formally defined or regulated at the European level.

As far as the legal effect is concerned, only the QES have the same legal value as handwritten signatures and are admitted as evidence in legal proceedings.[511]

One other crucial challenge in using electronic means in public procurements strongly linked to the authentication issue is ensuring the integrity of the exchanged information. The question of integrity relates to the assurance that the information has not been changed in any way during the communications process, i.e. the information received is the same as the information sent.[512] The integrity of data can also only be addressed by AES and QES.[513] All other solutions need further tools ensuring integrity of data.

It should be noted that the procurement Directives do not require the use of specific ES, and do not refer to electronic identity (eID) at all. The Directives' main emphasis is on ensuring that the integrity of data and the confidentiality of tenders and requests to participate are preserved, and that the means of communication are generally available.[514] However, the Directives actively encourage the use of AES as a measure likely to improve the security and confidentiality of the tendering process and refer to QES as possible option for the submission of tenders.[515]

[507] EC, Evaluation of the 2004 Action Plan for EPP, p. 65.

[508] http://publib.boulder.ibm.com/infocenter

[509] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 295.

[510] see 2.1.1.1

[511] see 2.1.1.3

[512] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 295.

[513] See definitions in 2.1.1.1

[514] In Directive 2004/18/EC Article 42 "Rules applicable to communication" states:

3. Communication of information shall ensure that integrity of data and confidentiality of tenders and requests to participate are preserved, and that CA examine tenders and requests only after time limit for submitting them.

[515] Recital 37 to Directive 2004/18/EC and art. 42.5 lit. b.

3.3.2 Solutions in place at national level

As the procurement Directives give contracting authorities the freedom to choose the appropriate method of authentication, the Member States set different levels of requirements, ranging from a user-ID and password-based model up to QES.

Regarding ES, of the 31 countries for which the eSignatures status is known, 13 do not explicitly require the use of ES. These are the countries which have thus left the largest amount of flexibility in their legal regimes, i.e. Denmark, Iceland, Finland, Norway, Sweden, UK and Ireland.[516] 13 Member States have a legal requirement to use AES, 6 of which require QES. The others require some form of ES, but it is not always clear which type is requested / accepted. Finally most applications still only support local credentials, with ad hoc exceptions and workarounds being identified in Austria and Norway.[517] According to the Siemens-time.lex study, eSignatures remain a significant interoperability barrier, and a real challenge to cross border public procurement.[518]

Although identification and authentication play a role in several eProcurement phases, the main field of application seems to be the submission phase. Therefore, the examples presented in the following refer mainly to the submission of tenders.

1. Solutions without Advanced Electonic Signatures / Qualified Electronic Signatures:
   - Submission of an unsigned electronic file and simultaneously, via ordinary mail, a paper standard form – generated by the eProcurement website itself and linked to the digital transmission – duly signed by the company's legal representative ("Mantelbogen" as for instance in use in Germany in the cities of Frankfurt[519], Düsseldorf[520] and Berlin[521]).
   - User-ID and password-based model, in which the user is signing an offer by uploading it to an eProcurement website after simple online registration that did not use any PKI components (Irish "eTenders procurement website").[522]
   - Major Contracting Authorities such as the European Commission (through Europaid or as the World Bank) accept very simple solutions such as a PDF document send via email.[523]

These options seem not to pose any interoperability barriers, including cross-border.

2. Solutions with Advanced Electronic Signatures / Qualified Electronic Signatures
   - The tenderer prepares the tender along with the necessary documentation on his local system, which is thereafter signed using signature software installed locally (e.g. using MS Word or Adobe PDF Writer). The resulting documents are thereafter electronically signed, and can be sent to the contracting authority in any supported way (e.g. via e-mail, ftp, uploading it to a specific website, mailing a CD-ROM containing the signed offer, etc.). E.g. Estonian Digidoc software.[524]

[516] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 308.

[517] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 311.

[518] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 311.

[519] www.vergabe.stadt-frankfurt.de

[520] www.duesseldorf.de/hauptamt/publikationen/vergabe.pdf

[521] www.vergabeplattform.berlin.de

[522] www.etenders.gov.ie

[523] PEPPOL, Response to Green Paper on eProcurement, 2011, p. 8.

[524] See www.sk.ee/pages.php/02030501

- The contracting authority requires the use of an eProcurement website which incorporates an electronic signing module. E.g. French Place de Marché Interministérielle.[525]
- The tenderer prepares his tender entirely online, e.g. by filling out the characteristics of his supplies/services in an eCatalogue preparation module. In this case, no upload of a tender document will be required, and the signature will be placed in the same way as in the example above: a signature module integrated into the website will be loaded, followed by the request to select a certificate and enter the appropriate PIN code. E.g. Cypriot eProcurement platform.[526]

All these options do pose interoperability barriers.

In this context, it should be noted that PEPPOL seeks to demonstrate that validation of certificates used to generate the eSignatures from different certificate authorities across Europe could be done through PEPPOL solutions and services, and that certificates from more than 300 certificate authorities can be validated through a PEPPOL service from March 2011.[527]

3.3.3 Risks assessment and recommendations

According to the procurement Directive, any solution should ensure integrity and confidentiality of tenders, whereas the question of authentication and identification depend mostly on national legislation.

Therefore, from a procurement Directive perspective, it has to be evaluated if the different options mentioned above sufficiently ensure integrity and confidentiality. In addition, it must be examined which solution in place is proportionate to ensure authentication and identification, also compared to the requirements for paper-based procurement.

The crucial question is whether the qualified electronic signature, which the Action Plan and the Directive emphasise, is really necessary and proportionate to the risks encountered in eProcurement.

On the one hand, only qualified electronic signatures guarantee a reasonable possibility of determining the reliability at a cross border level. They are not only the most secure and legally unambiguous signature type, but were seen to be the one with the greatest interoperability potential.[528] For other types of signatures, contracting authorities receiving a signed bid will have difficulties in determining the reliability (from a practical perspective, however, even the reliability of qualified signatures will be hard to determine for contracting authorities without sufficient technical know-how).[529]

On the other hand, interoperability of qualified electronic signature is not yet reached (see also chapter 2) and (cross-border) implementation seems complex and costly. In contrast, with the Irish username/password-based model a third of all companies in Ireland already used e-procurement last year[530] – mainly due to the fact that no advanced electronic signature or qualified electronic signature is required. This model does not pose any interoperability barriers, including cross-border.

[525] https://www.marchespublics.gouv.fr

[526] https://www.eprocurement.gov.cy/ceproc

[527] PEPPOL, Response to Green Paper on eProcurement, 2011, p. 7.

[528] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 304.

[529] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 313.

[530] Deutsche Bank, 2011 – Chart 7.

As long as integrity and confidentiality of the offers are ensured, there is no obvious reason not to choose this model. As regards identification, the situation is similar to the paper-based situation: In practise, the contracting authority often does not know – and does not control - if the person who signed the (written) offer is really legitimate to sign it. Why should then an eProcurement solution require higher standards than a paper-based one? However, for such systems, it is important that a security token is downloaded from the contracting authority website to ensure that the documents being submitted are protected against tampering.[531]

As regards the legal effectiveness of the declarations, qualified electronic signature must not necessarily be compulsory for the submission act, as long as the final contract is duly signed (e.g. with a qualified electronic signature, but in this case only the best bidder has to handle with the technical barriers).

Not to be recommended is, however, the approach with a handwritten signed attachment to be sent via ordinary mail. Although identification/authentication does not pose a problem due to the handwritten signature, it should only be seen as a transitional solution between paper-based and digital communication.

3.4. Further steps for a wider use of eProcurement in Europe

To bring forward the standardisation process as a key issue in eProcurement, a close coordination between the different EU-financed projects is necessary. To avoid the emergence of (again) differing standards, common standards should be developed within the existing system of CEN/ BII2.

It would also be helpful to clarify certain general questions with regard to the use of e-procurement in the Directive; besides, some of the obstacles could be removed by legislative modification, such as an improvement of mutual recognition of certificates, the permission of self-declarations on the fulfilment of the selection criteria and modifications to enhance the use of Dynamic Purchasing System (DPS).

Moreover, more efforts could be done to overcome language barriers.

The sections above have shown that a number of achievements with regard to eProcurement have been reached in Europe, however these are mostly implemented at national level only.

The Siemens TimeLex Study on the evaluation of the action plan for electronic procurement[532] has evaluated the remaining barriers and suggests some further steps. Also the Green Paper on eProcurement[533] has addressed necessary policy improvements and has asked for response regarding the addressed measures.

In the following chapter, the suggestions made for further steps will be described and evaluated.

[531] EC, Evaluation of the 2004 Action Plan for EPP, p. 113.

[532] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 344 ff.

[533] EC, Green Paper on expanding the use of eProcurement, 2010, p. 11 ff.

3.4.1 Convergence of existing initiatives towards common solutions

The different initiatives described before (see 3.1.3.2.) should be further encouraged. To avoid, however, the emergence of (again) differing standards, there should be a close coordination between the different programs. In response to the issues addressed by the green Paper, PEPPOL pointed out, that it has to be recognized that eProcurement standards are part of global business and consists of standards from various organizations which are continuously evolving.[534] To avoid a piecemeal approach, common standards should be developed within the existing system of CEN/ BII2.

PEPPOL suggests further the appointment of a Coordination Authority to provide governance of any common European eProcurement infrastructure service. This authority should ensure the close collaboration between ePRIOR, eCERTIS and PEPPOL.[535]

We also deem close coordination between the different EU-financed projects as vital for the advancement of eProcurement. The creation of a new institution, however, should only be further developed if other means of coordination fail.

3.4.2 Legislative obligation to use eProcurement?

A possible next step could also be the introduction of a legal obligation of contracting authorities to admit electronic tenders. Among stakeholders, as first evaluations of the responses to the Green paper suggest[536], there is no clear tendency with regard to this aspect:

In favour of this approach it could be argued that the (lack of) development in the past years has proven that the member states will not develop the necessary momentum by their own initiative. Consequently, a strong EU, imposing the use of eProcurement seems to be necessary to build up the necessary pressure needed to overcome the tendency to cling to "old solutions".

The opposing view points out that mandatory eProcurement would mean to make the third step before the first: Without a solution for the numerous challenges cross-border eProcurement has to face, mandatory eProcurement could not be efficiently installed. Further it is argued, that this approach would be in conflict with the principles of the Protocol on Services of General Interest, guaranteeing local authorities the right to decide independently how to provide, commission and organise such services.[537]

In our view, the concept of mandatory eProcurement imposed by the EU should, if at all, only be a long term concept with a realistic period of transition. The mandatory use could give the overall idea of eProcurement some momentum; however, an overall concept with major assisting measures (see below) would be essential. Otherwise this would entail the risk of reducing the participation in public tender procedures, particularly with regard to the participation of SMEs.

Therefore, the focus should be to ensure interoperability and common standards, while the decision whether to implement mandatory eProcurement solutions should be taken by the Member state.

[534] PEPPOL, Response to Green Paper on eProcurement, 2011,p.9.

[535] PEPPOL, Response to Green Paper on eProcurement, 2011, p.6.

[536] Presentation « Green paper on eProcurement-First analysis of responses", slide 7.

[537] CEMR Response, Green Paper on eProcurement, 2011, p. 4.

3.4.3 Creation of incentives

The Siemens-time.lex study emphasises the importance of simplification: eProcurement should not only be a transposition of the elements of "paper procurement", but has to be simpler than traditional procurement, if uptake is to be achieved.[538] Also the Green Paper addresses how eProcurement could be made more attractive for all relevant stakeholders.[539]

The following measure have been suggested:

- Further reduced time scales by using eProcurement.[540] This, however, as the Green paper correctly points out, may have negative effects on the quality of the tenders handed in.
- Shift of responsibility regarding the legality of the procurement proceedings from the contracting authority to the provider.[541] This proposal however, seems to be difficult as long as common requirements are not yet developed. Such principles for a recognised eProcurement system would be a necessary precondition.

3.4.4 Clarification/ modification of the Directives

More helpful in our view would it be to clarify certain general questions with regard to the use of eProcurement in the Directive; also some of the obstacles mentioned could be removed by legislative modification.

Clarification: use of eProcurement does not constitute discrimination

There are still some reservations among contracting authorities with regard to the general idea of eProcurement. It should be clarified that the use of eProcurement in all phases of the procurement will not be seen as discrimination against those suppliers not equipped with the appropriate technologies.[542] This clarification might not necessarily be part of the new Directive but could also be part of an informal guidance paper issued by the European Commission.

Cross border acceptance of certifications: modification with regard to the acceptance of self-declarations

As described before, the acceptance of certifications regarding the selection criteria is one of the obstacles for cross-border eProcurement. Also in conventional procurement procedures, however, this aspect leads to limited cross-border competition.

As described above[543], the PEPPOL program provides for the development of a so-called Virtual Company Dossier. This approach should be further encouraged.

A further possible measure to improve mutual recognition of certificates discussed within the context of the general reform of the Directives is the creation of a Europe-wide pre-qualification system.[544] This approach would lead to the question by whom such a system would be constituted.

[538] Study on the evaluation of the Action Plan for electronic procurement, 2010, p. 350.
[539] EC, Green Paper on expanding the use of eProcurement, 2010, p. 12.
[540] EC, Green Paper on expanding the use of eProcurement, 2010, p. 12.
[541] EC, Green Paper on expanding the use of eProcurement, 2010, p. 12.
[542] CEMR Response, Green Paper on eProcurement, 2011, p. 6.
[543] See 3.2.3.2.
[544] EC, Green Paper on the modernisation of EU public procurement policy, 2010, p. 31.

Additionally or in the meantime until one of the before mentioned solutions has been established, it could be foreseen to demand documents and certificates only of the successful bidder or the bidders admitted to the award phase. For all other bidders during the procurement procedure, a self-declaration on the fulfillment of the selection criteria could be sufficient. However, the contracting authority would have the possibility to request the documents at any moment during or even after the procurement procedure for fraud prevention purposes. This would make the process simpler and result in savings.[545] Also, this would reduce the administrative burden, particularly for SMEs, without compromising the guarantees for making sound choices.[546]

Consequently, the focus on the use of self – declarations should be stressed in the Directive.

Language barrier: Mandatory second language?

With regard to the language barrier it is further discussed whether contracting authorities should be obliged to draw up tender specifications for high-value contracts in a second language or to accept tenders in foreign languages.[547] This, however, would entail major transaction costs for contracting authorities. Only in certain situations where sufficient competition without additional measures cannot be expected, this could be useful. The decision should, however, be taken by the contracting authority.

Modification regarding use of DPS

To improve the use of DPS in practice, it is suggested[548] to modify the Directive in so far as a call for competition necessary according to Art. 33 (5) of Directive 2004/18/EC could be limited to those economic operators who have submitted an indicative tender and fulfil the qualification criteria of the DPS. The existence of the DPS could be continuously indicated on TED and possible to search by interested economic operators. This suggestion seems to be feasible and appropriate to make the use of this instrument more popular.

3.4.5 Raise awareness and build capability

All legal and technical measures should be accompanied by a program of capacity building with regard to people working in administration also as for the side of the bidders, with particular focus on SMEs.

Further, the benefits of eProcurement solutions have to be communicated more concisely among all relevant stakeholders. www.epractice.eu seems to be a useful platform. As intended by the European Commission’s eGoverment Action Plan, it should be developed into an effective tool for exchange of experience and information for practitioners.

[545] CEMR Response, Green Paper on eProcurement, 2011, p. 6.

[546] EC, Green Paper on the modernisation of EU public procurement policy, 2010, p. 31, PEPPOL, Response to Green Paper on eProcurement, p. 3.

[547] EC, Green Paper on the modernisation of EU public procurement policy, 2010, p. 31.

[548] PEPPOL; Response to Green Paper on eProcurement, page 7; CEMR Response, Green Paper on eProcurement, 2011, p. 6.

3.4. Conclusion

Standardisation issues are paramount if the needed advancement of eProcurement is to be achieved. The closely coordinated activities of the existing initiatives seem to be an appropriate basis for further steps. This, however, will mainly not be subject to legislative measures. Other aspects, as clarifying the leeway for practical eProcurement solutions, should be addressed by EU legislation.

Any legislative proposals to simplify the use of eProcurement, however, should be integrated into the planned review of the main public procurement directives. This would reflect the need to facilitate cross border participation also in traditional tender procedures and enable the legislator to find a coordinated approach. This would apply, for instance, with regard to the possibility to accept self-declarations as proof of the eligibility.

Of course this does not make activities at national level dispensable. However, if the challenges with regard to cross-border use, especially the lack of standards, the non-acceptance of certifications and the language barrier, shall be overcome, a stronger lead has to be taken by the EU.

REFERENCES

[BSI, 2006] German Federal Office for Information Security (BSI), *Grundlagen der elektronischen Signatur*, March 2006, Available at:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/esig_pdf.pdf?__blob=publicationFile

[CEMR Response, Green Paper on eProcurement, 2011] CEMR response to European Commission Green Paper on expanding the use of E-Procurement COM (2010) 571 final 18.10.2010, Available at:

http://www.ccre.org/prises_de_positions_detail_en.htm?ID=118

[Council, European eJustice Action Plan] COUNCIL, MULTI-ANNUAL EUROPEAN E-JUSTICE ACTION PLAN 2009-2013, 2009/C 75/01, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:075:0001:0012:EN:PDF

[CWA 14167-1] CEN Workshop Agreement, CWA 14167-1: Security requirements for trustworthy systems managing certificates for electronic signatures – Part 1: System Security Requirements, June 2003, http://www.dnielectronico.es/seccion_integradores/cwa14167-01-2003-Jun.pdf

[CWA 14167-2] CEN Workshop Agreement, CWA 14167-2: Security requirements for trustworthy systems managing certificates for electronic signatures – Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP), March 2002, http://www.interlex.it/testi/pdf/cwa14167-2.pdf

[CWA 14169] CEN Workshop Agreement, CWA 14169: Secure signature-creation device, March 2002, http://www.a-sit.at/pdfs/cwa14169.pdf

[CROBIES Study, 2010]

SEALED-Siemens-time.lex, *CROBIES-Study – cross-border interoperability of eSignatures: definition of common requirements*, External study for the Commission, July 2010,

Available at: http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm

[HD] Head Document, July 2010,

Available at: http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd0.pdf

[WP 1] Common Supervision Model of Practices of Certification Service Providers issuing Qualified Certificates, July 2010,

Available at: http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd1.pdf

[WP 2-1] "Trusted Lists" – Implementer's Guide, July 2010

Available at:

http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd2.1.pdf

[WP 2-2] "Trusted Lists" – User's Guide, July 2010

Available at:

http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd2.2.pdf

[WP 3] Interoperable Qualified Certificate Profiles, July 2010

Available at:

http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd3.pdf

[WP 4] Framework for Secure Signatures Creation Devices cross-border recognition, July 2010

Available at:

http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd4.pdf

[WP 5-1] Guidelines and guidance for cross-border and interoperable implementation of electronic signatures, July 2010

Available at:

http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd5.1.pdf

[WP 5-2] Quality Classification Scheme for eSignature elements, July 2010

Available at:

http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd5.2.pdf

[WP 5-3] Note on the "Algo Paper" issue, July 2010

Available at:

http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd5.3.pdf

[DATEV eG, 2003] *Stellungnahme der DATEV eG Nürnberg zur Evaluierung der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*, 19/08/2003, Available at: http://www.datev.de/portal/ShowContent.do?pid=dpi&cid=20138

[Decision 2003/511/EC] European 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*, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:175:0045:0046:EN:PDF

[Decision 2000/709/EC] European Commission, *Decision 2000/709/EC of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures*, Available at:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:289:0042:0043:EN:PDF

[Decision 2010/425/EU] European Commission, *Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States*, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:199:0030:0035:EN:PDF

[Decision C(2010)8467] European Commission, *Decision C(2010)8467 of 2 December 2010 setting up a European Multi-Stakeholder Forum on electronic Invoicing (eInvoicing)*, Available at :

http://ec.europa.eu/internal_market/payments/einvoicing/index_en.htm

[Decision 2011/130/EU] European Commission, *Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market*, Available at:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:EN:PDF

[Deloitte, 2009] Deloitte, *Final Evaluation of the IDABC Programme*, Report to the European Commission, January 2009, Available at: http://ec.europa.eu/idabc/servlets/Doccb6b.pdf?id=32117

[Deutsche Bank, 2011] Deutsche Bank Research, *EProcurement – public procurement worth two trillion euros needs smarter spending*, February 2011, Available at: http://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000269867.pdf

[Directive 77/388/EEC] Sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonization of the laws of the Member States relating to turnover taxes - Common system of value added tax: uniform basis of assessment, Available at:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31977L0388:en:HTML

Directive 1999/93/EC see [eSignature Directive]

[Directive 2001/115/EC] Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax, available at:http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001L0115&model=guichett

[Directive 2004/17/EC] 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, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0017:en:NOT

[Directive 2004/18/EC] Directive 2004/18/EC of 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, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0018:en:NOT

[Directive 2006/112/EC] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, available at: http://eur-lex.europa.eu/Result.do?T1=V3&T2=2006&T3=112&RechType=RECH_consolidated&Submit=Search

Directive 2006/123/EC see [Services Directive]

[Directive 2010/45/EU] Council Directive 2010/45/EU of 13 July 2010 amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing, available at:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:189:0001:0008:EN:PDF

[EC, Action Plan for EPP, 2004] European Commission, *Action Plan for the implementation of the legal framework for electronic public procurement*, December 2004, Available at: http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/actionplan/actionplan_en.pdf

[EC, Action Plan on eSignatures and eID, 2008] European Commission, *Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, 28*/11/2008, COM(2008) 798 final, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

[EC Action Plan on eSignatures and eID, main undertakings] Europe's Information Society Thematic Portal, *Main undertakings under the Action Plan*, Available at: http://ec.europa.eu/information_society/policy/esignature/action_plan/undertakings/index_en.htm

[EC, A Digital Agenda for Europe, 2010] European Commission, *A Digital Agenda for Europe, Communication from the Commission to the European Parliament, the Council, the*

European Economic and Social Committee and the Committee of the Regions, COM (2010) 0245 final, May 2010, Available at: http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf

[EC, Europe 2020], European Commission, *Europe 2020, A European Strategy for smart, sustainable and inclusive growth*, COM(2010) 2020, available at: http://europa.eu/press_room/pdf/complet_en_barroso___007_-_europe_2020_-_en_version.pdf

[EC, Evaluation of the 2004 Action Plan for EPP] European Commission, *Commission staff working document – Evaluation of the 2004 Action Plan for electronic public procurement*, SEC(2010) 1214, 18/10/2010, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2010:1214:FIN:EN:PDF

[EC, Final report of the Expert Group on eInvoicing, November 2009], Available at: http://ec.europa.eu/enterprise/sectors/ict/files/finalreport_en.pdf

[EC, Green Paper on the modernisation of EU public procurement policy, 2010] European Commission, *Green paper on the modernisation of EU public procurement policy Towards a more efficient European Procurement Markt, COM (2011)15 fina, January 2011, Available at:*

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:DKEY=556316:EN:NOT

[EC, Green Paper on expanding the use of eProcurement, 2010] European Commission, *Green Paper on expanding the use of eProcurement in the EU*, COM(2010) 0571 final, October 2010, Available at: http://ec.europa.eu/internal_market/consultations/docs/2010/eProcurement/green-paper_en.pdf

[EC, Legal barriers in eBusiness, 2004] European Commission, *Commission staff working paper – Legal barriers in e-business: The results of an open consultation of enterprises*, SEC(2004) 498, 26/04/2004, Available at: http://ec.europa.eu/enterprise/sectors/ict/files/legal_barriers_sec_2004_498_en.pdf

[EC, Reaping the benefits of electronic invoicing for Europe, 2010*]* European Commission, *Reaping the benefits of electronic invoicing for Europe, communication from the commission to the European parliament, the council, the european economic and social committee and the committee of the regions*, COM(2010)712, 2/12/2010, Available at:

http://ec.europa.eu/internal_market/payments/einvoicing/index_en.htm

[EC, Operation of eSignature Directive, 2006] [COM(2006) 120 final] European Commission, *Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures*, report from the Commission to the European Parliament and the Council, COM(2006) 120 final, 15/03/2006, Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0120:FIN:EN:PDF

[EC, Standardisation Mandate M/460, 2009] European Commission, *Standardisation mandate to the European Standardisation Organisations CEN, CENELEC AND ETSI in the field of information and communication technologies applied to electronic signatures*, M/460 EN, 22/12/2009, Available at: http://www.etsi.org/WebSite/document/aboutETSI/EC_Mandates/m460.pdf

[EC, Digital Agenda Website, 2010] European Commission Information Society, 2010, *A Digital Agenda for Europe*, Available at: http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[e-Certificates Study, 2008]

Siemens, *e-Certificates Study – Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures*, External study for the Commission, September 2008

[Final Report] Strategy and implementation roadmaps, September 2008, Available at:

http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/ecertificates_country_en.pdf

[National Reports] eProcurement – national reports, May 2007, Available at: http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/ecertificates_country_en.pdf

[National Country Profiles] European eProcurement schemes (WP 1) – National Country Profiles, May 2007, Available at: http://ec.europa.eu/idabc/servlets/Docd9cf.pdf?id=31578

[EFVS Study]

Siemens, SEALED, time.lex, *Study on European Federated Validation Service (EFVS)*, External study for the Commission, 2009/2010, Available at:

http://ec.europa.eu/idabc/en/document/7764.html

[Analysis & Assessment Report, 2009] Siemens, time.lex, *Feasibility and global implementation plan, Analysis and Assessment of the solutions, D 2.1, D 2.2, D 2.3*, September 2009,

Available at: http://ec.europa.eu/idabc/servlets/Doc31a6.pdf?id=32388

[Common Solution Model Report, 2009] Siemens, time.lex, *Analysis and Assessment, Common Solution Model, D 2.4, D 2.5, D 2.6*, September 2009,

Available at: http://ec.europa.eu/idabc/servlets/Doce7b7.pdf?id=32389

[CSM – Final Report, 2010] SEALED, time.lex, *Completion of the framework for Signature Validation Services, Common Solution Model, D 3.4, D 3.5, D 3.6*, Final Report, March 2010,

Available at: http://ec.europa.eu/idabc/servlets/Docf934.pdf?id=32633

22 Solution profiles for verification and validation,

Available at: http://ec.europa.eu/idabc/en/document/7764.html

[ELDOC Study, 2006] ELDOC *Legal Study on Legal and Administrative Practices regarding the Validity and Mutual Recognition of Electronic Documents, with a view to identifying the existing legal barriers for enterprises*, External Study for the DG Enterprise & Industry of the European Commission, November 2006, Available at: http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3121

[Final Report] Final Report, November 2006, Available at:http://ec.europa.eu/enterprise/sectors/ict/files/dumortier-final-report-draft_en.pdf

[Country Profiles] First Interim report (Country reports), July 2006, Available at: http://ec.europa.eu/enterprise/sectors/ict/files/legal-validity-32-nat-reps_en.pdf

[ELSIGN Study, 2003] Interdisciplinary centre for Law & Information Technology, Katholieke University Leuven, *The legal and market aspects of electronic signatures: Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EEA, the Candidate and the Accession countries*, External study for the Commission, Leuven, 2003, Available at: http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

[eSignature Directive] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:EN:PDF

[Green Paper on e-Procurment -first Analysis, of responses], Aviaillable at: http://www.epractice.eu/files/12%20GreenBook.pdf

[International Handbook of Public Procurement], edited by Khi V. Thai, 2009

[NTC, 2004] NTC Network training and consulting – Mehr Sicherheit durch PKI-Technologie, 04.06.2004, Available at:

http://www.networktraining.de/downloads/Mehr%20Sicherheit%20durch%20PKI-Technologie.pdf

[PEPPOL eInvoicing Pilot Specifications] PEPPOL eInvoicing Pilot Specifications report, Available at : www.peppol.eu/work_in_progress/wp5-einvoicing/results

[PEPPOL Website, WP 1 eSignature]:

http://www.peppol.eu/work_in_progress/wp-1-esignature (and subpages:)

http:/www.peppol.eu/work_in_progress/wp-1-esignature/project-plan

http:/www.peppol.eu/work_in_progress/wp-1-esignature/results/signature-validation-infrastructure-online

http:/www.peppol.eu/work_in_progress/wp-1-esignature/results/deliverable.1.2

http:/www.peppol.eu/work_in_progress/wp-1-esignature/results/deliverable-1.1/first-deliverable-of-wp1-has-been-released

http:/www.peppol.eu/work_in_progress/wp-1-esignature/current-status

[PEPPOL, Response to Green Paper on eProcurement, 2011] Peppol, *Response to the Green Paper on expanding the use of eProcurement in the EU*, January 2011,

Available at: http://www.peppol.eu/News/news-archive/20110131%20PEPPOL%20response%20to%20GREEN%20PAPER%20on%20eProcurement.pdf/at_download/file

[Preliminary Study on Mutual Recognition of eSignatures, 2007]

Siemens-time.lex, *Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications*, Report, November 2007,

Available at: http://ec.europa.eu/idabc/servlets/Docba2e.pdf?id=29484

29 National profiles, Available at: http://ec.europa.eu/idabc/en/document/6485.html

[Ramboll Management, 2006]

Ramboll Management, *Benchmarking of the existing national legal e-business practices, from the point of view of enterprises, with particular emphasis in the field of e-signature, eInvoicing as well as contract conclusion and implementation*, External study for the European Commission, Draft Final Report, November 2006, Available at:

http://www.epractice.eu/files/media/media_483.pdf

[Roßnagel, 2003] Roßnagel, Alexander, *Eine konzertierte Aktion für die elektronische Signatur*, Multimedia und Recht 2003, p. 1.

[Roßnagel, 2008] Roßnagel, Heiko, *Mobile qualifizierte elektronische Signaturen. Analyse der Hemmnisfaktoren und Gestaltungsvorschläge zur Einführung*, Dissertation Frankfurt a.M., 2008.

[Services Directive] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, Available at:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:376:0036:0068:EN:PDF

[Signature Perfect, 2008] Signature Perfect, *Leitfaden Elektronische Signatur (Signaturen mit und ohne Zertifikate, Signaturen mit eigenhändigen Unterschriften)* in Zusammenarbeit mit SigLab, Version 5, Release Date 4. December 2008, Available at:

http://www.signature-perfect.de/docs/Leitfaden_Elektronische_Signatur.pdf

[STORK Website, 2011] *Secure Identity Across Border Linked*, 2011, Available at: https://www.eid-stork.eu/

[Study on eID Interoperability for PEGS, 2009] Siemens-time.lex, *Study on eID Interoperability for pan-european eGovernment services (PEGS): Update of Country Profiles* External Study for the Commission, December 2009, Available at: http://ec.europa.eu/idabc/en/document/6484.html

[WP 1] Analysis and Assessment Report, October 2009, Available at:

http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521

[WP 2] Quick Wins, November 2009, Available at:

http://ec.europa.eu/idabc/servlets/Docb482.pdf?id=32522

[WP 3] Memorandum of Understanding, December 2009, Available at:

http://ec.europa.eu/idabc/servlets/Doccdcd.pdf?id=32523

32 country profiles on national eIDM schemes, Available at: http://ec.europa.eu/idabc/en/document/6484.html

[Study on electronic documents and electronic delivery, 2009]

Siemens-time.lex, *Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive*, February 2009, Available at:

http://www.epractice.eu/en/library/314375

[WP 1] National country profiles, 24.02.2009, Available at: http://ec.europa.eu/idabc/servlets/Doca132.pdf?id=32143

[WP 2] Analysis of country profiles, 30.01.2009, Available at: http://ec.europa.eu/idabc/servlets/Doc6b0c.pdf?id=32144

[WP 3] Recommendations on improving the cross border exchangeability of electronic documents and interoperability of delivery systems for the purposes of the implementation of the Services Directive, 25.02.2009, Available at:

http://ec.europa.eu/idabc/servlets/Doc7679.pdf?id=32145

[Study on Mutual Recognition of eSignatures, 2009]

Siemens-time.lex, *Study on mutual recognition of eSignatures: update of Country Profiles*, Analysis & assessment report, October 2009, Available at: http://ec.europa.eu/idabc/servlets/Doca7bf.pdf?id=32436l

32 National profiles, Available at: http://ec.europa.eu/idabc/en/document/6485.html

[Study on Standardisation Aspects of eSignature, 2007]

SEALED-DLA Piper-Across communications, *Study on the standardisation aspects of eSignature*, External study for the Commission, November 2007,

[Final Report], Available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/esignatures/e_signatures_standardisation.pdf

[ExS], Executive Summary, Available at:

http://ec.europa.eu/information_society/policy/esignature/docs/standardisation/e_sign_executive_summary.pdf

[Study on the evaluation of the Action Plan for electronic procurement, 2010]

Siemens-time.lex, *Study on the evaluation of the Action Plan for the implementation of the legal framework for electronic procurement (Phase II)*, External study for the Commission, July 2010, Available at:

http://ec.europa.eu/internal_market/consultations/docs/2010/eProcurement/siemens-study_en.pdf

GLOSSARY

Advanced Electronic Signature	AES	As defined in Art. 2.2 of the eSignature Directive, an *advanced electronic signature* means an *electronic signature* that meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Asymmetric Cryptoalgorithms		*Asymmetric cryptoalgorithms* are specific algorithms that are widely used for the creation of *electronic (digital) signatures* or the asymmetric encryption of secret documents. Each user holds a complementary pair of keys: one key for encryption and a second key for decryption. An electronic signature can be created through the signatory's private key by encrypting the so-called "hash value" (meaning a digest of the original document) which can be decrypted by the receiver with the signatory's commonly accessible public key. The positive comparison between the hash-value of the document and the decrypted hash-value thereby ascertains the integrity of the document. The two keys are connected through a mathematical one-way function to assure that the private key cannot be deducted from the public key.
Asymmetric Cryptographie		The term *Asymmetric Cryptography* is used here to describe a widely used method to create electronic signatures on the basis of *asymmetric cryptoalgorithms*.
Authentication service		*Authentication services* mean services that support the *electronic authentication* of a person or entity.
Certificate		As defined in Art. 2.9 of the eSignature Directive, a *certificate* means an electronic attestation which links signature-verification data to a person and confirms the identity of that person.
Certification Service Provider	CSP	As defined in Art. 2.11 of the eSignature Directive, a *certification service provider* means an entity or a legal or natural person who issues *certificates* or provides other services related to *electronic signatures*.
Digital Signature		*Digital signatures* are *electronic signatures* based on *asymmetric cryptoalgorithms*.
Electronic Authentication	eAuthentication	The term "*eAuthentication*" is used here as user authentication, i.e. the process by which a service confirms the claim of a user to use a specific identity by the use of credentials (and not within the meaning of "data authentication").
Electronic Identification	eIdentification / eID	*Electronic Identification* means the process by which the identity of a user is established. *Electronic identification* is often required for the access to and use of electronic procedures. It gives individuals the assurance that no unauthorised use is made of their identity and personal data and enables e.g. administrations to make sure that the individuals are the persons they claim to be and have the rights they claim to have.
Electronic Identity	eID	An *electronic identity* means an electronic representation of a certain subset of one or more attributes pertaining to a person/entity. While a person/entity has only one identity, it may have many *electronic identities*. *Electronic identities* can take many forms and can be stored on many different types of media.

Electronic Identity card	eID card	An *electronic identity card* is one of many tokens that can be used to support an *electronic identity*. It contains credentials, i.e. information attesting to the integrity of identity attributes.
Electronic registered mail service		*Electronic registered mail services* are services of secure and reliable electronic data transfer which have emerged in several member states. Such services may for example include the possibility for the sender to receive proof of sending and/or delivery to the addressee.
Electronic Signature	ES	As defined in Art. 2.1 of the eSignature Directive, an *electronic signature* means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.
Identification service		*Identification services* means services that support the *electronic identification* of a person or entity.
Public Key Infrastructure	PKI	*Public Key Infrastructure* is the infrastructure based on *asymmetric cryptography* used by a trusted third party to issue digital *certificates*.
Qualified Certificate	QC	As defined in Art. 2.10 of the eSignature Directive, a *qualified certificate* means a *certificate* which meets the requirements laid down in Annex I of the eSignature Directive and is provided by a *certification service provider* who fulfills the requirements laid down in Annex II of the eSignature Directive.
Qualified Electronic Signature	QES	A *qualified electronic signature* is an *advanced electronic signature* based on a *qualified certificate* and which is created by a *secure signature creation device*.
Secure Signature Creation Device	SSCD	As defined in Art. 2.6 and 2.5 of the eSignature Directive, a *secure signature creation device* means configured software or hardware which is used to implement the signature creation data and which meets the requirements laid down in Annex III of the eSignature Directive.
Signatory		As defined in Art. 2.3 of the eSignature Directive, a *signatory* means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents.
Supervision		The term "*Supervision*" is here used in the meaning of the eSignature Directive (recital 13, Art. 3.3, Art. 11). The Directive provides that member states shall establish an appropriate system allowing the supervision of *certification service providers* which are established on their territory and issue *qualified certificates* the public in order to ensure the supervision of compliance with the provisions laid down in the eSignature Directive.
Signature Policy		*Signature Policy* means a set of rules for the creation and *validation* of *electronic signatures* that defines the technical and procedural requirements for creation, validation and (long term) management of these *electronic signatures*, in order to meet a particular business need, and under which the *electronic signatures* can be determined to be valid.
Signature validation		*Signature validation* means a *signature verification* during which specific additional validation data collected by the *signatory* and/or a *verifier* (e.g. *certificates*, revocation status, *time stamps*) are needed to verify the *electronic signature*.
Signature verification		*Signature verification* means the process performed by a *verifier* after the creation of an *electronic signature* to determine if an *electronic signature* is valid.

Time stamp		A *time stamp* is the electronic certification of a *certification service provider* that certain electronic data were presented to it at a certain point in time. Time stamps can be used to document the moment in time before which or in which an *electronic signature* was created.
Trusted list	TL	As defined in Art. 2 of Commission Decision 2009/767/EC a '*Trusted List*' means a list containing the minimum information related to the *certification service providers* issuing *qualified certificates* to the public who are supervised/accredited by them. The *Trusted Lists* aim at providing reliable information in particular on the relevant services offered by the listed *certification service providers* and their *supervision*/accreditation status in order to facilitate the validation of electronic signatures supported by the listed certification service providers.
Trust Service Provider	TSP	A *trust service provider* means a (certification service) provider offering one or more (electronic) Trust Services meaning services which enhance trust and confidence in electronic transactions (typically but not necessarily involving cryptographic techniques or confidential material).
Unique identifier		A *unique identifier* is an attribute or a set of attributes of a person or entity which uniquely indentifies the person or entity within a certain context, e.g. a national number, certificate number, etc.
Validation Service Provider	VSP	A *validation service provider* is a *certification service provider* offering *signature validation* services.
Voluntary Accreditation		As defined in Art. 2.13 of the eSignature Directive, *Voluntary Accreditation* means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the *certification service provider* concerned, by the public or private body charged with the elaboration of, and *supervision* of compliance with, such rights and obligations, where the *certification service provider* is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Economic and Monetary Affairs
- Employment and Social Affairs
- Environment, Public Health and Food Safety
- Industry, Research and Energy
- Internal Market and Consumer Protection

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.

ISBN