scripted

Volume 9, Issue 1, April 2012

INFORMAL DEBATE ON THE ISSUES RELATING TO TERMINOLOGY AND CLARIFICATION OF CONCEPT IN RESPECT OF THE EU E-SIGNATURE LEGISLATION

Stephen Mason[*]

Abstract

The aim of this paper is to provide a high level analysis of (i) the three forms of electronic signature addressed by the Directive, "simple", "advanced" and "qualified"; (ii) the definition of "the signatory"; (iii) the definition of "secure signature-creation-devices" (SSCDs), and (iv) the meaning of "e-Signature in the public sector", incorporating definitions of legal terminology from a number of Member States that has led to different terminology or to different effects in the implementation of the eSignature Directive.

Consideration is also given to the different solutions advanced at national level, and how these might constitute best (or worst) practices to be taken into account at European level.

The paper provides critical views on the definitions and offers a commentary on the advantages and drawbacks of the current Directive. It highlights other possible options and proposals, and provides suggestions for improvement while assessing the consequences of these suggestions for the future of e-Signature and of the IAS framework as a whole.

DOI: 10.2966/scrip.090112.82

[*] Barrister. This Report was requested by the European Commission under the terms of the e-ID Compass Project: Advice on key issues related to the E-signature Directive Revision (relevant for the IPTS Knowledge Repository eID Compass) – appointment number 152391-2011 A08-UK. The EU approved the Final Report on 2 November 2011.

1. Introduction: The Present Position

By way of introduction, it will be helpful to make some observations of a fundamental nature in relation to the function that a manuscript signature can perform. The importance of considering this matter cannot be over-emphasised, bearing in mind the significance of the proposed revision of the e-Signature Directive.

The function of a manuscript signature is generally determined by the nature and content of the document to which it is affixed. This means a manuscript signature has a variety of purposes. Arguably, the primary evidential function is as follows:[2]

> It is suggested that the primary purpose of a signature serves to provide admissible and reliable evidence that comprise the following elements:
>
> (a) To provide tangible evidence that the signatory approves and adopts the contents of the document.
>
> (b) In so doing, the signatory agrees that the content of the document shall be binding upon them and shall have legal effect.
>
> (c) Further, the signatory is reminded of the significance of the act and the need to act within the provisions of the document. [3]

There are other, secondary and further functions, which include the provision of evidence of identification and authentication. It should be noted that some jurisdictions place a greater emphasis on the manuscript signature to determine authorship, and thereby authenticity, as a primary purpose. Other considerations (this is not exhaustive[4]) include to establish the identity of a particular characteristic, attribute, or status of the person (such as a government minister or company director); the existence of a signed document to provide a record of the intent of the signatory, and to demonstrate that the content of the document has not been altered subsequently to the affixing of the signature.

Policy makers in the United Nations and the European Union combined these functions when developing the legislation and Model Laws to provide for electronic signatures (*Model Law on Electronic Commerce 1996*, *Model Law on Electronic Signatures 2001* and the *UN Convention on the Use of Electronic Communications in International Contracts 2005*). In retrospect, it seems that it was intended to combine a number of the various features of a manuscript signature into an electronic signature. Two issues of relevance arise as a consequence:

> 1. It is not possible to combine all the various functions of a manuscript signature into an electronic signature. This is partly because it is not possible to foresee the context of the signing process with electronic signatures.

---

[2] For a more detailed consideration of the various purposes that a manuscript signature can perform, see *UNCITRAL Model Law on Electronic Commerce: Guide to Enactment*, para 48.

[3] S Mason, *Electronic Signatures in Law*, 3rd ed (Cambridge: CUP, 2012), at ch 1.

[4] See *Ibid* for an exhaustive analysis and a list of relevant references.

> 2. Arguably, it is neither desirable nor necessary to combine the functions that a manuscript signature is capable of conveying in the digital environment.

The issues that arise in respect of electronic signatures have been recognized by way of the *Feasibility Study on an Electronic Identification, Authentication and Signature Policy* (IAS) SMART 2010/0008. There are three aspects to the SMART study that are distinct, both in the physical and the virtual worlds, and relevant to the topic of this paper: identification, authentication and signatures. These are treated separately in the physical world but there is confusion about their treatment in the virtual world.

This paper will focus on the relationship between these three issues within the contexts of the SMART study and the various reports written for the European Union over the years. A further consideration might usefully be included in any debate that policy makers may consider when taking into account the future of the Directive. Art 5(1) has created what is termed the "qualified electronic signature" that in turn, in accordance with subparagraph (a), satisfies "the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data". However, because digital documents will be used increasingly as the future unfolds, it is debatable whether it is appropriate for the concept of an electronic signature to be predicated on the various functions that have been historically attributed to the manuscript signature in circumstances when manuscript signatures are no longer used.[5]

2. Problems

Given that signatures have certain legal implications, and a vast array of electronic forms of signature are wide-spread across the globe (typing a name in an e-mail; the name in an e-mail address; PIN; "click" wrap method; a manuscript signature that has been scanned; the biodynamic version of a manuscript signature; a digital signature), it is questionable whether an electronic signature should be connected to a form of electronic authentication, as provided by art 2(1) of the Directive.

2.1. Separating Identity, Authentication and the Function of the Signature

The legal aspects of identity and authentication have recently been explored in detail in Europe[6] and the American Bar Association is considering similar issues.[7]

---

[5] This was observed by G Dimitrov, *Liability of Certification Service Providers: How the Providers of Certification Services Related to Electronic Signatures Could Manage their Liabilities* (Saarbrucken: VDM Verlag, 2008), at 300, who noted that Professor Dumortier identified this tendency in his "The European Regulatory Framework for Electronic Signatures: A Critical Evaluation" in R Nielsen, *S* S Jacobson and J Trzaskowski (eds), *EU Electronic Commerce Law* (Copenhagen: DjOF Publishing, 2004) 69–95.

[6] N Bohm and S Mason, "Identity and its Verification" (2010) 26 *Computer Law & Security Review* 43-51. The practical issue relating to the content and verification of eID are covered in T Myhr "Regulating a European eID: A Preliminary Study on a Regulatory Framework for Entity Authentication and a Pan European Electronic ID for the Porvoo e-ID Group", 6.2 and, more recently and more thoroughly, in the "Study on eID Interoperability for PEGS: Update of Country Profiles Analysis & Assessment Report (D2.1 Report on analysis and assessment of similarities and differences; D2.2 Report on impact on eID interoperability)" (IDABC, October 2009) http://ec.europa.eu/idabc/en/document/6484.html.

The EU has recognised that there is a need to reconsider the effect of the e-Signature Directive, and in so doing, to take an expansive view of what might be changed, if modifications are considered to be appropriate. In this spirit, it is possible to return to fundamental legal principles and more fully understand what the technology is capable of, so as to provide for the three different but interlocking elements: identification, authentication and signatures.

In the main, much of the debate on electronic signatures, as exhibited by the various useful reports produced for the European Union (listed below), focuses on the interoperability of the digital signature regimes (advanced electronic signatures and qualified electronic signatures) implemented by Member States. The reader will observe that advanced electronic signatures and qualified electronic signatures are equated with digital signatures (which is what they are), but this misses the point. In virtually all of the literature produced for the European Union on this topic, authors refer to "electronic signatures" when they actually mean "digital signatures" or advanced electronic signatures and qualified electronic signatures. This may appear to be a semantic point but the use of language and the assumptions behind its use have a tendency to reinforce what constitutes an electronic signature. If we continue to fail to understand what we mean by an electronic signature, there is a danger that any revision of the e-Signature Directive will not be effective.

As noted above, there are different types of electronic signature, and the digital signature is only one version of an electronic signature. To imply that electronic signatures are not used commercially over the internet to buy and sell goods and services is far from correct, and such comments (and beliefs) act to distort the debate. Indeed, people enter contracts regularly by exchange of e-mails, with their names typed at the bottom of their e-mails. This form of electronic signature is both acceptable and legally enforceable, depending on the substantive law of the Member State.

It is essential to understand why so much commercial activity takes place over the Internet between consumers and businesses with the use of one particular form of electronic signature, the "I accept" icon. For instance, when an airline sells an e-ticket on-line, it carries out checks as the potential customer provides each item of personal information. The identity of the customers is authenticated by cross checking their addresses against other databases and, perhaps, their passport numbers. The customer does not see this cross checking, and does not need to see it working. The payment mechanism additionally acts to reinforce the accuracy of the data provided by the customers in relation to their identities and addresses, because the airline will ensure that the method chosen to pay for the e-ticket is capable of authenticating the identity of the customers. Invariably thieves will use the identity of another person to attempt to buy travel tickets, but the industry has obviously taken the view that the risks are such that they can be accommodated within the business model.

Given the technology and the nature of the interconnected databases that are now available, it is suggested that the European Union could take a world lead in this matter, and provide for the separation of identity, authentication and the signature. To

---

[7] Federated Identity Management Legal Task Force: http://www.abanet.org/dch/committee.cfm?com=CL320041.

highlight some of the practical problems, the legislation from five Member States is considered in brief below.[8]

2.2. The Form of Electronic Signature

This section demonstrates how the provisions of the Directive have been transposed into national law. It will be observed that in the selection noted below, as well as from the reports initiated by the European Union over the previous ten years, Member States have not necessarily implemented the provisions of the Directive by adopting the actual text of the Directive.

2.2.1. Belgium

The Belgian legislation has not provided alternative definitions of the three forms of electronic signatures, but has adopted the definitions almost word for word from the Directive. The legislation has not awarded a higher value to any of the forms of electronic signatures, although in practice, the current legislation favours the use of qualified electronic signatures because of the interaction between the rules of evidence and the assimilation principle (article 4, §4 of the Law of 9 July 2001). The assimilation principle effectively requires the courts to assimilate an electronic document signed with a qualified electronic signature with a "common (electronic) deed". In all other cases, at least in theory, there remains a margin for discussion and interpretation, which is limited by the conditions set out in article 1322 of the Civil Code and the non-discrimination principle.

Simple electronic signatures have been used and enforced in many commercial matters as evidence by presumptions and inferences, due to the commercial evidence regime being open. In general, any evidence is allowed in commercial matters. There has been extensive case law in relation to the use of manuscript signatures that are scanned and subsequently placed in an electronic document.

The case law relates to the use of such an electronic signatures mechanism by the Office for Foreigners in the context of immigration decisions. Even though the use of this type of electronic signature was initially rejected by various courts, the Council for Alien Claimants has enforced this electronic signature mechanism applied by the Office for Foreigners upon multiple occasions. The electronic signature mechanism used by the Office of Foreigners consisted of a combination of an electronic representation of a manuscript signature (scan) with additional security measures. This case law is also important because it seemingly confirms that accessory (security) procedures may have an effect on the assessment a court makes under art 1322 of the Belgian Civil Code. This implies that the intrinsic lack of an electronic signature to comply with the requirements of art 1322 of the Belgian Civil Code could be remedied by additional measures and procedures.

---

[8] The author thanks Johan Vandendriessche, Advocaat, Advocatenkantoor Johan Vandendriessche BVBA (http://www.adv-vandendriessche.be); George Dimitrov, PhD, Partner at Dimitrov, Petrov & Co (http://www.dpc.bg); Alexandra Heise, Rechtsanwältin, Fachanwältin für Gewerblichen Rechtsschutz and Dr Christian Lemke, Rechtsanwalt, Fachanwalt für Gewerblichen Rechtsschutz and Fachanwalt für Informationstechnologierecht of Heissner & Struck (http://www.heissner-struck.de) and Michael G Rachavelias, LLM, Senior Partner at Rachavelias & Partners Law Office (http://www.prlawyers.gr/) for taking time out of their busy working days to help by providing me with information about their respective jurisdictions.

There has been case law in relation to PINs, but this is not generally useful in relation to the assessment of the validity of PINs as simple electronic signatures, because PINs are generally governed by "evidence agreements" that provide a legal framework between the parties in relation to the value of the evidence value.

2.2.2. Bulgaria

The Bulgarian legislation strictly transposes the definitions set out in the Directive in respect to the types of the signatures. In the Bulgarian language, they are translated as follows: the simple signature is not translated as such. It is named only as electronic signature (art 13, para 1 of the *Law on Electronic Documents and Electronic Signatures*). The qualified signature is recognised as a handwritten signature in respect to all subjects, while the basic and advanced is recognised as handwritten if the parties agree so.

There is no case law to date.

2.2.3. Germany

In Germany, the legislation has provided slightly alternative definitions of these three forms of electronic signature that are different from that set out in the Directive (the writing in italic indicates the differences form the definitions set out in the 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

An "advanced electronic signature" means an electronic signature which is uniquely linked to the *owner of the signatory key*, capable of identifying the *owner of the signatory key*, created using means that the *owner of the signatory key* can maintain under his sole control and is linked to data to which it relates in such a manner that any subsequent change of data is detectable.

A "qualified electronic signature" is an advanced electronic signature based on a qualified certificate *which is valid at the time of creating the electronic signature* and which is created by a secure-signature-creation device.

The German law uses the phrase "owner of the signatory key" instead of "signatory". The "owner of a signatory key" is a natural person who holds a signatory key. Further and for qualified electronic signatures, the relevant signature-creation data needs to be assigned to the owner of a signatory key by the means of a qualified certificate.

"Simple electronic signatures" may be used to conclude a contract and can be considered as declarations of intent; however, it might be difficult to prove such a declaration was made as well as its content. Thus, there is the question of the evidentiary value of simple electronic signatures. Courts will consider simple electronic signatures freely as evidence.

Qualified electronic signatures have the same legal effect as a handwritten signature, § 126 a "Bürgerliches Gesetzbuch" (BGB – German Civil Act). If the written form is statutory, only qualified electronic signatures may replace the handwritten signature unless there is any prohibition in law. Further and according to § 371a "Zivilprozessordnung" (ZPO - German Code of Civil Procedure), qualified electronic signatures are admissible as evidence in legal proceedings as prima facie evidence. Their authenticity may only be questioned if there are substantial doubts that the

statement was made by the owner of the private signature key. Thus, the evidentiary value of qualified electronic signatures is much higher.

2.2.4. Greece

The Directive was implemented in Greek law with Presidential Decree 150/2001 (published in the *Official Gazette of the Government* (FEK A') 125/25.6.2001). In essence, the Greek legislator adopted the text of the Directive, rather than adding to or modifying the text, although the Greek law deviates from the Directive in that the Greek legislation uses the terminology "digital signature" disjunctively with the definition "advanced electronic signature", although it complies with the four characteristics that are set out in the Directive.

Although the presidential decree focuses, in the main, on the use and consequences of advanced electronic signatures, the recognition of "simple" electronic signatures is not hampered. This discrimination between the two forms of electronic signature is observed in respect of the formation of contracts, depending on whether the Greek law requires a contract to be in writing or not. Where it is essential for a contract to be in writing, only an advanced electronic signature can be used, while the use of a simple electronic signature will unavoidably lead to the invalidity of the document; only in instances where the parties are free to choose the form of their contractual relationship, can a "simple" electronic signature be used validly.

A debt submitted that comes from an agreement that was concluded by way of e-mail was recognized in a payment order decision (Court of First Instance of Athens, 1327/2001) (MonPrAth 1327/2001), published in [2001] NoB; and a simple electronic address (unique for each user) has the character of a manuscript signature (Court of First Instance of Athens, 1963/2004) (MonPrAth 1963/2004) and (Court of First Instance of Athens 6302/2004 (MonPrAth 6302/2004); note also a more recent case, Court of First Instance of Athens 8444/2011 Payment Order, published in EfAD 5/2011 (ΕΦΑστΔ 5/2011).

2.2.5. United Kingdom

The *Electronic Communications Act 2000* does not incorporate any of the definitions of electronic signature into domestic legislation, although the *Electronic Signatures Regulations 2002* (SI 318/2002) introduces the various definitions provided in the Directive verbatim. In English law, a document is signed or it is not. There is no distinction between types of electronic signature, although it is acknowledged that digital signatures have the capacity to provide more evidence with which to counter repudiation than do simple electronic signatures.

2.3. The Definition of "Signatory"

The definition of "signatory" (art 2(3)) provides that only a natural person is capable of being in possession of a signature-creation device, which (arguably) must be right. A legal entity is an artificial construct, and being incorporeal, is not capable of being a signatory. Only a human being, with appropriate authority, can be a signatory for and on behalf of a legal entity.

However, note the discussion in Hans Graux, Guy Lambert, Brigitte Jossin and Eric Meyvis,[9] where some of the correspondents taking part in the study thought that qualified certificates could be issued to legal entities. However in reality, qualified certificates were issued to a natural person in their role as an officer or representative of the legal entity, with the exception of Estonia, the Czech Republic (it is called an "electronic mark" which is more accurate, or perhaps it might be called an "electronic seal", which is even more relevant), Greece (for which see below) and Slovakia.

2.3.1. Belgium

The definition of "the signatory" has intentionally not been implemented under Belgian law, which uses the concept "holder of a certificate" as an alternative. The concept of "signatory" is deemed to be inappropriate by the Belgian legislator in legislation that governs the rights and obligations of the persons to whom certificates are issued.

The "holder of the certificate" is defined as "a natural or legal person to whom a certification-service-provider has issued a certificate" (art 2, 5° of the Law of 9 July 2001). The concept of the "holder of the certificate" must be distinguished from the concept of the "holder of the signature-creation device" which is not defined by the Law of 9 July 2001. The Belgian legislator is of the opinion that the holder of the signature-creation device is not necessarily the person to whom the certificate was issued. General legal principles determine the relationship between the "holder of the certificate" and the holder of the signature-creation device (e.g. contractual or extra-contractual liability in case of issues regarding the representation of the "holder of the certificate"). Especially in relation to legal persons, the relationship between the "holder of the certificate" (i.e. the legal person) and the holder of the signature-creation device (in principle, the legal representative of the legal person) is defined by the legal principles that apply to the representation of those legal persons.

2.3.2. Bulgaria

Under Bulgarian law a "signatory" is a natural person who is the author of the signed message. He or she is the one who holds the signature-creation device. This is because only a natural person is capable of legally expressing valid will, even when he or she does so on behalf of a legal person. The person, on whose behalf a statement is made, is referred to as a titular (owner). His or her property is affected by the signed message by the author. The titular could be listed in the qualified certificate (in the named field "owner"), but this is not necessary, when from the statement it becomes clear that the author acts as a proxy of another person.

2.3.3. Germany

The owner of a signatory key can only be natural a person, in accordance with the provisions of SigG.

2.3.4. Greece

---

[9] *Study on Mutual Recognition of e-Signatures: Update of Country Profiles Analysis & Assessment Report* (IDABC European eGovernment Services, October 2009) 89–91.

The definition of "signatory" is provided in art 2 §3 of Presidential Decree 150/2001, and includes a legal person "that holds a signature-creation device and acts either on his own behalf or on behalf of another natural or legal person or entity he represents".

2.3.5. United Kingdom

The *Electronic Signatures Regulations 2002* (SI 318/2002) introduces the definition of "signatory" where this means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the person he represents.

This definition differs from that provided in the Directive, in that it misses out the words in square brackets, although there is no material difference. In the Directive, "'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".

Schedule 1 to the *Interpretation Act 1978* provides a definition of "person", which "includes a body of persons corporate or unincorporate".

The definition provided in the Statutory Instrument includes the ability of a person to sign on behalf of a legal entity.

2.4. The Definition of "Secure Signature-Creation-Device"

The Directive provides, in art 2(6) that a secure signature-creation-device is "a signature-creation device which meets the requirements laid down in Annex III". The concern is whether or not there is a requirement to obtain a formal conformity assessment regarding a device before it can legally be considered a secure signature-creation-device. In Belgium, Bulgaria and Germany, an assessment must be made of such a device in accordance with national legal requirements. Given that there is no reference to the term in the legislation in the United Kingdom, the only reference that relates to the "secure signature-creation-device" is on the web site of the Cabinet Office in relation to the guidelines that are under review that should be used when assessing such devices.[10] Secure signature-creation-devices are used in the United Kingdom because they enforce certain security aspects. That they are not certificated with qualified status is generally because of the issues pertaining to liability.

2.4.1. Belgium

The regime of electronic-signature products is set out in arts 6 and 7 of the Law of 9 July 2001:

> Art 6. If an electronic-signature product corresponds with the standards, of which the reference numbers are published in the Official Journal of the European Union in accordance with the procedure provided by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, this product shall be considered as complying with the requirements of annex II, littera f), and annex III of this law.
>
> Art 7. § 1. The requirements concerning secure-signature-creation device are listed in Annex III of this law.

---

[10] http://interim.cabinetoffice.gov.uk/govtalk/schemasstandards/e-gif/technical_standards_catalogue/e-servicesaccess.aspx.

> § 2. The competent organisms, appointed by the Public Service, shall confirm the conformity of the secure-signature-creation devices with the requirements listed in Annex 3 of this law. The list of appointed organisms shall be transmitted to the European Commission.
>
> § 3. The King shall determine the requirements, which the abovementioned organisms must meet.
>
> § 4. The conformity determined by another organism, appointed by another Member State of the European Economic Area, shall be recognised in Belgium.

Art 7, §2 of the Law of 9 July 2001 provides that the conformity with the legal requirements shall be confirmed by an appointed organisation.

2.4.2. Bulgaria

The "secure signature-creation device" has its definition set forth by the law, set out in line with the requirements of Annex III of the Directive. However, art 6 of the *Regulation on the Requirements to the Algorithms for Qualified Electronic Signature* explicitly envisages that the conformity of the SSCD with the statutory requirements shall be ascertained by a relevant certificate, issued by a laboratory duly accredited to perform such conformity assessments.

2.4.3. Germany

Electronic-signature products need to be registered. The fulfilment of the requirements laid down in the SigG and SigV need either to be announced to and/or confirmed by a public authority, the "Bundesamt für Sicherheit in der Informationstechnik" (BSI – Federal Office for Information Security).

Producers of electronic-signature products need to ensure that the signature-creation device detects the forgery of a signature and falsification of the signed data. Moreover, they are required to be protected, in a reliable manner, against unauthorised use by others. Thus, the signatory key can only be used after its owner has been identified either by means of "possession of the signature creation device and knowledge" or "possession and one or more biometric data", while the signatory key is not disclosed. It must be impossible to calculate the signature key knowing the signature verification key or the signature or to duplicate signatory keys.

Regarding the presentation of data that is to be secured by e-signing, the device needs to be clear and without ambiguity that an e-signature will be created, and to which data it refers. With respect to the verification of data which has been secured by e-signing, the secure signatory creation devices need to provide verification regarding the following:

> (i) which data refers to the e-Signature
>
> (ii) whether the data been altered
>
> (iii) the owner of the signature key to whom the signature belongs
>
> (iv) the content of the qualified certificate that has been the basis of the e-signature, showing the attribution certificates
>
> (v) the result of the check regarding the assignment of a signature verification key to an identified person by a qualified certificate.

If applicable, the devices need to give reference to the content of the data signed. Further and amongst other attributes, the devices need to provide for:

> (i) the creation and transfer of the signatory key can only occur once and that their secrecy is assured and that storage outside the signature-creation device is not possible
>
> (ii) qualified certificates are protected against unauthorised alteration and unauthorised release
>
> (iii) qualified time stamps cannot be forged and adulterated
>
> (iv) the blockings of keys are shown and blockings cannot be reversed unnoticed.

2.4.4. Greece

The definition of a "secure-signature-creation device" in art 2 §6 of Presidential Decree 150/2001 is the same as in the Directive, and article 4 §4 provides that certification services are not subject to any prior provision of licensing or authorisation.

The inspection of Certification Service Providers is assigned to the National Telecommunications and Post Commission (EETT), as predicted in art 4 §§2, 8 of the Presidential decree. This commission has issued a regulation on the Conformity Assessment of Secure Signature Creation Devices and Secure Cryptographic Modules (regulation 295/64/2003, which was published in the Official Government Gazette – FEK B' 1730/24.11.2003).

2.4.5. United Kingdom

The *Electronic Signatures Regulations 2002* (SI 318/2002) do not provide a definition of "secure signature-creation-device".

2.5. The Meaning of "e-Signature in the Public Sector"

The use of electronic signatures in the public sector is, apparently, not clear. Art 3(7) of the Directive provides that:

> Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

Where additional requirements are imposed by Member States, the question is what the effect might be of such requirements, given that any additional requirements must be "objective, transparent, proportionate and non-discriminatory". Some Member States have decided to use qualified electronic signatures for such purposes, whilst the United Kingdom does not appear to have taken any legal or regulatory view of the matter. In a study conducted by Ralf Cimander and others, the difficulties in relation to the use of electronic signatures in e-procurement were highlighted against a number of Member States – a state of affairs that illustrated the diverse approaches adopted

amongst the Member States when interpreting the provisions of the Directive in the light of cultural and legal customs.[11]

2.5.1. Belgium

Art 4, §3 of the Law of 9 July 2001 sets out the regime in relation to electronic signatures in the public sector:

> §3. The King may impose, by Decree decided upon after deliberation in the Council of Ministers, additional requirements for the use of electronic signatures in the public sector. Such requirements shall be objective, transparent, proportional and nondiscriminating and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

The additional criteria may only be imposed (i) when they are objective, transparent, proportional and nondiscriminating, (ii) may only relate to the specific characteristics of the public sector application and (iii) may not constitute an obstacle to cross-border services for citizens.

The royal decree mentioned in art 4, §3 of the Law of 9 July 2001 has not yet been enacted.

In the public sector, the legislation often requires particular requirements for the use of electronic signatures, e.g. the use of the qualified certificate contained in the Belgian electronic identity card.

2.5.2. Bulgaria

Bulgaria has enforced the *E-governance Act* whereby it introduces some requirements of using e-signature in the public sector for the purposes of provision of e-government services. The requirements are that

> (i) only qualified e-Signatures could be used for provision of e-government services where the special laws require signature as a mandatory requisite under the application for provision of the service;
>
> (ii) the acts of the administrative authorities in electronic form should only be signed by qualified e-Signatures;
>
> (iii) it is not permitted to use qualified certificates where only the pseudonym of the signatory is entered for the purposes of the provision of e-government services;
>
> (iv) qualified certificates could include the name of the owner on whose behalf the application is filed, but this is not necessary. It may become clear from the application.

2.5.3. Germany

According to § 1 III SigG, legislative provisions may make the use of qualified electronic signatures for administrative public activities subject to possible additional

---

[11] R Cimander, M Hansen and H Kubicek, *Electronic Signatures as Obstacle for Cross-Border E-Procurement in Europe Lessons from the PROCURE-project* (Institut für Informationsmanagement Bremen GmbH, June 2009).

requirements. Such requirements shall be objective, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned.

One of these legislative provisions is § 3a *Administrative Procedures Act* ("VwVfG" – Verwaltungsverfahrensgesetz). For the communication between government agencies and a citizen, it provides that:

> (i) The transmission of electronic documents shall be permissible provided that the recipient provides this possibility.
>
> (ii) Where the written form is stipulated by law, this may be replaced by electronic form unless otherwise required by law. In this event, the electronic document shall bear a qualified electronic signature in accordance with the Electronic Signature Act. Signing with a pseudonym which does not provide for authentication of the person who is the owner of the signatory key is not permitted.
>
> (iii) Where an electronic document transmitted to the government authority is not suitable for processing by it, it shall inform the sender without undue delay, stating the technical specifications that apply. Where a recipient claims that he is unable to process the electronic document transmitted by the government authority, it shall send it to him again in a suitable electronic format or as a written document.

Thus, providing there are no specific requirements for the form of communication, electronic communication is allowed if both the government agency and the citizen have access to electronic communications. However, the realisation as well as details and interpretation of the clause are still developing in Germany.

Similar provisions are laid down in § 87a of the Fiscal Code of Germany ("AO" – Abgabenordnung), however, further and specific rules apply.

2.5.4. Greece

The Greek legislator has not implemented any additional requirements in the use of electronic signatures in the public sector, as no such provision is included in Presidential Decree 150/2001.

Recently, law 3979/2011 has been enacted (*Official Government Gazette* – FEK 138/16.6.2011), which deals with the integrity and evidential weight of electronic documents that are produced by the public sector (art 13). According to the first two paragraphs of art 13, electronic documents that are drafted by public sector departments must have an advanced electronic signature of the authorised person that is based on a qualified certificate and is created by a secure-signature creation device. These electronic documents have the same legal and evidential weight with documents that are manually signed and stamped. Furthermore, in the second paragraph, it is also required that "electronic administrative documents must necessarily have secure time stamp". The provisions of this law are very recent and have not yet been tested in the courts.

2.5.5. United Kingdom

There are no provisions relating to electronic signatures in the public sector that require a particular form of electronic signature.

In summary, the foremost concerns relating to the e-Signature Directive are as follows (this list is not exhaustive):

1. A misunderstanding of what constitutes an electronic signature (the vast majority of lawyers and judges across the globe do not even have sufficient grasp of what is a simple concept, and to have three different forms of electronic signature only adds to the confusion[12]) – this has been exacerbated because the PKI industry wanted to sell digital signatures (which in turn purport to offer proof of identity and authentication), and used a variety of mechanisms to influence politicians and policy makers on this topic.

2. The definition of an electronic signature, as provided by art 2(1) of the Directive, confuses the purpose of the signature by referring to it serving as a "method of authentication", rather than as a mechanism that demonstrates the will of the signatory in approving and adopting the contents of the document.

3. The introduction of different forms of electronic signature is not helpful ("electronic signature", also referred to as a "simple" electronic signature; "advanced electronic signature" and "qualified electronic signature"). The definitions of "advanced electronic signature" and "qualified electronic signature" refer to the mechanisms used by which the form of the electronic signature is reinforced by technology, with the aim of providing for a higher degree of assurance that the data has not altered or is not capable of being altered without it being made manifest, and purportedly to demonstrate identity.

4. As a corollary to 3 above, a great deal of time and money has been spent by the European Union in dealing with the difficult problem of providing for the interoperability of the technology related to PKI, and much of the work has failed to provide for certainty.

5. Member States have implemented the e-signature Directive in different ways. The confusion that abounds rests partly on the way the Directive has been implemented, partly on the cultural and legal norms of each Member State, and partly because of the rules of evidence in each Member State.

3. A Brief Review of How Others Propose to Solve the Problems Identified

3.1. Amending the Directive

The general consensus has been, from the first report by Professor Dr Jos Dumortier and his colleagues in 2002, that the objective of the Directive has not been met,[13] but other authors have generally refrained from suggesting that the Directive should be revised. One reason for resisting a review of the Directive is because it would cause Member States to reconsider the issues of authentication and electronic signatures. On more than one occasion it has been suggested that the Commission should provide clarification of the provisions of the Directive, but bearing in mind that the legal

---

[12] This is also remarked upon by S Lacroix et al, *Study on the Standardisation: Aspects of e-Signature* (EU DG Information Society and Media, Final Report dated 22 November 2007), 24; see also A Srivastava, "Businesses' Perception of Electronic Signatures: An Australian Study" (2009) 6 *Digital Evidence and Electronic Signature Law Review* 45–65.

[13] Although for the view that the objectives have been "largely fulfilled", see 5.1, at 10 of the *Report on the operation of Directive 1999/93/EC on a Community Framework for Electronic Signatures*, COM(2006) 120 final, 15 March 2006.

status of the different forms of electronic signature differ from one Member State to another, this will not be an easy document to produce. In addition, it is debatable what status, if any, such a document would have in legal proceedings.

However, in 2011, Dr Annette Rosenkötter and her colleagues recommended a comprehensive review of the Directive,[14] although they also suggested that if this was not considered to be appropriate, the Commission might contemplate issuing a non-binding document with a view to interpreting the Directive and to clarify specific issues. For the reasons noted above, such a document would not be of much help.

3.2. Technical Issues

All of the issues relating to Certification Service Providers, Trust Service Providers, accreditation, signature-creation devices, the qualified electronic signature, non-discrimination and standardisation have been covered with regularity across both legal and technical reports (for which see the bibliography). The lack of standard approaches to the technology and the different ways in which Member States have implemented qualified electronic signatures represent the reality of dealing with a number of Member States that have different legal and cultural approaches to electronic signatures and how to respond to them. In addition, a significant number of people in business, when asked about the use of advanced electronic signatures and qualified electronic signatures, are not able to see the benefit of them, nor understand why they are so complex, lack operability and are so expensive.

3.3. Cross-border Interoperability

The problems relating to cross-border interoperability are closely linked to the various difficulties identified under "technical issues". The general tenor of the response by most of the authors of the reports on this topic suggests that the increased use of advanced electronic signatures or qualified electronic signatures will resolve the issue. However, the imposition of advanced electronic signatures or qualified electronic signatures is not politically or culturally acceptable to some Member States who have no wish or intention to operate such systems (for instance, the eCODEX project is predicated on the use of PKI). There is also a substantial difficulty with cross-border interoperability in the perceived lack of trust in the advanced electronic signatures and qualified electronic signatures issued by Member States: some Member States do not or will not trust the advanced electronic signatures and qualified electronic signatures issued by other Member States.[15]

3.4. Comment

---

[14] A Rosenkötter et al, *Digital Internal Market Study* (Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Internal Market and Consumer Protection, IP/A/IMCO/ST/2011-04, June 2011), at 8 and 54-55.

[15] On this point, VASCO Data Security International placed DigiNotar, the Dutch certificate authority it owned into voluntary bankruptcy on 20 September 2011 at the Haarlem Court. This was because DigiNotar issued a fraudulent certificate to an unknown person in the name of Google on 10 July 2011, which was used to make a number of attacks on the internet. It appears that DigiNotar may have issued as many as 531 certificates that were not issued correctly. The Dutch government subsequently regained control over DigiNotar's intermediate certificate, and replaced the certificates that could not be trusted with new ones from another provider. For the interim report by Fox-IT, see http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html.

Given that Rosenkötter and her colleagues have provided an up-to-date and comprehensive analysis of the problems (legal, technical, trust and practical issues), it is not proposed to rehearse these again. In a recent article, Hans Graux indicated that the legal framework is unclear and ambiguous, the technical framework is out of date and the trust framework is vague. He noted that the legal framework

> mainly covers e-signatures to the exclusion of any other service using, or ancillary to, electronic signatures, such as time-stamping services, long term archiving services, electronic registered mail, or signature validation services.[16]

This analysis is sound. Each of these additional services have been noted and commented upon by all of the other authors of the reports listed in the bibliography, and they are of relevance in the digital environment.

It is necessary to reconsider the Directive in the light of how people use changing technology. There is a greater emphasis on identity and authentication now than hitherto. Graux has proposed the development of a coherent and comprehensive framework for the services around authenticity. This must be the central thrust for the future, but it is essential to separate identity, authentication and the function of the signature.

4. Legal Analysis and Proposed Remedy

Humans have only recently stumbled into the virtual world, in which digital technology has become the dominant form of communication in an exceedingly short time. This new dimension to life has been rapidly taken up across the globe. Invariably, the technology has provided opportunities and created difficulties (especially by criminals using the technology to the detriment of others).

The technology has also caused us to reconsider certain fundamental issues that are central to the provision of a safe online environment for ordinary people. The state, through its organs, is responsible for providing a framework of rights and obligations within which citizens are able to conduct their daily lives with a degree of certainty. It is for this reason that consideration is given to the risks that accompany the virtual world. Threats can only be ameliorated: they cannot be eliminated. However, this does not prevent risk being assessed with a view of introducing a proportionate response. The need to have systems in place for authenticity and integrity and for detecting the forgery of information has always been present in human discourse, hence the development of the profession of the notary.

In the twenty-first century, it is imperative to formulate an appropriate response to these same issues (identity, authenticity, integrity and trustworthiness). In so doing, it is necessary to accept that any response should be different to the physical world, because in the virtual world, criminals have a greater ability to undermine any process put in place because of a single, important and inherent weakness that few acknowledge: poor quality software.[17] Unless it is accepted that any process devised

---

[16] H Graux, "Rethinking the e-Signatures Directive: On Laws, Trust Services, and the Digital Single Market" (2011) 8 *Digital Evidence and Electronic Signature Law Review* 9-24, at 16.

[17] For an analysis, see S Mason, *Electronic Evidence*, 2nd ed (LexisNexis Butterworths, 2010), at ch 5.

in the virtual world is open to being subverted or successfully undermined, those responsible for attempting to produce certainty in the digital environment only give a false sense of safety to the end user (the banks continually misinform their customers in this way with the "security" that 'protects' debit and credit cards).

4.1. The Current Directive

It is not necessary to rehearse the disadvantages of the Directive. The various reports summarised above illustrate the problems in detail. However, two issues will be considered here, one of which is more significant than any other, and which ought to be taken into account during the course of the debate in reassessing the Directive.

First, until the Member States of the European Union form a united political entity (if this ever happens), the European Union continues to comprise separate sovereign states. Each Member State will continue to enact legislation in accordance with its cultural and legal customs. In this respect, each Member State has enacted legislation relating to electronic signatures in a slightly different manner to that proposed in the Directive. That this has occurred should not be a surprise. What also should not astonish observers is that few practical problems have occurred in relation to electronic signatures, other than in relation to the technical issues surrounding PKI for advanced electronic signatures and qualified electronic signatures.

For instance, e-commerce has continued to thrive, and governments have set up various mechanisms to permit their citizens to obtain electronic access to a range of central and local government services. It is regularly noted that because the method employed to obtain access to a government portal by each Member State differs, it effectively means that citizens of other Member States that wish to interact with another Member State are at a disadvantage. In theory, this must be right. In practice, it has to be questioned whether spending vast amounts of money on a single method of authentication across the European Union will achieve what the proponents of such a system wish to accomplish, notwithstanding that some Member States will not, for political and cultural reasons, want to adopt the particular form of authentication that might be proposed (for instance, some Member States neither wish to introduce identity cards nor adopt log-on methods that use PKI), whatever the technical solution might be.

In response to this first point, any change to the Directive should take the autonomy of Member States into account, and refrain from attempting to find and then impose a single solution on all Member States. Variety is crucial. Acknowledging the legal and cultural conventions of Member States provides for more harmony. At this point, it is relevant to point out that special rules were not drafted to cover the legal ramifications of signatures on telegrams, telex of facsimile transmissions, yet commerce was not hindered for the lack of any legislative certainty. It is therefore questionable as to why different forms of electronic signature were incorporated into the Directive, given the different rules across Member States regarding the evidential value to be given to a particular form of electronic signature.

The second observation relates to the definitions of "electronic signature" provided in the Directive. With respect to those responsible for drafting the text of the Directive, in retrospect, the definitions were inherently going to cause problems. A number of different concepts were included in the Directive, each of which is more usefully separated to prevent confusion and to simplify the purpose of the Directive.

The definition of electronic signature is provided in art 2(1), and "means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication". The problem with this definition is that it does not provide for the intent to sign, which is a central rationale for the use of a signature. The other forms of electronic signature, the advanced electronic signature and the qualified electronic signature, are merely digital signatures using PKI that are defined by a set of characteristics. Both forms of signature can be removed in their entirety from the Directive with no ill effect. From a policy perspective, it is not desirable to provide for technologically specific forms of electronic signature in legislation, because the technology will change, and such forms of electronic signature will inevitably become obsolete as new forms of technology are developed.

4.2. Options

The following options are proposed:

> 1. Identity, authentication and signature in the virtual world should be treated separately.
>
> 2. That the e-signature Directive be:
>
> (a) repealed and a new Directive introduced to accommodate each of the separate concepts of identity, authentication and signature, or
>
> (b) the e-signature Directive is amended to make it simpler to understand and to provide for legal certainty, with a single definition of "electronic signature".

4.2.1. Suggestions for Improvement

The federal legislation relating to electronic signatures in the United States of America is the *Electronic Signatures in Global and National Commerce Act* (E-SIGN), 15 USC §§ 7001-7003. S 106(5) provides a definition of electronic signature that might be considered to be more pertinent to the fundamental purpose of a signature:

> The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

This definition is all encompassing, in that any form of electronic signature is provided for, whatever its technical characteristics. In addition, the issue of authentication is removed and the definition only deals with the intent to sign. This is a simpler definition than that provided by art 7 of the *UNCITRAL Model Law on Electronic Commerce,* and closer to the definition provided in article 2(a) of the *UNCITRAL Model Law on Electronic Signatures*:

> "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.

Unfortunately, art 2(a) defines the signature in relation to two of the functions a signature is capable of performing, which, it is suggested, is no longer desirable to combine in the virtual world.

Given the attributes of the technology, it is pertinent to adjust the notion of signature, identity and authentication. It is necessary to simplify these concepts to reflect what the virtual environment is capable of achieving. By doing so, it is possible to provide adequate technical responses to each. It is no longer appropriate to include all of these concepts into a single definition of the notion of "signature", otherwise confusion abounds. That is what has inadvertently occurred with the e-signature Directive.

The following definition of electronic signature is proposed for discussion:

> "electronic signature" means data in electronic form, incorporated into or otherwise logically associated with any electronic data or communication, and adopted by a person with the intent to indicate their approval and agreement to the content.

It will be noted that this definition narrows the scope of the purpose of the signature. As previously indicated, a manuscript signature has a number of different functions. It is now time to re-consider the analogy between manuscript signatures and electronic signatures by restricting the meaning of an electronic signature to a specific purpose: that of providing for the will of the person to approve and agree to the content. Proof of identity and authentication of identity (and, perhaps, authentication of the signature) are more usefully separated from this process. It may be necessary to consider the meaning of the words "electronic data or communication" to differentiate between the signing of a communication and the signing of data, because each term may have different consequences, depending on the definitions of these terms in the legislation of individual Member States.[18]

The aim is not necessarily to abolish the concepts of "advanced electronic signature" and "qualified electronic signature", although the "advanced electronic signature" seems somewhat otiose, given the concept of the "qualified electronic signature". In any event, both forms of signature fit within the definition of "electronic signature". What each of these forms of electronic signature attempt to do with the use of technology is to make them more secure and to provide for authenticity.

By adopting a wide definition of electronic signature, each Member State will be free to determine their use for each form of signature (as is presently the case), and work can continue at a European Union level under the rubric of identity and authenticity, as proposed by the "Feasibility Study on an Electronic Identification, Authentication and Signature Policy" (IAS), thus removing the concept of the signature from the notion of identity and authentication.

5. Assessment

5.1. Proposal: Repeal of the Directive

The Directive can be repealed in one of two ways:

1. The Directive is repealed in its entirety.

---

[18] For instance, s 15(1) of the *Electronic Communications Act 2000* defines "electronic communication" as

> a communication transmitted (whether from one person to another, from one device to another or from a person to a device or vice versa) —
>
> (a) by means of an electronic communications network; or
>
> (b) by other means but while in an electronic form.

> 2. The Directive is repealed and a single definition of "electronic signature" is incorporated into the proposed new regime covering identity and authentication.

5.1.1. Repeal of the Directive – Consequences

Given the different ways that Member States have implemented the e-Signature Directive, an outright repeal of the Directive will not be disruptive, because it will not affect the current electronic signature legislation of Member States (e.g., the PIN and "I accept" icon as forms of electronic signature which used routinely by millions of citizens every day across all Member States). The way the Directive has been implemented by Member States illustrates the complexity of the legal landscape across Europe. The common assumption by people outside Europe is to take for granted that Directives issued by the European Union are implemented by each Member State equally. Such conjecture is erroneous. For instance, commercial entities in the United States of America are amazed when they realise that they have to understand the electronic signature legislation and substantive evidential law in each Member State. This will not change if the Directive is repealed.

For this reason, repealing the Directive will not further the aim of trying to harmonise electronic signatures in the European Union, unless option 2 is adopted, that is electronic signatures are incorporated into the proposed IAS framework, or the present Directive is amended. This option enables the changes to be made as noted below in respect of amending the Directive, but enables any new Directive to be structured in such a way as to ensure the complexity of the present e-Signature Directive is not replicated.

5.1.2. Proposal: Leave the Directive Unchanged – Consequences

It is possible to leave the Directive unchanged, but it is, arguably, time to amend or repeal it for the reasons already discussed.

If the Directive is not amended, the present confusion will remain.

5.2. Proposal: Amend the Directive

The e-Signature Directive can be amended by providing for a single definition of "electronic signature", and for issues relating to identity and authentication to be the subject of a new regime. This can be done reasonably rapidly, and with little or no need to change legislation immediately if the definition of "electronic signature" is restricted to a single definition. In which case, the following is possible:

> Art 1, in the first paragraph is amended to read: 'The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures in order to ensure the proper functioning of the internal market".
>
> Art 2, the definition of "electronic signature" is changed, and the remaining parts of the article are removed in their entirety.
>
> Arts 3 and 4 are repealed.
>
> Art 5(1) is repealed and art 5(2) is amended to read: "Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form".

Arts 6 and 7 are repealed.

Art 8 is amended to ensure aspects of data protection are taken into account.[19]

5.2.1. Amending the Directive – Consequences

Whether the Directive is amended as proposed or repealed and the amendments, as suggested, incorporated into the proposed IAS framework, it is certain that a number of attributes of the e-Signature Directive will have to be reconsidered. For the sake of legal clarity and to adapt to our use of the virtual world effectively, consideration ought to be given to the separate issues of identity, authentication and signatures. Each concept is different, and the technological response to each also ought to be appropriate. To do nothing is not helpful.

If the Directive is amended as suggested, then it might be necessary to provide a separate regime for advanced electronic signatures and qualified electronic signatures, should both be retained. Member States have adopted varying approaches to both forms of signature in respect of the legal requirements and the technical and security standards. The different approaches taken by various Member States will not change if the Directive is repealed, and need not change if the simplified definition of electronic signatures is agreed.

It will be useful to give a few examples of the different approaches taken by some Member States in respect of electronic signatures. In Hungary, an e-mail without an advanced electronic signature affixed does not meet the requirements of written form;[20] this compares with the position in Greece, where an e-mail is considered a private document and the e-mail address is capable of being an electronic signature.[21] The legislation in Latvia does not provide for an advanced electronic signature[22] while a signature is required by law in Finland. This is defined as "an advanced electronic signature based on a qualified certificate, created by a secure signature creation device, provided by a certified service provider, and satisfying the criteria in the Act will fulfil the requirement".[23] In respect of the technology, the technical problems relating to certificates have been amply illustrated by Paweł Krawczyk.[24]

Discussions in the European Union about e-identity and e-authentication have continued for some time, and the IAS study implemented by the European Commission is a welcome platform for a proper, substantive and informed assessment

---

[19] For a case regarding data protection and electronic signatures, see S Mason, note 3 above, at ch 10.

[20] G Bacher et al, "Electronic Evidence in Hungary: A General Overview" (2011) 8 *Digital Evidence and Electronic Signature Law Review*, at 53 (referring to case BH (Court Decisions) 2006/324. For a translation of this decision into English, see (2011) 8 *Digital Evidence and Electronic Signature Law Review* 235-237.

[21] M G Rachavelias, "Translation of Case No. 1327/2001 – Payment Order" (2006) 3 *Digital Evidence and Electronic Signature Law Review* 104-107.

[22] A Repšs and I Znotiņa, "Electronic Evidence in Latvia: A General Overview" (2011) 8 *Digital Evidence and Electronic Signature Law Review*, at 63.

[23] J Ollila and E Storskrubb, "Finland" in Stephen Mason (ed), *International Electronic Evidence* (British Institute of International and Comparative Law, 2008), at 288.

[24] "When the EU Qualified Electronic Signature becomes an Information Services Preventer" (2010) 7 *Digital Evidence and Electronic Signature Law Review* 7-18.

of the problems that we have begun to face as individuals, businesses, service organisations, and government agencies as the virtual world matures. Sectors that are affected by e-identity and e-authentication include obtaining access to government services, and eCODEX and eJustice are two projects of many that are considering these issues in different ways. It is of importance for a government to be satisfied that those obtaining access to government services that are provided on-line are who they claim to be (although online "identity" can never be certain), which is why these topics are of importance (other services include e-health, e-prescriptions; e-invoicing, e-procurement, etc). However, when considering the approach to be adopted by the European Union, consideration must be given to the nature of *subsidiarity* and the cultural and legal norms of individual Member States.

In summary, if the Directive is amended, or if it is repealed and revisions are incorporated into the proposed IAS framework (whether the revisions are as proposed in this paper, or any other revisions that are adopted), it is necessary to ensure that there is no room for careless thinking. It is essential to ensure the drafting of any future Directive or amended Directive is precise. Particular care must be given to the accuracy of the words used and what they mean. Two examples illustrate the need to consider this carefully:

1. Art 2(2) of the Directive sets out the characteristics of an "advanced electronic signature", and item (a) provides that "it is uniquely linked to the signatory". No form of electronic signature can conform to this part of the requirement. For instance, a user relinquishes control over their scanned signature once it has been sent. An advanced electronic signature is not linked to the person creating it: the unique link is made with the private key, not the user. No one is capable of committing a private key to memory, because it is far too complicated.[25]

2. It is asserted that advanced electronic signatures are a form of electronic signature that enables the recipient to prove a document or communication actually came from the person whose advanced electronic signature was used to "sign" the data. This is not correct. The private key of an advanced electronic signature is protected by a password. The most important point to be aware of is this: *the private key of an advanced electronic signature is only as good as the password that protects it*. This means that when the password is inserted into a computer to provide access to the private key, it proves any of the following:

> The person that keyed in the password (or username and password) knew the password (or username and password); or
>
> The person with access to the computer (whether they were sitting in front of the computer or whether they obtained control of the computer remotely) did not need to know the password because the computer was instructed to remember the password.

It is certain that the Directive will benefit from being amended. The legal foundation of electronic signatures in the European Union is not satisfactory. The definition of an electronic signature can be simplified, and the other forms of electronic signature ought to be reconsidered in the light of the technical security measures that might be adopted in respect of e-identity and e-authentication.

---

[25] See S Mason, note 3 above, at ch 3 for substantial analysis of this sub-section.