ARTICLE:

RETHINKING THE E-SIGNATURES DIRECTIVE: ON LAWS, TRUST SERVICES, AND THE DIGITAL SINGLE MARKET

By **Hans Graux**

This paper aims to explore possible avenues for the future development of the European eSignatures Directive, and more generally of a common European legal framework for trust services. It builds on the observation that the eSignature Directive has largely been unable to support an internal market for certification service providers, i.e. entities that issue signature certificates or provide other services related to electronic signatures.[1] Part of the problem lies undoubtedly in non-legal factors, including the still uncertain business case for certification service providers: is there sufficient market interest for citizens and businesses in spending money on digital signatures, or do simpler, more flexible and cheaper e-signature solutions suffice? However, it is also clear that the Directive itself is too ambiguous on crucial points, and does not consider the essential link between e-signatures and ancillary services. The current review of the Directive is an opportunity to remedy these problems.[2]

Introduction

In recent years, e-signatures have enjoyed increasing attention at the European policy level. As such, this is not surprising: both in the private and public sector, more and more sensitive transactions are conducted electronically, increasing the need for mechanisms that enable trust. E-signatures are a primary example of such a tool, given their stated purpose of serving as a method of authentication.[3]

Unfortunately, this increasing policy interest in e-signatures is largely caused by a relatively gloomy observation: advanced e-signatures (known as digital signatures elsewhere) in the European Union and elsewhere function largely in the context of closed public key frameworks. As long as a signatory remains within that specific context – e-banking applications, national e-government services, professional document management systems – the policy framework established within that context provides clearly for any problems. But as soon as he attempts to use a digital signature outside of that policy framework, digital signatures are virtually unused.[4] This is a fairly disappointing and sobering conclusion for a technology that was entrusted with the seemingly simple task of replacing the hand written signature. Hand written signatures are at best a moderately reliable authentication tool, whose value stems mainly from the fact that people have been used to them for a long time, rather than from any objective security characteristics. And yet, modern technology has failed to come up with a similarly simple, flexible and universally accepted electronic equivalent.

To some extent, this observation is a matter of

1 *As defined in Article 2.12 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p. 12 (e-Signatures Directive).*

2 *Supported by the ongoing study SMART 2010/008 'Feasibility study on an electronic identification, authentication and signature policy (IAS)'. The EU have awarded the contract to DLA Piper, Brussels, supported by subcontractors PricewaterhouseCoopers, SEALED, Studio Notarile Genghini and time.lex. The author a co-contributor to this study.*

3 *As stated in Article 2.12 of the e-Signatures Directive.*

4 *Dr Aashish Srivastava considered the problems of electronic signatures for his PhD, and some of his findings can be found at 'Businesses' perception of electronic signatures: An Australian study', Digital Evidence and Electronic Signature Law Review, 6 (2009) 46 – 56.*

perception and expectation. It is debatable whether it is a problem if no open interoperable market develops for complex e-signature services. The observation about the current limitations of PKI based signature technologies is mainly valid for e-signature technologies that rely on strong identification and authentication of the signatory. While these can offer substantial benefits in terms of trustworthiness and security over simpler technologies, it is not clear whether they are relevant in respect of the realities of today's digital market, where trust seems to be based as much on subjective factors such as reputation as on objective security considerations. One might reasonably wonder if there is such a significant business opportunity in higher quality electronic signatures. If there was a genuine demand for this type of interoperability, would not the market have spontaneously gravitated towards it?

None the less, certain applications clearly have higher objective security needs. The financial sector is a good example, as are higher value transactions such as electronic public procurement. In these cases, the lack of interoperability between advanced signature solutions is inefficient (how many smart cards can your wallet realistically contain?) and encourages bad security practices (how many of those cards currently have the same PIN?). For these reasons alone, interoperability would be desirable as a device to stimulate confidence in the digital market, to avoid needless costs, to enable high value trusted electronic services, and to facilitate the uptake of such services by everyday citizens.

Background and scope of the eSignature Directive

Much of the issues covered in the introduction above are also reflected in the e-signatures Directive, or more formally, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. This Directive states its purpose in article 2: it aims "to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market."

The Directive aimed to ensure that legal uncertainties surrounding the value of e-signatures would not become a barrier to the budding e-signatures market in the European Union, or perhaps more accurately, that such uncertainties could reasonably be kept to a minimum. The elimination of any kind of legal uncertainty was (and remains) a practical impossibility, due to the large variety of approaches to e-signatures and their technical characteristics. The European law maker had to tread a fine line between flexibility (allowing different technologies with different degrees of reliability) and legal certainty (ensuring the predictability of the legal value of at least some types of e-signature).

This resulted in the compromise that is now relatively well known. Conceptually, the Directive creates three tiers of e-signatures:

1. The basic e-signature concept, i.e. data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. The advanced e-signature concept, i.e. an electronic signature which:

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

   In practical terms, the advanced e-signature concept currently implies the use of PKI technology, and is therefore not entirely technologically neutral.

3. The advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, commonly referred to as qualified electronic signatures. This is also the terminology that will be used in this article.

When considering legal certainty however, the Directive contains only two tiers:

1. All e-signatures benefit from a non-discrimination rule (article 5.2), meaning broadly that their legal effectiveness and admissibility as evidence in legal proceedings cannot be denied merely on the grounds of being electronic or of not complying with one of the requirements for qualified signatures. Of course, this does not eliminate the possibility of e-

signatures being rejected for any number of other reasons, including for instance the use of insufficiently reliable technologies, taking into account all circumstances which are relevant to the case (e.g. the behaviour of the parties after an e-signature has been created).

2. Only qualified signatures benefit from the equivalence rule (article 5.1), meaning that these signatures are automatically considered to satisfy the legal requirements of a signature in the same manner as a hand written signature, and that they are always admissible as evidence in legal proceedings.

In effect, the system of legal certainty in the Directive is remarkably binary: qualified signatures are endowed with legal certainty, and other types of e-signatures are not. This situation can be affected substantially by additional rules, such as by specific laws declaring other forms of e-signature to also be equivalent to hand written signatures, or more typically by contractual arrangements in which the relevant parties make separate arrangements on the legal validity and admissibility of e-signatures in advance.

The conceptual framework in European e-signature laws is thus very much centered around e-signatures as a tool for emulating hand written signatures. While the market access and internal market rules (articles 3 and 4 of the Directive) apply to all types of certification service providers and certification services, the only provision in the Directive that governs the legal effect of these services is focused on achieving equivalence with hand written signatures. This observation may appear to be trivial, but it is not. From a technical perspective, the cryptographic process of signing specific data can serve many other functions which have little to no logical connection to a hand written signature. As examples, one might consider:

1. The identification of a person (entity authentication) may use identical technologies, yet there is no intention of achieving equivalence to a hand written signature.

2. The use of electronic stamps or seals, where a entity signs a document to authenticate it on behalf of a legal person (e.g. a company seal or administrative stamp), or even on behalf of an computer system or process, in which hand written signatures may be entirely inappropriate or even nonsensical as an analogy.

3. Authorization management, where the user wants to demonstrate a certain legal mandate (e.g. to confirm the status of doctor, lawyer, notary public, etc) or access/usage right (e.g. the status of employee, citizenship, or simply of being an adult). In these cases, equivalence to a hand written signature may not necessarily be the desired goal.

4. Time stamping, where the equivalence to a hand written signature is irrelevant, since the only intention is to add a trustworthy time reference to a specific transaction.

The Directive is only marginally relevant to all of these functions. This is not to say that it has no effect on them:

1. First, the e-signature itself is defined as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication" (emphasis added). This definition makes no explicit or implied reference to the purpose of creating a substitute for a hand written signature; indeed, based on this terminology alone, all of the examples above could be said to be covered by the definition of an electronic signature, since they are all methods of authentication (either entity authentication or data authentication).[5]

2. Second, the notion of a "certification-service-provider" is very broadly defined in the Directive as "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures" (emphasis added). Again, the definition is so broad that virtually all types of authentication service providers could be said to be covered.

None the less, even under this broad interpretation of the Directive's terminology, the Directive does not provide a material legal framework for the services mentioned above. Admittedly, the market access and internal market provisions of the Directive (mainly article 4.1) apply, meaning that Member States may

5 *Stephen Mason, Electronic Signatures in Law, (2nd edn, Tottel, 2007), 4.5 also illustrates this issue.*

establish the rules which apply to service providers established on their territories, and that they may not restrict the provision of services originating in another Member State. However, with respect to the legal value of trust services, the relevant provisions of the Directive (article 5 of the Directive) are only meaningful when the signatory aims to create a substitute for a hand written signature. In all the other examples mentioned above, it is impossible on the basis of the Directive to link any legal value to a service, other than perhaps to state that its electronic nature does not invalidate it outright. As legal support to a trust service goes, this would appear to be a relatively weak endorsement.

In conclusion, the implicit focus of the Directive is quite clearly on enabling electronic tools that emulate traditional hand written signatures to be recognized as a form of e-signature. It aims to achieve this effect through a number of simple and logical rules and principles. These will be discussed in the following section, as they may be relevant when resolving the trust issues that the Digital Single Market currently faces, as will be commented below, at least from the legal perspective.

The main principles of the eSignature Directive

The rules established by the Directive addresses the legal, technical and trust landscape required to allow an interoperable e-signatures market to function, with a strong focus on digital signatures. The conceptual framework (definitions of e-signature tiers and CSPs) has already been briefly explained above, as has the approach of the legal effect of e-signatures. However, the other building blocks also deserve some consideration, if only to help explain why the Directive has not been able to achieve the desired purpose.

As a basic foundation of the Directive, the free market principle (or more accurately: the internal market rules) are a logical consequence of treating certification services as a market service. To enable the internal market, it is vitally important that Member States cannot set arbitrary barriers to foreign CSPs. This goal has been implemented via article 4 of the Directive, declaring that "[e]ach Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive." CSPs are thus largely governed by a country-of-origin rule, which ensures that they do not need to comply with 27 materially different sets of rules if they choose to operate in all 27 Member States.

As a technical tool, advanced e-signatures also require a minimum common technical framework to ensure their operation. This technical framework is not included directly in the Directive as such. Indeed, that would have been a poor strategic choice, given the relative procedural complexity of renegotiating a Directive, which would make it very difficult to keep the technical framework updated. Instead, the Directive contains only a fairly high level set of requirements in its four annexes, relating to:

> Annex I: requirements for qualified certificates
>
> Annex II: requirements for certification-service-providers issuing qualified certificates
>
> Annex III: requirements for secure signature-creation devices
>
> Annex IV: recommendations for secure signature verification

With respect to technical standardization, the Annexes do not aim to provide guidance for specific implementation or assessment activities, as they are far too generic for that purpose. Instead, the Directive foresees the possibility of providing additional guidance through Commission Decisions, to be taken upon the advice of an "Electronic-Signature Committee" created under article 9 of the Directive, thus colloquially known as the "Article 9 Committee". This Committee may:

1. clarify the requirements laid down in the Annexes;
2. clarify the criteria that Member States should apply when designating a body to determine the conformity of secure signature-creation-devices with the requirements of the Directive;
3. clarify "generally recognized standards for electronic signature products", notably by establishing and publishing reference numbers of such standards in the Official Journal of the European Communities. When this has been done, the internal market provisions of article 3.5 require the Member States to presume that meeting those standards also implies compliance with the

requirements laid down in Annex II, point (f) (relating to the requirement for CSPs issuing qualified certificates to use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them), and in Annex III (requirements for secure signature-creation devices).

Through this process, two main Commission Decisions were taken: Decision 2000/709/EC[6] establishing the minimum criteria for conformity assessment bodies, and Decision 2003/511/EC[7] publishing reference numbers to three generally recognized standards[8] for electronic signature products which create a presumption of compliance with part of the qualified electronic signature requirements. Perhaps surprisingly, neither one of these Decisions was ever updated, despite developments in global e-signature standardization initiatives.[9]

Finally, the Directive also incorporated a trust infrastructure to support certification service providers. Essentially, the trusted (or untrusted) state of an electronic signature is a function of many factors, one of which is the role of a trusted third party. In the absence of a trusted third party (e.g. a simple e-signature consisting of a text file appended to an e-mail, where the text file and e-mail are both solely created by the signatory), an e-signature has a limited ability to provide confidence in the text that has been signed, where the authenticity of the e-mail is uncertain. In those cases, the signature amounts to little more than the word of the signatory, which was already reflected in the signed text without any signature. Through the involvement of a trusted third party (such as the CSP issuing signature certificates in a PKI-based advanced e-signature system), relying parties have a more substantial anchor to which they can attach confidence. If they know that the issuer is trustworthy, then that removes at least one possible area of doubt.

A significant issue is how a relying party can determine whether such a trusted third party is in fact to be trusted.[10] The Directive provides a solution to this question through the concepts of supervision, conformity determinations and accreditation:

1. Member States must establish appropriate supervision schemes, in which (at a minimum) CSPs established within their borders that issue qualified certificates to the public are supervised (article 3.3 of the Directive). Since qualified certificates are a prerequisite to creating qualified signatures, this implies that qualified signature solutions by definition benefit from some degree of supervision, thus improving their trustworthiness.

2. As noted above, the second component of a qualified signature (apart from the qualified certificate) is the use of a secure signature-creation-device. The Directive specifies that Member States can designate bodies with assessing the compliance of such devices with the requirements of the Directive (as laid down in Annex III). Such findings of conformity are to be recognized in all Member States (article 3.4).

3. Finally, Member States are also allowed to introduce "voluntary accreditation schemes aiming at enhanced levels of certification-service provision" (article 3.2 of the Directive). Member States can use such schemes to institute quality labels, or to define 'trust levels' of signature types in an effort to make the market more transparent and intuitive to consumers and service providers. It is important to recognize that "enhanced levels of certification-service provision" does not necessarily imply a high reliability of e-signature solutions; even basic (non-advanced) e-signatures may be subject to voluntary accreditation, irrespective of their objective reliability. The Directive requires that the conditions related to such schemes must be "objective, transparent, proportionate and non-discriminatory", to avoid market distortions. However, since accreditation schemes are by definition established at the national level, they tend to enable trust at the expense of

6 2000/709/EC: Commission Decision 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 (notified under document number C(2000) 3179) (Text with EEA relevance) OJ L 289, 16.11.2000, p. 42–43.

7 2003/511/EC: Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council (Text with EEA relevance) (notified under document number C(2003) 2439) OJ L 175, 15.7.2003, p. 45–46.

8 Notably the following standards: CWA 14167-1 (March 2003): security requirements for trustworthy systems managing certificates for electronic signatures - Part 1: System Security Requirements; CWA 14167-2 (March 2002): security requirements for trustworthy systems managing certificates for electronic signatures - Part 2: cryptographic module for CSP signing operations - Protection Profile (MCSO-PP); CWA 14169 (March 2002): secure signature-creation devices.

9 For an 11-page exhaustive list of standards across the globe, see Stephen Mason, Electronic Signatures in Law, Appendix 3.

10 On this topic, note chapters 11, 12 and 13 in Stephen Mason, Electronic Signatures in Law.

Apart from technical complexity, the European advanced e-signature market in 1999 was developing rapidly, with relatively few services being made available as stand-alone products for the public in most EU Member States

interoperability, since foreign service providers are less likely to have a business case for seeking voluntary accreditation in another Member State, even if their signature solutions objectively meet or exceed the requirements of the voluntary scheme.

On the basis of these trust enablers, each Member State *must* have a supervisory body to supervise CSPs issuing qualified certificates to the public. In addition, it *may* also have an accreditation body to manage any voluntary accreditation scheme, and it *may* have one or more conformity assessment bodies to determine the compliance of any supposed secure signature creation devices. Conceptually, this approach is sound, as it ensures that the legal and technical framework are linked through a workable supervisory framework.

Thus, the Directive provided a basic legal framework that established the main legal, technical and trust building blocks. While clearly slanted towards state of the art PKI solutions, this was considered to be appropriate to sustain an interoperable e-signatures market.

Effect on the e-signatures market

A cursory examination of current EU initiatives involving or requiring the cross border use of e-signatures (e.g. in relation to e-procurement, e-justice, e-invoicing, the implementation of the Services Directive, or any exchange of authentic e-documents) shows that the eSignature Directive has largely failed to achieve this objective. Even leading initiatives in this area are still developing or piloting solutions, twelve years after the adoption of the Directive. Solutions for cross border interoperability either require closed contractual frameworks – essentially cutting out the influence of the Directive to a large extent – or abandon the high-security, high-certainty goals of the Directive by adopting simple (non-PKI) e-signature solutions or by reducing the trust assurances to relying parties. In effect, even if one accepts that the eSignature Directive has helped create a market for advanced e-signature services at the national level, any beneficial effect on the internal market (i.e. at the cross border level) is modest at best.

The present position

A number of factors can be identified that may be partly responsible for the lack of an internal market for advanced e-signatures, or more generally for the lack of cross border interoperability. It is important to recognize that not all of these factors are related to the EU framework for advanced e-signatures as briefly described above. For one, it is inherently difficult to provide an appropriate legal framework in a technological area which evolves very quickly, notably in order to respond appropriately to security challenges. This is especially true in relation to advanced electronic signatures, where new standards are continuously developed and algorithms are deprecated when weaknesses become apparent.

Apart from technical complexity, the European advanced e-signature market in 1999 was developing rapidly, with relatively few services being made available as stand-alone products for the public in most EU Member States. Finally, as was already noted in the introduction to this article, the business case for the advanced e-signatures as a separate service (i.e. in isolation from applications in which they are intended to be used, such as e-banking) remains uncertain. All of these elements made it inherently complex to create a legal framework that would enable a flourishing internal market for advanced e-signature services.

Nevertheless, the current EU framework is clearly also not without its flaws, and a number of issues can be clearly linked to the lack of an internal market. An exhaustive study of these issues and their effect was conducted on behalf of the European Commission in 2010 under the acronym CROBIES (Study on Cross-

Border Interoperability of e-signatures), which is available for online consultation.[11] Briefly summarized, the CROBIES study identified, amongst other things, the following weaknesses and criticisms:

1. The **legal framework is unclear and ambiguous** on certain important points. For instance, opinion is split in the Member States on the question of whether the concept of a 'signatory' can include legal entities, i.e. whether an e-signature can be ascribed directly to a company rather than to the person signing on behalf of that company. Similarly, it is still debated whether a secure-signature-creation device (SSCD) must undergo an affirmative conformity assessment by a designated body, or whether such an assessment is merely advisable to remove or reduce doubts on its status.

2. The **technical framework is outdated** and does not link cleanly to legal requirements. The Commission Decision above only references three specific standards which are partially outdated and do not unambiguously apply to some advanced e-signature creation approaches. For instance, the use of mobile telephones or HSMs (Hardware security modules) is increasingly popular in the advanced e-signature market, yet these are not clearly addressed by the referenced standards.[12] Furthermore, the EU standardization landscape is highly complex: beyond the aforementioned three standards, there are around 30 other standardization projects whose link to specific legal requirements is not clear. The fact that Commission Decisions under the Directive can only create a presumption of compliance with the requirements of Annex II(f) and Annex III of the Directive, and not with other requirements, makes it even harder to assess any formal value to these standardization documents.

3. The **trust framework is too vague** to create justifiable trust in the internal market. As described above, CSPs issuing qualified certificates to the public are subject to national supervision schemes. However, the Directive merely requires that these supervision schemes are 'appropriate', without providing guidance to the Member States as to what this entails. As shown in the CROBIES study, national requirements range from a simple notification letter to the supervision body to full and periodically recurring audits, creating an uneven trust landscape, not to mention internal market distortions. Apart from this inequality, there was no homogeneous way for relying parties to determine whether a CSP was indeed supervised in practice, since supervision bodies did not have a common communication strategy on this issue. This problem was only addressed in October 2009 – ten years after the adoption of the Directive – when a Commission Decision[13] issued against the backdrop of the Services Directive required supervising bodies to use a common trusted list approach to publicly announce the supervision status of their CSPs. Prior to that time, relying parties would need to check the supervision status of a CSP manually each time they wanted to rely on a signature. Similarly, when SSCDs have undergone conformity assessments (the need of which is already unclear, as noted above), there is no common approach to publish this status, and no way to keep this status updated over time as potential weaknesses threatening the SSCD status are uncovered.

Clearly, the legal, technical and trust frameworks established by the eSignature Directive have their flaws. It should be noted however that these flaws primarily apply to qualified signature solutions, since questions related to supervision and SSCDs are much less relevant to other signature types. None the less, since the eSignature Directive only created a clear and predictable legal effect for these types of signatures, this can be considered a real weakness.

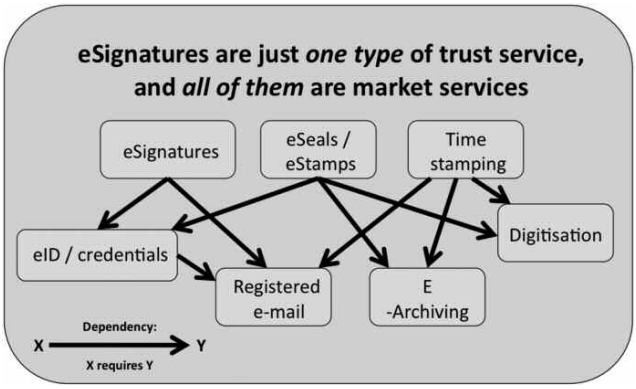
While important, these problems could be fixed through limited changes and updates of the legal, technical and trust framework. There is, however, a broader weakness in the Directive, which would require

11 *Study on Cross-Border Interoperability of e-signatures (CROBIES), A report to the European Commission from SEALED, time.lex and Siemens (Version 1.0, 2010); the author helped to write this report, available at http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm.*

12 *For instance, see Frederic Stumpf, Markus Sacher, Claudia Eckert and Alexander Roßnagel, ' The creation of Qualified Signatures with Trusted Platform Modules' , Digital Evidence and Electronic Signature Law Review, 4 (2007) 61 – 6.*

13 *Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the ' points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market, OJ L 274, 20.10.2009 p. 36 (Corrigendum to Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the points of single contact under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (OJ L 274, 20.10.2009) OJ L 299, 14/11/2009 P. 0018 – 0054); as amended by the Commission Decision 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, OJ L 199, 31.7.2010, p. 30.*

substantially greater changes. As noted above under the description of the scope of the Directive, its provisions clearly focus principally on electronic signatures as a substitute for hand written signatures. This emphasis disregards the reality that finding a substitute for hand written signatures is only one possible application of certification services. There are many other varieties of such services, as shown in the graphic below:



As it stands, the EU 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. More importantly, there are clear dependencies between these services that affect their viability in the market.

As an example, an e-signature as a substitute for a hand written signature is only meaningful if it can be adequately linked to a signatory, either as an identifiable individual, or at least by a pseudonym. Indeed, the eSignature Directive recognizes this issue, as it defines certificates as electronic attestations "which link signature-verification data to a person and confirm the identity of that person" (article 2.9). Similarly, advanced[14] signatures under the Directive must (amongst others) be "uniquely linked to the signatory" [15] and " capable of identifying the signatory" (article 2.2). Thus, when e-signatures are intended to emulate hand written signatures, identification is a prerequisite. Yet the Directive does not address how this should be done, other than to note that the use of pseudonyms in certificates "should not prevent Member States from requiring identification of persons pursuant to Community or national law" (recital 25). This requirement is echoed in Annex II (d) in relation to qualified signature certificates, noting that CSPs must "verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued." Identification (either as an independent process preceding the issuing of signature certificates or as a separate type of authentication service) is not harmonized by the Directive in any meaningful way.

The same observation applies to time stamping, another type of certification service that supports the determination of the authenticity of e-signatures. The value to be given to an e-signature is partly predicated on the mechanism used to reliably determine when it was created. This is a crucial question, since relying parties mainly need to be able to assess whether an e-signature was valid at the time it was created, not merely at the present time (which may be years later). The time factor is an important pillar to the trustworthiness of e-signatures and a valuable certification service in its own right. Again, the Directive does not cover this aspect in a meaningful way.

Other ancillary services mentioned in the overview above build on these tools: electronic archiving depends on time stamping,[16] and electronic registered mail requires both reliable identification of the signatories (senders and recipients alike) and time stamping. In the absence of the basic tools, the derivative services cannot be created either.

In short, it is important to recognize that e-signatures are a component of an ecosystem of certification services. When the Directive covers only one element of that ecosystem (and imperfectly at that, as argued above), new market distortions will inevitably arise. Some Member States have already made the decision of creating their own national legal frameworks for some of these certification services, including time stamping, electronic registered mail and archiving. In the absence of harmonizing provisions at the European level, this is creating new internal market barriers: a "qualified time stamping service" in Member State A may have no legal value in Member State B, either because Member State B has no legal framework for this type of service, or

14 *Interestingly, no such requirement applies to the base notion of "electronic signatures", for which the Directive requires that they 'serve as a method of authentication' in general. This is in line with the observation made above, namely that electronic signatures in general could be interpreted to cover any application of authentication services, but that the Directive only provides a meaningful legal framework for e-signatures as a substitute for hand written signatures.*

15 *For a critical analysis of this concept, see Stephen Mason, Electronic Signatures in Law, 4.9.*

16 *Stefanie Fischer-Dieskau and Daniel Wilke, 'Electronically signed documents: legal requirements and measures for their long-term conservation' Digital Evidence and Electronic Signature Law Review, 3 (2006) 40 – 44*

because the legal framework is different. In practical terms, the time stamping service provider has no way of learning about possible issues other than to seek legal advice on a country by country basis, in order to discover whether its service has any value outside of its national borders, and what changes might be necessary to satisfy national legal requirements. This would appear to be a textbook example of the type of barrier that the European internal market should aim to avoid.

Based on these observations, it would appear that the eSignature Directive is in serious need of review, at a minimum to fix the smaller issues mentioned above. However, this may also be a good opportunity to broaden the legal framework to ensure that certification services are more comprehensively covered and to avoid further barriers in the internal market. Obviously, the lessons learned from the eSignature Directive should be considered if this broader approach is taken.

Trust in the digital single market: what rules, if any, are required?

The EU Digital Agenda and its perspective on IAS

The Digital Agenda was published as a Communication of the European Commission in 2010,[17] and contains the common European strategy for creating "a flourishing digital economy by 2020". It outlines a number of policies and actions that support this objective, grouped around various action areas. For the purposes of this article – examining the challenges and options for the eSignature Directive – the most relevant action area relates to improving trust and security.

The Digital Agenda positions e-signatures in the broader context of trust and security challenges in the information society, which include such topics as misappropriation of identity, fraud, cyber crime, data protection, privacy-by-design, and critical information infrastructure protection. E-signatures (and electronic identities) can be considered as mechanisms that can contribute to building viable solutions on each of these points.

The Agenda correctly stresses the necessity of ensuring the trustworthiness of technology as a prerequisite to its use in practice. It has been observed above that this was one of the main issues of the current EU framework for advanced e-signatures: objectively, there are no sufficient assurances with respect to advanced e-signatures from other Member States. Complexity and user friendliness are equally important: end users will never accept foreign advanced e-signatures if they first have to learn what an SSCD is or if they have to check the supervisory status of a certificate. End users should not be confronted with these questions in their normal use of electronic signatures. However, the eSignature Directive currently does not provide appropriate tools to develop secure, reliable and easy to use signature creation and validation solutions that can enable end users to rely on advanced e-signatures without worrying about the technological, legal and operational minutiae. The development of such solutions would first require existing ambiguities in the Directive and the surrounding framework to be coherently addressed.

Recognizing that the Directive has been unable to meet its stated purpose of "facilitat[ing] the use of electronic signatures and contribut[ing] to their legal recognition" (article 1 of the Directive), the Digital Agenda proposes a revision of the e-signatures Directive, "with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems."

It is worth noting the interesting phrasing of the proposed action set out in the Agenda: the revision should result in a legal framework for 'secure eAuthentication systems'. The Commission might have also simply called for a revision focusing on 'secure electronic signatures', and this would appear to have been the more intuitive choice if there had been no intention of contemplating the scope of the e-signatures Directive. The choice of phrasing, focusing on 'eAuthentication systems' in general, suggests that the Commission might be open to explore further options.

The specific challenges relating to electronic identification undoubtedly play a role in this particular phrasing. Indeed, the Agenda contains a further related action, namely to propose by 2012 a Council and Parliament Decision "to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector)". This action could be used to address one of the current challenges in relation to electronic identification: while innovative EU projects (such as the large scale pilot STORK[18]) have developed functioning technical solutions to eID challenges, there is currently

17 *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe – 26.8.2010; COM(2010) 245 final/2.*

18 *https://www.eid-stork.eu/.*

no broader legal or policy framework to move these pilots into operational solutions for the general public. A Commission Decision could clarify this point, by ensuring at a minimum that Member States have a list of electronic identification methods from other Member States that they agree to treat as equivalent.

Thus, the Agenda seems to have a strategy to improve the trustworthiness of eAuthentication systems, albeit without specifying at this stage exactly what those systems might entail, beyond the obvious candidates of e-signatures and electronic identities.

The needs of the Digital Single Market

While the summary above focuses on the trust and security aspects of the Digital Agenda, it should be recognized that the Agenda takes a much broader perspective, and correctly notes that the EU has in many respects failed to bring about a true Digital Single Market, in which on-line service borders are eliminated (or at least reduced) in the same way as for the offline single market.

Specifically, the Agenda notes that:

> "[t]he internet is borderless, but online markets, both globally and in the EU, are still separated by multiple barriers affecting not only access to pan-European telecom services but also to what should be global internet services and content. This is untenable. First, the creation of attractive online content and services and its free circulation inside the EU and across its borders are fundamental to stimulate the virtuous cycle of demand. However, persistent fragmentation is stifling Europe's competitiveness in the digital economy. It is therefore not surprising that the EU is falling behind in markets such as media services, both in terms of what consumers can access, and in terms of business models that can create jobs in Europe. Most of the recent successful internet businesses (such as Google, eBay, Amazon and Facebook) originate outside of Europe[3]. Second, despite the body of key single market legislation on eCommerce, eInvoicing and e-signatures, transactions in the digital environment are still too complex, with inconsistent implementation of the rules across Member States. Third, consumers and businesses are still faced with considerable uncertainty about their rights and legal protection when doing business on line. Fourth, Europe is far from having a single market for telecom services. The single market therefore needs a fundamental update to bring it into the internet era."

These observations seem entirely correct, and can also be applied to eAuthentication services in general. The recent Public consultation on electronic identification, authentication and signatures[19] have provided some support of the Digital Agenda's statements from the perspective of others with an interest or concern in the matter, asking among other points which trust building services and credentials should be considered for regulation at the European level in order to ensure their cross-border use. The 418 respondents to the question provided the following replies:

For which of the following trust building services and credentials should legal or regulatory measures be considered at EU-level in order to ensure their cross-border use?

	Number of replies	% of total number of replies to this question
Certified electronic documents in general	270	64,59%
Electronic seals	216	51,67%
Time stamping	219	52,39%
Certified delivery of mail	195	46,65%
Authorisations/mandates	194	46,41%
Long term archiving	191	45,69%
Electronic transferable records	136	32,54%
Official delivery address	119	28,47%
Others (please list)	68	16,27%
Pseudonyms	67	16,03%
Anonymous agents	47	11,24%
None	26	6,22%

Thus, only 6,22% felt that no further trust services required any regulation. Respondents who chose this answer and provided additional comments frequently stated that regulations were unnecessary or too rigid, and that standardization, accreditation schemes and private sector initiatives would be adequate to address cross border challenges.

Among those who felt that new regulations could be valuable, certified electronic documents in general – without further definition in the consultation – were the main service type chosen for further regulation (64,59% of respondents), with electronic seals and time stamping each also being mentioned by more than half

19 *For an overview of the consultation's questions, approach, and the contributions received, see http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/pub_cons/index_en.htm.*

of respondents. As to whether electronic identification should be regulated at the European level, this was asked as a separate question. A majority of respondents (65,07%) indicated that they would favour a European legal framework of some sort for electronic identification.

The issues related to advanced e-signatures have already been discussed at length above, but similar considerations apply to other digital services. Consider a simple and realistic scenario: an international undertaking wants to digitize its paper document archives throughout the EU, including invoices and a variety of contracts. New contracts will be created and signed electronically wherever possible, but – as a matter of commercial realism – the company knows that many contracts will still initially be signed on paper, before being converted. The issue is whether this possible in the EU.

Technically, the answer is yes. All the required technologies have existed for decades. Legally, the answer is no. The company would need to assess which documents can be digitized, and under what conditions. The answer to that question depends from Member State to Member State, and will include questions on the types of contracts, paper formalities without electronic equivalents (e.g. seals), specific national legislation, archiving requirements, use and type of signatures, time stamping, notarization, etc. Any company brave enough to conduct an assessment on this point will probably get only two clear results: a very large legal report from at least 27 lawyers across 27 Member States filled to the brim with gray areas and caveats, and no reliable way to move forward with a single harmonized approach.

This is just the customer perspective. Consider the situation from the service provider's point of view. Assume that a CSP wants to provide archiving services, including assurances of long term legibility, integrity, and time stamping. The first question any customer will ask, is whether the service can be relied on, and what assurances the service provider offers. In the absence of a harmonized legal framework, the provider can only reply that its service is technically and operationally state of the art, and that it is (presumably) legal under its own national laws. Whether the archived content actually has any value in other Member States if legal action arises in 15 years will depend on the national law that will be applied to the legal action.

In the year 2011, this state of affairs is nothing short of a tragedy to the economic development of European businesses. Barriers that stifle the legal usability of services across the European Union – both from the perspective of service providers and from the perspective of service users, as noted above – harm European economic growth and stunt the adoption of more efficient technologies. The potential for cost savings in the EU for innovative e-authentication systems – which includes the scenario above – must be substantial. At a time where everyone is looking for both cost cutting and innovation – typically in that order – this is an opportunity that the EU should not miss. A mere framework for e-signatures – even if the challenges mentioned above are resolved – with a smaller scale solution for eID recognition will not provide an answer for the scenarios above.

Options for the future

A future legal framework for IAS services in Europe: a not-so-modest proposal

The Digital Agenda has unambiguously announced a revision of the eSignature Directive, which will probably strive to fix at a minimum the shortcomings summarized elsewhere in this article, together with a possible Decision to ensure mutual recognition of certain eIDs between Member States. This would undoubtedly be a good step forward for the EU. None the less, a more ambitious vision is discussed below, a vision that would – hopefully – be capable of addressing the scenarios mentioned above.

This vision builds on a simple but powerful observation: e-authentication systems (to use the terminology of the Digital Agenda) are similar in most respects, but differ in small important details. This can already be witnessed in the terminology as discussed above: the definition of an electronic signature as presented by the Directive ("data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication") is broad enough to potentially cover e-signatures (in the equivalent-to-hand-written sense), eID and time stamping, among many others. It is worth considering whether a similar policy framework is also possible, and even desirable, for these related services.

As a starting point, it is possible to consider prior experiences across the Member States. The need for a legal framework for ancillary services (time stamping, company seals, electronic registered e-mail, long term archiving) has been known for some time, and some

Member States have been active in this field. To name but a few examples:

1. Austria, as one of the leading EU Member States in this area, has implemented legislation regulating not only e-signatures, but also electronic identification, through the 2004 eGovernment Act.[20]

2. Belgium adopted a generic legal framework for certain trusted services in 2007,[21] including electronic registered mail, time stamping and electronic archiving. Despite a recent update for the rules on electronic registered mail in 2010 (integrated into the general e-signatures Act), executive rules were never fixed, and the law remains largely inoperative at present. However, new legislation in this area is planned for the near future.

3. The Czech Republic has implemented rules for time stamping in its e-signatures Act of 2000.[22] Interestingly, the law uses the same logic and terminology ('qualified time stamp') that is also in vogue for e-signatures.

4. Estonia, as another technology leader in the EU, has a legal framework[23] that supports (and indeed requires) time stamping, digital stamps (advanced e-signatures created by legal entities), and official e-mails.

5. Similarly, Finland has adopted an Act on strong electronic identification and electronic signatures.[24]

6. Germany likewise introduced the notion of qualified time stamping in its e-signatures Act.[25]

7. Italian law contains rules on electronic registered mail.[26]

8. The Slovakian e-signatures Act contains specific rules for time stamping.[27]

9. The Slovenian e-signatures Act recognizes the concept of a time stamp as being comparable to advanced e-signatures, with the same rules applying by changing those things which need to be changed;[28]

10. Finally, the Spanish Act on Electronic Citizen Access to Public Services[29] recognizes e-signatures, e-seals (company signatures), and time stamping.

This listing is neither fully up to date nor exhaustive. Its purpose is merely to illustrate that a significant and increasing number of Member States have recognized the important role of e-authentication systems other than mere e-signatures, and that they have provided a legal framework for such services. When doing so, these laws are often integrated or at least closely aligned with general e-signature rules.

This is important for two reasons. First, it suggests that the principles and challenges for various e-authentication systems are similar, and that it might be possible to address them in unison. Second, it also shows a potential internal market barrier. If time stamping service provider A can guarantee the legal value of its services in one country (for instance, because it is considered a qualified time stamping service in that country) but not in another country (for instance, because that country has no rules, or worse yet, different ones), then that creates a market barrier. This is a challenge for the EU to address, as it was an almost identical observation that led to the adoption of the e-signatures Directive.[30]

The sections below will examine what such a policy framework for e-authentication services might look like, and how it could be structured. As with e-signatures, this policy framework should consist of a legal framework, a technical framework, and a trust

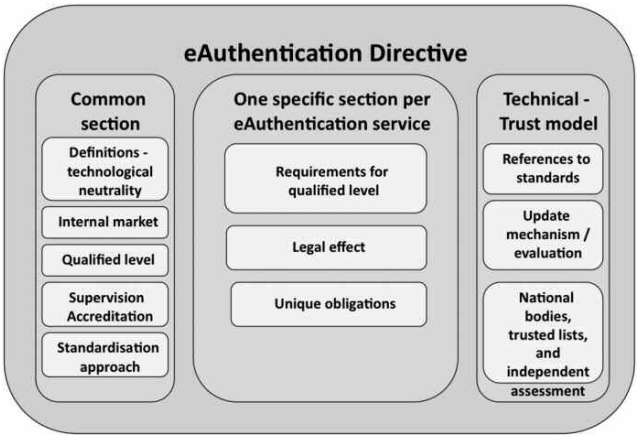
20 *E-Government-Gesetz.*
21 *Wet van 15 mei 2007 tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten/Loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance.*
22 *Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).*
23 *Digitaalallkirja seadus, RT I 2000, 26, 150.*
24 *Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, 7.8.2009/617.*
25 *Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16.5.2001 (BGBl. I S. 876).*
26 *Through the Codice dell' Amministrazione Digitale (the current version is Decreto Legislativo 30 dicembre 2010, n. 235); Roberta Falciai and Laura Liberati, ' The Italian certified e-mail system' , Digital Evidence and Electronic Signature Law Review, 3 (2006) 50 – 54.*
27 *Zákon č.215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov –The Slovakian Act (' as amended' or ' v znení neskorších predpisov') was consolidated in 2009 (§9 of this Act still explicitly refers to time stamping (Časová pečiatka – time stamping)), see http://www.zbierka.sk/zz/predpisy/default.aspx?PredpisID=208862&FileName=zz2009-00076-0208862&Rocnik=2009.*
28 *Zakon o elektronskem poslovanju in elektronskem podpisu.*
29 *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.*
30 *For example, see the table of diverging national legislations on p. 4-5 of the 1998 Proposal for a European Parliament and Council Directive on a common framework for electronic signatures, at http://ec.europa.eu/information_society/policy/esignature/docs/com1998_0297en.pdf. The table is strikingly similar to the list above.*

As with the current eSignature Directive, it is possible to envisage technical elements that require greater flexibility and more frequent updates to be adopted separately via Commission Decisions

framework, all of which must be clearly aligned and attuned to business reality. The emphasis in the sections below will be on the possible regulatory framework – provisionally designated as an e-authentication Directive – but observations on the technical and trust aspects will be added to clarify how this could work in practice.

Basic principles of e-authentication services

The fundamental concept behind a more comprehensive framework for e-authentication services is the observation that all service providers in this area share certain similarities, and the policy framework should reflect this. Broadly, an e-authentication Directive could be structured as follows:



Logically, the common section would specify the common characteristics of all e-authentication services. Subsequent sections would thereafter focus on specific services and their unique characteristics. As with the current eSignature Directive, it is possible to envisage technical elements that require greater flexibility and more frequent updates to be adopted separately via Commission Decisions.

Consistency and comprehensiveness

An important question is how e-authentication services will be defined, and which types of service providers should be covered by such a Directive. The common element of e-authentication services can be derived from the current definition of e-signatures (which, as noted above, is not inherently linked to the emulation of hand written signatures): an e-authentication service is any type of information society service[31] which serves as a method of authentication of electronic data. This definition is technologically neutral, and is sufficiently broad to cover most of the services mentioned above.

Based on this generic definition, the Directive can define subtypes of e-authentication services, using similar technologically neutral language. As a basic requirement, electronic signatures (both for natural persons and legal entities), electronic identification and time stamping would be obvious candidates for inclusion. These are the fundamental building blocks to make other e-authentication services work, and are thus crucial to an e-authentication framework.

To provide for the full potential of e-authentication services, it would be appealing to include other services in a common Directive, including electronic archiving, digitization, validation services, and electronic registered mail. It should be acknowledged, however, that the addition of new services may also create unforeseen complexities. To mention two examples: the digitization of paper documents cannot unequivocally be considered to be an information society service, since it is not necessarily provided at a distance; and the introduction of rules for electronic registered mail as an internal market service may well have interesting overlaps with existing EU regulations for postal services.

Apart from the different definitions, most of the Common Section of the Directive would borrow heavily from the existing eSignature Directive, as the principles

31 *Building on the definition provided by the eCommerce Directive 2000/31/EC, which in turn was based on the definitions of Directive 98/34/EC, as amended.*

of this Directive – if not necessarily the details behind their implementation – are fundamentally sound. Basic principles of the common section would include:

1. Internal market rules, based on articles 3 and 4 of the eSignature Directive. The basic rule for all e-authentication services would be free market access, without prior authorization schemes, and applicability of the rules of the service provider's country of establishment.

2. The introduction of two basic tiers of services: general e-authentication services (as determined by the definitions) and qualified e-authentication services. As is currently the case for e-signatures, general services need not meet any additional requirements (other than respecting applicable laws, such as the national transpositions of the Data Protection Directive), and benefit from a non-discrimination principle (i.e. they may not be denied legal value on the grounds that they are electronic services or on the grounds that they are not qualified, comparable to the phrasing of article 5.2 of the eSignature Directive). In contrast, qualified services would:

    a. Be granted a clear legal effect, to be established in the relevant specific section.

    b. Need to satisfy basic quality requirements. Common quality requirements for all qualified e-authentication services would include independence, liability (comparable to article 6 of the e-signatures Directive), availability of suitably qualified staff, insurance coverage to satisfy its potential liabilities, etc. The common section should only specify requirements that apply to *all* qualified e-authentication services; requirements that apply only to specific e-authentication service types can be specified in the relevant specific section.

3. The introduction of a mechanism for recognizing equivalent non-European e-authentication service providers, similar to the principles in article 7 of the eSignatures Directive.

4. Rules in relation to supervision, voluntary accreditation, and conformity assessments. These will require some changes compared to the present eSignature Directive:

    a. Supervision should remain mandatory for qualified e-authentication service providers, and should still be undertaken by national supervisory bodies. However, minimum requirements for appropriate supervision should be set through a Commission Decision, and national supervisory bodies should publish the supervised status of service providers through trusted lists. This would address the weaknesses of the eSignature Directive as described in the introductory section.

    b. Voluntary accreditation may still be undertaken at the national level by any body designated to operate such a national voluntary accreditation scheme in the Member State. However, as an important terminological point, it may be useful to no longer describe such accreditation as 'permissions' (the way the current Directive does in article 2.13), since this often makes it virtually impossible to distinguish legitimate voluntary accreditation from forbidden prior authorization. Rather, it may be advisable to simply refer to them as what they should be: quality assurance schemes.

    c. As a new element, the e-authentication Directive should also permit the establishment of European voluntary accreditation schemes through Commission Decisions. This is a simple but very potent addition to address a crucial problem with accreditation schemes: currently, they may be beneficial at the national level, but they cause disruptions in the internal market. The introduction of common EU level accreditation schemes could address this: an EU accreditation scheme could determine quality requirements that Member States agree on to enable interoperability in cases where a service does not meet the qualified level, but is still 'good enough' for a specific horizontal or vertical application domain. By way of examples, one might consider:

        i. An EU accreditation scheme formalizing the STORK Quality Authentication Assurance framework, thus allowing any e-ID means to be assessed and accredited against this framework.

        ii. An EU accreditation scheme for e-

procurement, identifying the types of e-signatures accepted for public procurement portals.

iii. An EU accreditation scheme for legal services, identifying the basic requirements for e-ID providers in the legal services sectors (e.g. bar associations, Ministries of Justice, professional bodies of public notaries).

iv. An EU accreditation scheme linking international schemes to their European equivalents, which could facilitate the establishment of international interoperability of e-authentication services, with the benefit of a clear legal basis.

It would go beyond the purposes of this contribution to assess for each of these examples whether they make business and policy sense or whether they are conceptually sound; but based on discussions in relation to e-ID and e-signatures – including the contemplated Commission Decision relating to the mutual recognition of e-IDs – it would appear that there is a clear need for such instruments. Rather than a one-off Decision for e-IDs, it might be beneficial to establish a re-usable approach to establish such EU wide schemes when there is a need and benefit for European administrations, businesses and citizens.

d. Conformity assessments in relation to e-authentication devices (such as SSCDs in the case of qualified e-signatures) will require a clarification whether such assessments are mandatory or optional, and who should provide them. At any rate, when a conformity assessment is granted, there will be a need to publish the assessment status in a homogeneous way, to ensure that they are actually useful at the European level. Again, the use of trusted lists (as is currently already done for CSPs issuing qualified signature certificates to the public) would be a good instrument for this.

5. Finally, a mechanism will need to be defined for the establishment (or more accurately, the referencing) of standards at the European level. This can be based on the current approach, with a Committee evaluating the need for such standards and formalizations through Commission Decisions. However, the requirement of occasional updates will require some further attention, either by making the Committee permanent, or by clarifying the legal value of updates of referenced standards.

Addressing specific e-authentication services

Separately from the Common Section, the details in relation to individual e-authentication services – mainly their specific requirements and legal effect at the qualified level – should be regulated in separate sections. As an alternative, consideration might be given to implementing the e-authentication Directive as a pure framework directive, consisting only of the common section as presented above, and to which specific e-authentication services can be added through separate regulations whenever they are justified. This would certainly offer the benefit of flexibility. However, the need for urgent progress for e-authentication services – in keeping with the timing of the Digital Agenda – would seem to amply justify the creation of a more comprehensive instrument.

The main challenge in this respect is obviously the definition of clear legal effects for qualified services. While the legal effect of qualified e-signatures (equivalent to hand written signatures) now seems obvious, it would also be necessary to define the legal value of qualified identities or qualified time stamps.

However, this is not an insurmountable obstacle. The most difficult type of qualified authentication service is probably the qualified electronic identity, which lacks a clear physical analogy. Since an electronic identity is fundamentally a collection of electronic attributes pertaining to a specific entity, the legal effect of a qualified electronic identity could however be addressed by regulating the reliability of these attributes and the liability model behind their correctness, in much the same way as the eSignatures Directive already does. With respect to qualified certificates – a prerequisite for the creation of qualified electronic signatures – article 6.1 states that certification service providers issuing qualified certificates to the public are as a minimum liable

> "for damage caused to any entity or legal or natural person who reasonably relies on that certificate:
>
> (a) as regards the accuracy at the time of issuance

of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;

(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;

(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;

unless the certification-service-provider proves that he has not acted negligently."

Similarly, such a certification service provider is also liable for damages resulting from a failure to register revocation of the certificate (article 6.2). Limitations on this liability may be indicated in the certificate itself (articles 6.3 and 6.4).

This liability model certainly has its flaws, notably the lack of any explicit obligation to act on indications that the information in the certificate is no longer correct, and the rather broad flexibility of the liability mitigation options. None the less, this approach of providing assurances of identity through liability may be as viable for qualified identities as they are for qualified signatures. While qualified identities would not benefit from an intuitive equivalence rule, they would at least provide the assurance of monetary compensation.

Of course, stronger approaches could also be considered, but are likely to be much less palatable from a political or practical perspective. A significantly more far reaching approach to regulating the legal value of qualified identities would be to require Member States to ensure that the constituent attributes are admissible as evidence in legal proceedings and benefit from a refutable legal presumption of correctness. However, this approach is unlikely to hold much appeal for certain Member States with a strong tradition of official identity documents, who might perceive this model as encroaching upon their monopoly of issuing strong credentials. It may also not appeal due to the reversal of the burden of proof, as it would then be for relying parties to show that the end user's identity claims would not be correct, which might be a costly and complicated process. For these reasons, a lighter liability based approach might be preferable.

Concluding notes

The observations above on the weaknesses of the e-signatures rules are not new, and it is clear that these ambitious suggestions for an e-authentication framework are incomplete and imperfect. The goal of this contribution was however, not to draft a near-final Directive, or to convince the reader that all the answers are readily available.

Rather, this paper aims to make and justify a few observations:

1. The current European framework for e-signatures is built on healthy principles, but flawed in many important respects. These issues need to be fixed.

2. E-signatures are not the only type of authentication service. Authenticity is a basic building block for trust and security in the information society. By focusing exclusively on e-signatures, the European policy framework will remain incomplete.

3. There is a business opportunity in establishing a coherent and comprehensive framework for authenticity services. So far, the European Union has failed to do this. Is it possible for a person to create, sign and store any type of contract electronically, anywhere in the EU, and be sure that it will still be enforceable in 15 years? This is a simple question, and there is no clear affirmative answer. That is not acceptable in the year 2011.

Ultimately, the aim of this paper is to add to the discussion on policy, and provide at least one avenue for progress. It is certainly not the only available solution, and may not be the best one. But one thing is clear: the EU needs to be more ambitious. And it cannot afford to wait.

Hans Graux is a bar lawyer and founding partner at the Brussels based law firm time.lex, which specializes in ICT law and ICT policy challenges. In addition, he is an affiliated researcher at the Interdisciplinary Centre for Law and ICT at K.U. Leuven.

http://www.timelex.eu/

http://www.icri.be

