JICLT
Journal of International Commercial Law and Technology
Vol. 8, No.2 (2013)

Moving towards a comprehensive legal framework for electronic identification as a trust service in the European Union[1]

Hans Graux[2]

Abstract: This paper explores avenues for the creation of a legal framework for electronic identification, specifically by tying this into the future development of the European eSignatures Directive. It builds on the observation that the eSignature Directive has largely been unable to support an internal market for certification service providers, partially because it insufficiently considers the essential link between e-signatures and ancillary services. Electronic identification is one of these ancillary services. The current review of the Directive is an opportunity to remedy this issue. Based on this idea, this paper examines the possibility of creating a comprehensive framework for trust services, that would also include electronic identification services.[3]

1. 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.[4]

Unfortunately, this increasing policy interest in e-signatures is largely caused by a relatively gloomy observation: advanced e-signatures 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, and 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.[5] 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 it 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.

---

[1] Note: this discussion paper is largely based on a more comprehensive article called "Rethinking the e-signatures Directive: on laws, trust services, and the digital single market", which is planned to be published in the Digital Evidence and Electronic Signature Law Review in the second half of 2011.

[2] Hans Graux is an affiliated researcher at the K.U.Leuven – Interdisciplinary Centre for Law and ICT (ICRI – www.icri.be), and a partner at the ICT law firm time.lex (www.timelex.eu) – Hans Graux, Vengerhof 8, 3360 Korbeek-Lo, Belgium

[3] 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 other of the present article is thus a co-contributor to this study.

[4] As stated in Article 2.12 of the e-Signatures Directive.

[5] 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.

2. 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 is 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 conceptual framework in European e-signature laws is 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 an 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:

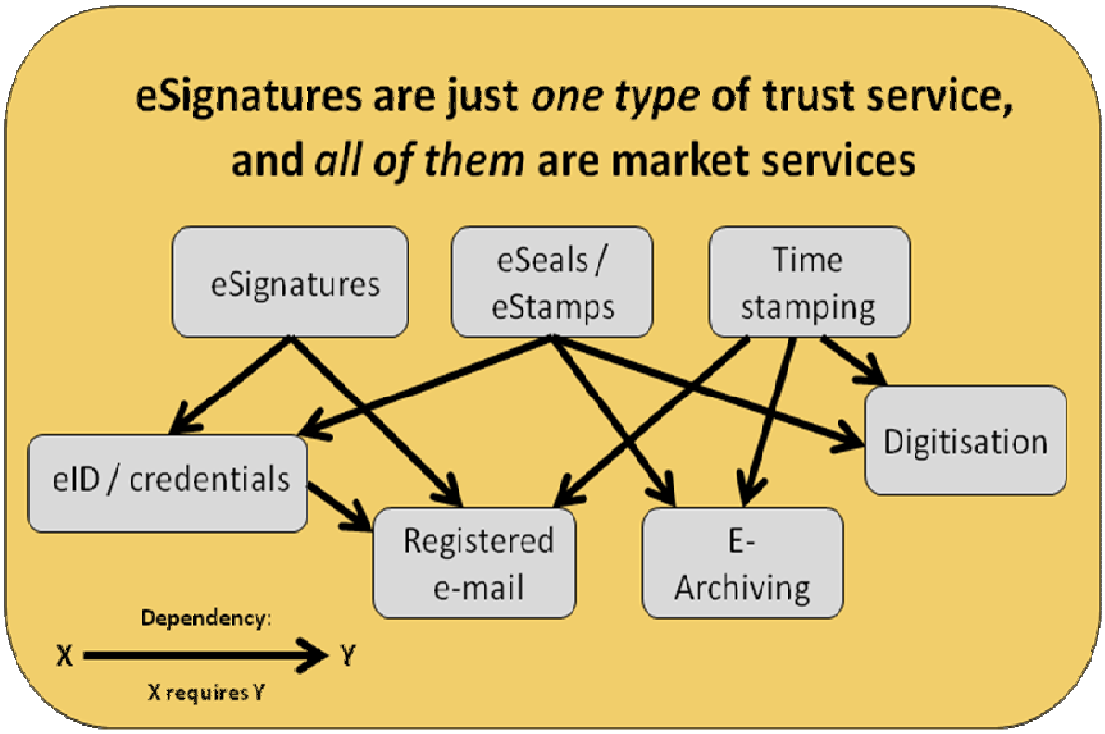
1. First, the e-signature itself is defined as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication" (emphasis added). This definition makes no explicit or implied reference to the purpose of creating a substitute 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).[6]
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.

Nonetheless, 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 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

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

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.

The provisions of the Directive thus 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, at the exclusion of any other service using, or ancillary to, electronic signatures, such as electronic identification, 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[7] signatures under the Directive must (amongst others) be "uniquely linked to the signatory"[8] 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 whom a qualified certificate is issued." Identification (either as an

[7] 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.

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

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. Other ancillary services mentioned in the overview above build on these tools: electronic archiving depends on time stamping,[9] 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.

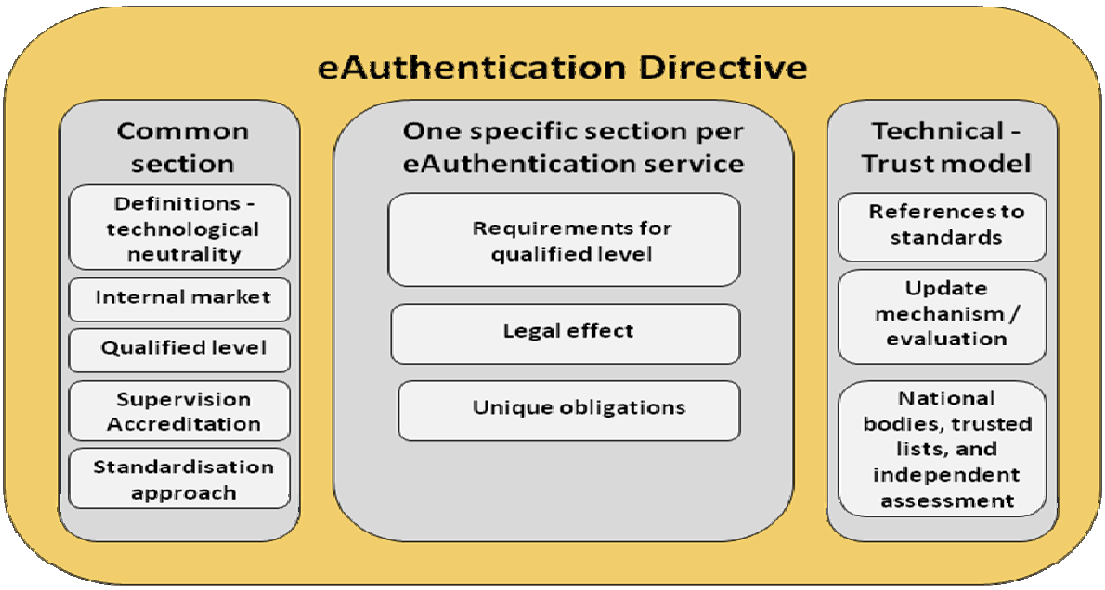
In short, it is important to recognize that e-signatures are a component of an ecosystem of certification services. When the Directive covers only one element of that ecosystem (and imperfectly at that, as argued above), new market distortions will inevitably arise.

Based on these observations, it would appear that the eSignature Directive is in serious need of review. This may be a good opportunity to broaden the legal framework to ensure that certification services (thus including electronic identification) 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.

3. 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, together with a possible Decision to ensure mutual recognition of certain eIDs between Member States. As an input to this process, this paper discusses an ambitious vision for a much more comprehensive framework.

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. The policy framework should ideally 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.

[9] 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

4. 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[10] 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 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

[10] 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.

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 anybody 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 eID and e-signatures – including the contemplated Commission Decision relating to the mutual recognition of eIDs – it would appear that there is a clear need for such instruments. Rather than a one-off Decision for eIDs, 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.

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.

5. Electronic identification as an e-authentication service in this Directive

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. 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.

6. 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, including electronic identification. So far, the European Union has failed to do this.

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.

.* * * * *

Cite as: Graux, Hans. Moving towards a comprehensive legal framework for electronic identification as a trust service in the European Union .*Journal of International Commercial Law and Technology*, Vol.8 No.2 (April,, 2013)