On the implementation of the 1999 European Directive on electronic signatures

STEFAN KELM

More than four years have passed since the European Directive 1999/93/EC on a Community Framework for electronic signatures (the "Directive") was enacted. While many have hoped the Directive would boost the European market for both public key infrastructure (PKI) services and applications, member states have seen highly different results when implementing the Directive into national legislation. While most countries (even the non-EU ones) have, more or less faithfully, transposed the Directive into national laws, a number of issues have nevertheless been identified as problematic. The author provides an analysis of national legislation implementing the Directive in terms of the legal and practical issues involved. A number of recommendations are put forward for a possible modification of the Directive's scope with respect to technology, market and legal developments.[1]

Scope

The EU Directive has led to the adoption of national regulatory frameworks for electronic signatures in almost every European country. The divergences between these regulatory frameworks are noteworthy, and the resulting picture very complex.

The main aim of the Directive was to create a Community framework for the use of electronic signatures, allowing for the free cross-border flow of products and service provisions, together with a basic legal recognition of electronic signatures throughout the EU. This objective has clearly not completely been reached. This, however, may not necessarily be the fault of the Directive itself. To the largest extent, this is due to the low market uptake of the public key technology itself. However, the diverse nature of the implementations of the Directive in the Member States has, in addition, created uncertainties about the use of electronic signatures. Some of the Directive's provisions seem to have been misunderstood in part, and the Member States, while transposing the Directive into national law, have sometimes failed to focus on the European dimension of the new regulatory framework. We are therefore under the impression that there is a primary need for a consistent, clear and workable re-interpretation of the Directive's provisions.

In our view the Commission should begin by examining the way in which a more "Community-focused" interpretation of the Directive could be supported. Of course the ultimate judge on the correct interpretation of EU law rests with the European Court of Justice. Nevertheless the Commission is in a position to issue a non-binding document that can influence considerably the electronic signatures debate in Europe. Such an instrument could be combined with realistic accompanying measures that can be implemented in the short term. Such measures can focus on the improvement of interoperability between solutions, procedures, schemes and applications, the streamlining of national solutions for supervision of certification service providers, co-ordination of voluntary accreditation schemes, and of conformity assessment schemes for secure signature-creation devices, interchange between electronic signature-related applications and schemes in the public sector.

We are therefore under the impression that there is a primary need for a consistent, clear and workable re-interpretation of the Directive's provisions

[1] The use of the plural is used in this article, because this article is a synopsis of the main study undertaken for the European Commission by Jos Dumortier, Stefan Kelm, Hans Nilsson, Georgia Skouma and Patrick Van Eecke *The legal and market aspects of electronic signatures.*

Findings

The authors discovered that most of the EU Member States have, more or less faithfully, transposed the Directive into national legislation. In addition, many of the non-EU countries surveyed have based their own electronic signatures and delivery of signature related services legislation on that of the EU Directive. From a technical point of view the Directive has even influenced international standardization initiatives, such as the IETF standardization work on Qualified Certificates. It is clear that the Directive has influenced legal and technical activities outside of the European Union boundaries. Remarkably, the European Economic Area (EEA) countries, Switzerland, the Accession and the Candidate countries have accepted new terminology introduced by the Directive (especially Qualified Certificate, Advanced Electronic Signature, and Certification Service Provider).

Although the broad lines of the Directive have been respected by the Member States when transposing the Directive, a number of issues have nevertheless been identified as problematic. These problems can mainly be attributed to a misinterpretation of the Directive's wording, which in turn leads to divergences in national laws and divergences in the practical application of the rules.

Regarding the market access rules as stipulated by article 3 of the Directive, the following remarks need to be made. The good news is that for the moment, none of the Member States surveyed submit the provision of certification services by providers established in another Member State to prior authorization, thus formally respecting article 3.1 on market access. It is, indeed, perfectly possible for a Certification Service Provider (CSP) established in one Member State to provide certification services in another Member State, without having to ask the prior permission of a national authority. This was not possible everywhere in Europe before the Directive was issued and transposed.

On the other hand, various Member States have established supervision schemes that are very close to prior authorization, and are possibly infringing article 3.1 provisions. Given that CSPs have been established in all but a few of the countries surveyed, and given that the majority of supervision schemes are still in the very early stages of development, it is not presently possible to offer a comparison of the practical implications of the supervision systems. Nevertheless, it has become obvious that there are very important divergences between the various supervision schemes in the Member States. Although the effect of these divergences remains limited, since most of the CSPs still operate exclusively in their home country, the divergences will begin to show negative effects once European or non-European providers start to launch more cross-border certification services across the EU.

Also, the Directive's rules on voluntary accreditation seem to be misunderstood by national governments. Many European countries wrongfully consider voluntary accreditation schemes as a means of controlling whether or not a CSP operates in compliance with the provisions of the Directive. Another alarming observation is that the voluntary accreditation schemes in many European countries are, in practice, not really voluntary. A typical example being that many national e-government programmes only accept accredited CSPs to participate in the programme, and thus indirectly oblige a CSP to get an accreditation. This evolution is certainly not in line with the Directive's vision.

Concerning the so-called "public sector exception" of article 3.7, which allows Member States to make use of electronic signatures in the public sector subject to possible additional requirements, we have seen divergences in both the interpretation and implementation of this provision. It seems clear that in many countries the use of electronic signatures in the public sector is subject to additional security requirements. Communicating electronically with public authorities is in many European countries possible only through the use of signatures based on Qualified Certificates issued by an accredited CSP. Member States need to be reminded that applying additional conditions can only be justified by objective reasons and should only relate to the specific characteristics of the application concerned. Also, Member States need to ensure that basic competition rules are not being infringed by their initiatives.

As to the conformity assessment of secure signature-creation devices (SSCDs), many countries seem quite reluctant to designate their own designated bodies for SSCD assessment. This may be due to the very high SSCD security requirements and the lack of active vendors in most countries. Another reason is the very large resources needed for operating an assessment body. The process of assessing a product is usually extremely expensive as well as time-consuming.

Two further reasons why vendors are sometimes reluctant to have their products assessed is that an assessment is usually only valid for a fairly short amount of time (the product needs to be re-assessed), and a conformity assessment "freezes" a product so that it cannot be changed (e.g., in order to apply a security patch) without making the assessment invalid. Consequently, although there already are a small number of SSCDs that have been assessed, all of these have been assessed by a relatively small number of designated bodies. Only in Austria, Germany and the Czech Republic have the number of products assessed been higher than two. In some countries (Austria, Germany) signature products other than SSCDs have been assessed as well.

The non-discrimination principle of electronic signatures, as regulated by article 5.2 of the Directive, has been taken over by national legislators. However, the transposition of article 5.2 has not always been explicitly done, and in those countries with an explicit transposition the scope of article 5.2 has not always been covered in its entirety. It is not yet clear whether this rather vague transposition in some countries will have a practical effect on the legal use of electronic signatures. Thus, how electronic signatures will be treated in future national legislation and case law requires close monitoring.

It would be too premature to jump to early conclusions on judges' position vis-à-vis electronic signature given that to date there are but a few legal cases on this subject. Indeed, until recently, the sample of case law tackling directly or simply evoking electronic signatures issues is still too small and fragmented to be considered as representative enough of the judge's mind in this area.

As to the legal effect of Qualified Electronic Signatures (the ones regulated by article 5.1 of the Directive), there has been a general tendency in the majority of European countries to explicitly recognise the equivalence between a handwritten signature and a specific "type" of signature by imposing the same or slightly different conditions than the ones stipulated in article 5.1. It is, however, important to know that the Directive obliges Member States only to make sure that a Qualified Electronic Signature is, legally speaking, treated in the same way as a handwitten signature, but that it does not regulate the legal use and consequences of a handwritten signature itself, and thus not the legal consequences of the Qualified Electronic Signature either. The legal use and consequences (such as which transactions need a signature, and what evidential value is given to a signature) remains a nationally regulated matter.

Qualified electronic signatures need to be in compliance with the requirements as stated by the first three Annexes of the Directive. It is, therefore, important that the Annexes are correctly transposed into national legislation. The implementation of Annex I is very similar in most of those countries surveyed. The only risk is related to interoperability problems which might occur if technical implementations of Annex I diverge by, for example, not using ETSI TS 101 862, or any other common format for encoding the requirements of Annex I. The European Commission should therefore promote the use of interoperability standards for the technical implementations of Annex I. For the implementation of Annex II, implementation levels sometimes vary, meaning that the establishment and running of a CSP will differ considerably. Any organization wishing to establish a CSP business in several countries must therefore adapt itself to different requirements and procedures. Product vendors will also have difficulties building products for this very fragmented market. In addition, several countries put additional detailed and unnecessary requirements on the CSP, thus creating barriers for the establishment of a CSP. The Commission should therefore point out any unnecessary and excessive requirements for CSPs, which might be perceived as market obstacles. For the implementation of Annex III, there is also evidence of fragmentation. The requirements for SSCDs are, for example, much higher in Austria and Poland than in some other European countries. As far as Annex IV is concerned, article 3.6 is very clear. The list contains only recommendations, which have to be taken into account by the Member States and the European Commission when they work together in order to promote the development and the use of signature-verification devices. They cannot be changed into obligatory requirements at a national level, as some Member States have done.

With very few exceptions, all European countries have provided for a special liability provision, transposing article 6 of the Directive into national legislation. Within the European Union, the respective liability clauses of the EU Member States have followed the wording and rationale of article 6. In cases where transposition was not explicit, the general tendency has been to provide stricter liability clauses, by broadening the scope of

Technology evolves rapidly, and in the near future many electronic signature technical solutions will be based on new technological developments, such as new secure personal computer environments, mobile signatures and signature servers

application of the article, notably, by extending the list of liability causes as laid down in the Directive.

All countries under examination have prescribed in their national laws rules on the legal recognition of foreign Qualified Certificates in their territory. Only Ireland, the United Kingdom and Malta do not distinguish between domestic and foreign Qualified Certificates. Most of the EU and EEA countries have faithfully transposed the conditions of article 7 into their national legislation. In the Accession and Candidate countries, the situation appears to be somewhat more complicated.

The implementation of the data protection rules of article 8 into national legislation apparently do not pose any real difficulties. Some countries, though, did not correctly implement article 8.2 of the Directive. In those countries, a CSP is not obliged to follow the stricter data protection rules, whereas a CSP established in another Member State must adhere to its national rules. This may give rise to complaints of unfair competition, in that it could act as an obstacle to trade within the internal market. Further discussion also needs to centre on whether the stringent rules of article 8.2 for CPS issued certificates to the public, (such as obligation to for direct personal data collection), are realistic, given that most CSP data is obtained from third parties such as a local registration authority. The use of a pseudonym in a certificate is allowed in all but two of the countries surveyed. Only Estonian and Bulgarian electronic signature legislation forbids the use of pseudonyms in their national rules on Qualified Certificates. Many countries explicitly require the disclosure of real names to the public authorities upon request and under strict conditions.

An important question, which needs to be posed, is to what extent are Qualified Electronic Signatures used in Europe? The number of supervised and accredited CSPs issuing Qualified Certificates in the European countries varies considerably from country to country, with many countries having either no or only one CSP. In the few countries where any larger numbers of Qualified Certificates have been issued, this is almost exclusively due to some form or another of government promotion. There is currently no natural market demand for Qualified Certificates and related services. The largest application area in Europe for Qualified Electronic Signatures is generally linked to e-banking applications in a closed user environment, and thus outside the scope of the Directive. Within the scope of the Directive, very few applications are in use today and they are almost completely limited to e-government.

It is interesting to note that many application service providers currently on the market falsely believe that their applications require Qualified Electronic Signatures as a minimum in order to be legally compliant, leading to unnecessary costs and complexity on planning and designing for the use of Qualified Electronic Signatures.

Technology evolves rapidly, and in the near future many electronic signature technical solutions will be based on new technological developments, such as new secure personal computer environments, mobile signatures and signature servers. Consequently, supervision bodies, designated bodies and others involved in the regulation of Qualified Electronic Signatures should look at these technologies with an open mind, and not restrict security assessments to what is known and available today.

The lack of interoperability, both at national and cross-border level, is a big obstacle for market acceptance and the proliferation of electronic signatures. It has resulted in many isolated "islands" of electronic signature applications, where certificates from only one CA can be used for one application. In a few cases only can certificates from multiple CAs be used for multiple applications. Much more should therefore have been done earlier at a European level to promote interoperability.

The European Electronic Signature Standardisation Initiative (EESSI) programme has developed some standards that comply with the Directive. However, the delay in developing the standards and having their references published in the Official Journal has led to a situation whereby several countries have either developed their own technical interpretations of the Directive, (leading to varying requirements in different countries), or else have waited for standards to be developed, leading to a vacuum for product and service vendors on the market. Not until the publication of references to standards in the Official Journal in July 2003 has there been any clarity on the standards acceptable to all Member States. Another risk relating to interoperability is that currently only one set of standards related to Qualified Electronic Signatures (based on PKI) currently exists, which may hinder further technologies being used for Qualified Electronic Signatures.

The recommendations

■ Introduction

Our first recommendation is not to amend the Directive. Such amendments would have to be considered as an ultimate solution, only to be used when all other measures are deemed to be insufficient. Amending the Directive is a long and cumbersome operation that should be avoided if at all possible. As with all EU Directives, the Directive is by no means a perfect legal text. It is a compromise that has been reached after long and difficult negotiations between 15 Member States, all of whom have very divergent views on these issues. Our main conclusion is that the text of the Directive is adequate enough to serve its purpose in the near future but that it needs re-interpretation and clarification.

■ General recommendation

The primary aim of the Directive was to create a Community framework for the use of electronic signatures, allowing for the free cross-border flow of products and provision of services, together with a basic legal recognition of electronic signatures throughout the EU. This objective has clearly not entirely been met. However, this negative situation is not necessarily the fault of the Directive, but rather to the way in which it has been implemented by the Member States. Some of the Directive's provisions seem to have been, in part, misunderstood and the Member States, when transposing the Directive into national legislation, have not always taken the European perspective of the new regulatory framework into account. It is therefore our impression that, at this moment, there is a primary need for a consistent, clear and workable re-interpretation of the provisions of the Directive.

In our view the European Commission needs to first and foremost examine how a more "Community-focused" interpretation of the Directive could be supported. Of course the ultimate judge on the correct interpretation of European law provisions rests with the European Court of Justice. At the same time, however, the Commission is in a position to issue a non-binding document, which could considerably influence the electronic signatures scene in Europe. Such an instrument could be combined with realistic accompanying measures capable of being implemented in the short term.

■ Supervision of CSPs

The European countries surveyed for this report appear to have difficulties in striking a balance between the appropriate supervision of CSPs, and the prohibition to submit their activities to prior authorization. It would therefore be useful to publish guidelines on how the supervision can be organized in order to make it conform to the Directive's provisions. The European Commission can take action against Member States that have established a scheme for the supervision of CSPs leading to measures that have the equivalent effect as a prior authorization.

The guidelines to be published by the European Commission can also be used to clarify a number of currently unresolved legal issues in this area. One of the most difficult questions is to know what the notion of "establishment on the territory" in practice means for a Certification Service Provider. For example, it is debatable as to who is in charge of the supervision where a certificate issuer established in one Member State, collaborates with registration authorities, directory service providers, and others in other Member States.

Not all the Member States have established a scheme for the appropriate supervision of CSPs issuing Qualified Certificates to the public. The Commission can take action against these Member States, because this situation creates the possibility for CSPs established in those Member States to issue Qualified Certificates to the public in other Member States without being submitted to appropriate supervision.

Ideally the supervision schemes in the Member States should be harmonized, at least to a certain degree. We think that efforts in this direction should be supported. The Commission should, in our view, discourage supervision of CSPs other than those issuing Qualified Certificates to the public.

Since EESSI has already published a number of valuable documents in this area, it is recommended that supervisory authorities be encouraged to make use of these specifications. In our view, however, the use of such specifications by supervisory authorities has to be closely monitored. The standardization documents describe possible paths to fulfill the requirements of the Directive, but should never be considered obligatory for CSPs wishing to issue Qualified Certificates to the public. If a CSP believes that it fulfils the requirements of the Annexes, it should

be free to issue Qualified Certificates to the public without asking for authorization.

■ Voluntary accreditation

Measures should be taken in order to clarify the vision of the European legislator with regard to voluntary accreditation schemes for Certification Service Providers. In our view, cross-border accreditation and diversification of the schemes should be encouraged. The Commission should, on the other hand, discourage as much as possible the establishment of national accreditation schemes for Certification Service Providers issuing Qualified Certificates to the public. Accreditation schemes should focus on the assessment of best practices and appropriate security, and not be considered as instruments to control the compliance with the Directive or with national legal provisions.

Given the scarcity of top experts in the area of information security, and given the relatively small amount of CSPs, the Commission should stimulate the clustering of efforts on a Community level. The objective should be to establish a limited number of high quality European accreditation schemes, preferably focusing on or specializing in specific categories of certification services for application domains.

■ Secure signature-creation devices

Partly because the Directive currently sets very high requirements on SSCDs, such devices still rarely find their way to the market. In order to stimulate the production of secure signature-creation devices, the requirements for formal assessment needs to be more flexible in the future. The procedures for obtaining a conformity declaration should be shorter and less costly. The European Commission should support every effort in this direction.

As to the rules to be followed by the designated conformity assessment bodies, the Commission should provide coordination and guidance. The Commission Decision of 2000 on the minimum criteria when designating conformity assessment bodies is a valuable first step, but needs to be pursued.[2] The independent, transparent and non-discriminatory character of the assessment procedure should ideally be monitored.

In the view of the authors of this report, it is absolutely necessary to discourage the perception that it is an obligation to submit every SSCD to a lengthy Common Criteria influenced assessment performed by a designated body. Instead, limited evaluations, based on 50-100 pages of documentation and requiring 10-20 days of checking, needs to be promoted. In not allowing self-assessment, an independent party should be able to assess the security claims (with respect to Annex III) as made by the vendor and checked to some extent whether or not this is state of the art. The Commission should examine how it can tackle the obligation to submit an SSCD to a designated body for conformity assessment, currently existing in many Member States. By discouraging a too strict conformity assessment would allow for a larger variety of products, while at the same time protecting consumers.

■ Public sector exception

The Commission should emphasize the conditions that are needed before the Member States can use the public sector exception of article 3.7 of the Directive. Member States should be made aware that the non-discrimination rule of article 5.2 of the Directive applies not only to the private but also to the public sector.

The Commission should examine in more detail the compliance of certain e-government initiatives, not only in relation to the Electronic Signatures Directive's provisions, but also in relation to general EU competition rules, particularly with a view on article 86 of the EC Treaty.

More generally, it is necessary to perform a more detailed study on the Internal Market consequences of the e-government programmes of the Member States. There is a clear danger that these programmes will result in national barriers, fragmentation and interoperability. Efforts towards improvement of interoperability between e-government programmes, and particularly between their electronic signature applications should be supported or initialized at a European level.

■ Qualified Electronic Signatures

With regard to article 5.1, there is primarily a need for clarification about the scope of this provision. It should be made clear to all interested parties that:

- "Qualified Electronic Signature" is not a synonym of "legally valid electronic

[2] Commission Decision of 6 November 2000 on the minimum criteria to be taken into account by Member States when 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 (OJ 16.11.2000 L 289/42).

signature", and
- fulfilling the requirements of a Qualified Electronic Signature is one – but by no means the only - way to get the rules on handwritten signatures applied.

From a European perspective, the success of article 5.1 depends entirely on the availability of a very well standardized and easily recognizable European Qualified Electronic Signature, including not only criteria for creation devices and certificates, but specifying the complete signature and verification chain. A standardized Qualified Electronic Signature should merely give users a presumption that a signature complying with this standard will be presumed equivalent to handwritten signatures throughout Europe.

Member States should be discouraged from inserting references to Qualified Electronic Signatures in new legal texts. The concept of the Qualified Electronic Signature should be used mainly for its original purpose, namely to obtain automatic acceptance of electronic signatures, and that the same provisions governing handwritten signatures apply to electronic ones.

Member States should be made aware that the concept of the Qualified Electronic Signature is mainly useful for cross-border transactions in Europe. It serves as a "passport" that guarantees in every Member State the application of the rules applicable to handwritten signatures.

The Annexes have been more or less literally transposed into national legislation by virtually all the countries surveyed. The remaining task is to make sure that the implementation gets streamlined throughout Europe. Every effort in this direction should be supported. National implementations of the Annexes have, on the other hand, to be firmly discouraged. The Commission can, perhaps should take action against those Member States who have not correctly transposed the Annexes by, for example, translating the recommendations of Annex IV into requirements for Qualified Electronic Signatures at a national level.

■ Non-discrimination rule

With regard to the application of article 5.2, there is a primary need for clarification. All interested parties should be better informed about the objective and the scope of this provision. The Commission should systematically examine if the Member States have issued legislation referring to Qualified or Accredited Electronic Signatures, and detect where such references do not comply with the rule of article 5.2.

■ Standardization

The Commission and Member States must ensure that all Member States correctly implement presumption of conformity with standards referenced in the Official Journal. This is currently not the case everywhere.

The Commission and Member States should encourage further work on standards related to Annex II (f) and Annex III, in order to promote the use of alternative technologies for Qualified Electronic Signatures. Although the present standards are mostly technology neutral (within the framework of PKI), they still favour the use of smart cards as SSCDs for example. The long-term maintenance of the standards referenced in the Official Journal must be ensured, either by transferring the current CWAs to a more permanent body, for example ETSI, or promote the CWAs to European Norms.

The Commission must urgently ensure the acceptance of a common specification for algorithms and parameters, as well as a common maintenance procedure for that specification.

The complex areas of archiving and long-term validation of electronically signed documents are often perceived as obstacles for the use of electronic signatures. The Commission should promote work on guidelines and standards in these areas.

The Commission and the Member States should find mechanisms to promote or recommend the standards for interoperability already developed by ETSI within the framework of EESSI. The Commission should support the work being done in EUCLID and CEN Workshop on e-authentication, steering them towards developing appropriate European standards, taking into account the results from EESSI, pki Challenge and other projects.

The European Commission should promote or arrange a European forum for electronic signatures, directed towards CSPs, product vendors and application providers in order to stimulate development and use of standards, possibly also initiating the setting up of interoperability testing facilities.

It is probably useful to systematically scan the existing standardization documents from a user's perspective. With regard to Qualified Electronic

Signatures, the aim of the standardization activities should be to develop the specifications of a solution that gives the user the possibility to use electronic signatures on a European-wide scale. Such a solution has to take into account all the aspects of an electronic signature, not only covering the whole signature chain but also taking care of typical users' concerns such as ease of use, language obstacles, and cost considerations, amongst other issues.

The efforts of the EU to promote advanced personal data protection for its citizens should not be contradicted by its regulatory framework for electronic authentication

■ Trust service providers

The Directive is very strongly focused on one business model, which was the centre of the attention from 1998 and 2000, but which has progressively been replaced by a much more heterogeneous and complex market situation. The regulatory framework thus includes, for example, quite detailed rules for certificates providers, but does not deal with other categories of certification providers. The regulatory needs relating to other categories of trust service providers are nevertheless at least as urgent as those with regard to certification service providers. There is, for example, a clear need for regulation dealing with archival service providers, or with registered mail services. From a users' perspective it is difficult to understand why such services remain completely unregulated, while at the same such a complex regulatory framework has been established for issuers of certificates. We therefore recommend undertaking studies about the need for regulation with regard to other categories of trust services.

■ Data protection

Last but not least it is necessary to combine electronic authentication with personal data protection. The current European regulatory framework is very much focused on the use of identity certificates. In recent years, attention has shifted towards better privacy protection in the on-line environment. Research has been done on various possibilities, combining electronic authentication with the needs for anonymity or the use of multiple virtual identities. The efforts of the EU to promote advanced personal data protection for its citizens should not be contradicted by its regulatory framework for electronic authentication. Closer examination is needed on the possibilities to combine anonymity and pseudonymity with the provisions of the Directive.

■ Final remarks

Our final reflections in the framework of this report focus on the user. In our view it is absolutely necessary to put more emphasis on the user's perspective in all discussions regarding the European electronic signatures regulatory framework. The absence of this perspective has been a more or less constant theme not only in the legal discussion, but also in the standardization activities around the Directive. Business and technical considerations prevailed strongly in every debate in this area. This has resulted in a set of legal and technical solutions that are often far removed from the daily needs of the common user.

As far as standardization is concerned, it is probably useful to systematically scan the existing standardization documents from a user's perspective. With regard to Qualified Electronic Signatures, the aim of the standardization activities should be to develop the specifications of a solution that gives the user the possibility to use electronic signatures on a European-wide scale. Such a solution has to take into account all aspects of electronic signatures, not only covering the whole signature chain but also taking account of typical users' concerns such as ease of use, language obstacles and cost considerations.

With regard to the legal framework, it may become necessary to take a more practical approach. The Directive focuses very strongly on one business model, which took centre stage from 1998 to 2000 but which has since been replaced by a much more heterogeneous and complex market. As a result of this, the current regulatory framework includes detailed rules for issuers of certificates but fails to consider other types of certification providers. Services like time-stamping, revocation, repository, and archival can be offered by third parties which are contracted by the authority issuing certificates. Yet regulatory needs relating to other categories of trust service providers are at least as important as those relating to the certification service providers. There is, for example, a clear need for regulation dealing with archival service providers, or with registered mail services. From a users' point of view it is difficult to understand why such services remain completely unregulated, while complex regulatory frameworks have been well established for those issuing certificates. We therefore recommend that further studies be carried out dealing with other categories of trust services.

Finally, it is necessary to combine electronic

authentication with personal data protection. The current European regulatory framework is very much focused on the use of identity certificates. In recent years, attention has shifted towards better privacy protection in the on-line environment. Research has been focused on the possibility of combining electronic authentication with the needs for anonymity or the use of multiple virtual identities. The efforts of the European Union to promote advanced personal data protection for its citizens should not be contradicted by its regulatory framework for electronic authentication. Further research is needed into the possibility of combining anonymity and pseudonymity with the provisions of the electronic signatures Directive.

The authors are aware of the fact that its conclusions and recommendations can only be considered as a first step in the review of the European regulatory framework for electronic signatures. We hope that our recommendations will provide interesting material for launching a European-wide discussion on this subject. Although this report does not cover the legal landscape of the United States, Canada, Japan and Australia, it is still wise to consider what is happening in other parts of the world before formulating European recommendations. The major market players global strategies vis-à-vis electronic signatures and internet standardization will also have to be considered in order to get a clear forecast for the future situation in Europe in this field. ■

Stefan Kelm has been a computer security researcher for fifteen years. He has been with Secorvo Security Consulting GmbH for the past five years, dealing with various aspects such as electronic signatures, computer forensics and network security. Stefan is author of several national and international publications.

stefan.kelm@secorvo.de
http://www.secorvo.de