Department of
Trade and Industry

BPR 251
151 Buckingham Palace Road
London SW1W 9SS

A REPORT PREPARED ON BEHALF OF THE DEPARTMENT OF TRADE AND INDUSTRY

INTO

THE IMPACT IN THE UNITED KINGDOM OF THE EU ELECTRONIC SIGNATURES FRAMEWORK DIRECTIVE

- EXTENDED VERSION -

Report Reference
DTI TFBJ/C/003/0061X

Document status
Issue: 1.0.0 (Final)
Date: 12th October 2003

Authors

Richard G. Wilsher,
Managing Director
the Zygma partnership limited
RGW@Zygma.co.uk

Jane Hill
Barrister
Chambers of Benet Hytner Q.C.
JH@JaneHill.com

With support from:
Christopher Kuner, Partner, Hunton & Williams (Brussels)

THIS PAGE INTENTIONALLY DEVOID OF OTHERWISE USEFUL TEXT

CONTENTS

Executive Summary 6
Background to this Report 9
Scope & Performance of the Study 10
The Response from Industry 11
Relevance of Dir.1999/93/EC 11
U.K.'s implementation 14
Use of electronic signatures 16
Use of conformant solutions 17
The legal effect of electronic signatures 17
Trading advantages 17
Additional international perspectives 18
Inhibiting factors 19
Fulfilment of Dir.1999/93/EC's objective 20
HMG use of electronic signatures 21
Oversight 21
Complexity and lack of clarity 22
Data Protection 23
Liability 24
EESSI Standards 24
International Aspects 26
Changes to Dir.1999/93/EC 27
Future Dir.1999/93/EC review 28
Stimuli for market change 30
Clarity of legal effect of Advanced Electronic Signatures 30
Technology neutrality 32
Liability 33
Data Protection 34
Greater consistency in national implementations 34
Clarity for Relying Parties 35
Harmonisation of oversight of Trust Service Providers 35
Awareness of oversight in the U.K. 37
Over-regulation 38
Conformity and Compliance 38
Greater support from HMG 39
Co-ordinated development of Directive and standards 40
Future Dir.1999/93/EC review frequency 42
Miscellany 42
Conclusions 43
About the Authors 45

THIS PAGE INTENTIONALLY DEVOID OF OTHERWISE USEFUL TEXT

Executive Summary

This report is based principally upon focused consultation, undertaken across a broad spectrum of U.K. interests, in order to form a view of U.K. industry's reactions and attitudes towards Directive 1999/93/EC on a Community framework for electronic signatures (Dir.1999/93/EC) and to support HMG in the preparation of a constructive position in relation to the review and possible revision of this Directive. The study has also taken into consideration incidental issues concerning operational procedures related to this Directive and to HMG's role in adopting and promoting the use of electronic signatures, both within government and in industry.

The consultation identified a marked consistency in the views of the respondents on a number of significant issues. The responses showed a general antipathy to Dir.1999/93/EC ranging from outright cynicism about the inevitable effects of premature legislative intervention in an embryonic industry, to resigned scepticism that the Dir.1999/93/EC would ever achieve its objective, as set out in Article 1 (Art.1). Surprisingly, there was a lack of in-depth understanding of the Dir.1999/93/EC, but this could be accounted for by the overwhelming view that it was largely irrelevant to the development of e-commerce in the U.K., at least at the present time. Those who had had greater exposure to the Dir.1999/93/EC, whether directly as a vendor/ trust service provider, or as a legal advisor/ consultant, recognised that the current lack of interest in electronic signatures would probably change at some time. Their view was that it was necessary to ensure that whatever changes to Dir.1999/93/EC might arise as a result of the on-going review process, they should, as far as possible, benefit U.K. industry.

Principle among these issues was the view that the U.K.'s legal systems already conferred legal effectiveness upon electronic signatures, as intended by Dir.1999/93/EC, without the need for significant revision to existing, or introduction of, new legislation. Secondly, the fact that, in the U.K., signatures are rarely required by law in the majority of commercial transactions, means that the Directive has had little relevance or impact on current methods of conducting e-commerce. Respondents pointed out that the intention of the parties to make an agreement was generally enforceable under English law, with or without a signature; and many had focused on technical means to indicate intention, which would not necessarily be considered as an electronic signature as defined by the Dir.1999/93/EC. Additionally, most e-commerce is underpinned by pre-existing / master (paper-based) contractual relationships between the parties, which regulate situations where, otherwise, signatures may have been used.

The variability of implementation of Dir.1999/93/EC in other Member States has compounded uncertainty as to the legal effectiveness of electronic signatures, and has not encouraged U.K. businesses to adopt electronic signatures as the principal means of authentication and integrity in cross-border transactions. It was the view of many that this uncertainty has impeded the development of e-commerce and that Dir.1999/93/EC has failed in its objective of promoting the internal market (Art.1). Some respondents added there may have been some limited success in restraining some of the more excessive measures proposed in German and Italian legislation in 1997 - 99, and in that by forcing business to consider the potential impact of the Dir.1999/93/EC, it has created

debate and raised awareness about the deployment of electronic signatures in a commercial context.

It was difficult to assess the impact of Dir.1999/93/EC on trade between the U.K. and other EU Member States. It would appear that there is very little demand, between commercial entities, for qualified certificates, or indeed for electronic signatures generally, other than that artificially created by the governments of some Member States. Very few respondents were aware of the Electronic Invoicing Directive: none were in a position to comment on the potential impact of implementations by Member States requiring qualified signatures on electronic invoices.

The emphasis must therefore be that the relevance of Dir.1999/93/EC to e-commerce as it currently exists within the U.K. is negligible, but cannot be disregarded where cooperation with partners and counter-parties elsewhere within the internal market is contemplated.

Regarding the U.K.'s implementation of Dir.1999/93/EC, there was considerable empathy towards government's *de minimis* approach. On the whole, the respondents felt that the U.K. implementation was the best that could have been achieved given the obligations to implement the Directive. In particular, there was broad support for the government's approach to the implementation of Art.5(1).

There was little enthusiasm for any legislative change and it was perceived as a potential source of prolonged uncertainty and further impediment to the development of e-business / e-services. Exceptions were changes that would provide certainty that non-qualified electronic signatures would be given the same legal effect as hand-written signatures (where they were intended to be equivalent), and minor changes that might give greater clarity as to the intended meaning of certain aspects of Dir.1999/93/EC. This might include greater prescription in some areas, already defined. There was however a clear view that such changes should not be used to bring about any greater control. This comes from a desire to see greater harmonisation between implementations, at legal, operational and technology levels, without extending the scope and coverage. The call is for consistent minima, not exhaustive over-control.

There was also notable call for greater take-up and leadership in this field by HMG, as a practical user of electronic signatures.

The report concludes that some specific major changes to Dir.1999/93/EC would benefit the U.K. These include revisions to Art.5 regarding the legal effect to be given to electronic signatures, amendments to the scope of Dir.1999/93/EC making it technology specific, clarification of the liability provisions in Art.6 and the establishment of minimum criteria for oversight mechanisms.

These changes should provide greater interpretative detail for Dir.1999/93/EC where interpretation has been an issue, keeping wherever possible to a minimum set of baseline requirements, rather than an exhaustive development of them.

Furthermore, any changes should be only within the present scope of the Dir.1999/93/EC, rather than using those changes as an opportunity to broaden its scoping.

One can conclude that Dir.1999/93/EC has not had any major influence over U.K. industry, that it is not likely to have any such influence in the short to medium term (i.e. before the end of 2004), and that the U.K.'s implementation is supportive of and beneficial towards U.K industry. Changes to Dir.1999/93/EC could make its provisions clearer and more specific, thereby removing uncertainties and possibly differences in implementation and practice, but they should certainly not extend its scope. Some even argue strongly for a severe limitation to its scope, if not abandonment of this Directive altogether.

Thus DTI should use its influence over the European Commission to ensure that there is no extension of scope for Dir.1999/93/EC, that opportunity for its interpretation is resolved in a fashion which applies a *de minimis* approach to establishing specific criteria (for, e.g. supervisory systems), and that nothing is done to change a situation which is presently beneficial to U.K. industry. In addition, DTI and Government in particular could do more to promote and increase awareness of potential benefits of using electronic signatures. This presents a challenge in that opening up debate on what might constitute minimum criteria could be seen as a further opportunity by more authoritarian Member States to establish higher levels of requirements than industry needs to resolve its uncertainties. It could be argued that maintaining the present incertitude is in fact preferable.

As a final comment, it has to be recorded that the study uncovered a far greater degree of indifference, cynicism and lack of faith in private sector use of electronic signatures than it did enthusiasm and belief in a burgeoning market. The fact that there are a few continuing sources of enthusiasm leaves some hope, but there is no doubt that a strong Government lead, if it believes that there is a real benefit to be gained, would be the single greatest encouragement to the marketplace. Otherwise, so far as the U.K. is concerned, electronic signatures and PKIs may remain within closed groups and Dir.1999/93/EC will remain of academic interest.

The alternative is unavoidable external pressure upon U.K. industry (not yet existing) created by broad adoption of more demanding practices amongst other Member States, increasing in number in the medium term, leading to enforced adoption of more rigorous requirements across the board.

Background to this Report

On 1997-04-16 the European Commission presented to the European Parliament, the Council of the European Union, the Economic and Social Committee and the Committee of the Regions a Communication on a European Initiative in Electronic Commerce. This led to the approval of Directive 1999/93/EC of the European Parliament and of the Council of 1999-12-13 on a Community framework for electronic signatures (published in the Official Journal L 013, 2000-01-19, p. 0012 - 0020) - hereafter referred to as 'Dir.1999/93/EC'.

DTI consulted extensively on the proposed implementation of Dir.1999/93/EC in two stages: a consultation exercise in 2001, and a further discussion paper in 2002. There was a good response representing a broad range of interests.

This Directive was implemented in the United Kingdom via two pieces of legislation:

the Electronic Communications Act 2000; and
the Electronic Signatures Regulations 2002.

(It should be noted that prior to the publication of Dir.1999/93/EC DTI had consulted with industry during the initial drafting of the Electronic Communication Bill in 1998 and 1999).

The implementation is unremarkable except to say that it fulfils the U.K.'s Treaty obligations whilst preserving as much flexibility for the future development of the deployment of electronic signatures as can reasonably be achieved. Whilst there may be some scepticism from some other Member States as to whether Art.5(1) has been fully implemented, there is a consistent argument amongst British jurists that it has.

Dir.1999/93/EC is (at the time of publication of this report) due to be reviewed by the European Commission by the second half of 2003.

In 2003-07 the Department of Trade and Industry, Information Security Policy Group, issued an invitation to tender for a study that would centre on a process of focused consultation in order to form a view of circumstances in the U.K. and to support the preparation of a constructive position in relation to the review of this Directive and its possible revision.

This Report is the outcome of that study. It has been produced by Richard G. Wilsher, Managing Director of the Zygma partnership limited and Jane Hill, Barrister at law, Chambers of Benet Hytner Q.C. Specific support was provided by Christopher Kuner, a Partner of Hunton & Williams, Brussels.

Scope & Performance of the Study

The study was commissioned to look principally at the following issues:

- Why the Directive has not had an impact in the U.K. market and whether this is likely to change in the short to medium term as a result of pressures within the U.K. and from elsewhere;

- What sort of changes to the Directive would be desirable and what sort of changes would be unacceptable;

The authors have undertaken a process of focused consultation in order to form a view of circumstances in the U.K. The group of respondents chosen was relatively small, in keeping with the available timeframe for the study and preparation of a report, but broad in its scope. In eliciting input to the study the authors have sought the views of representatives of the following sectors and interests: acadæmia, banking, generalised U.K. businesses, government departments, legal practitioners, providers of systems and components of trust services, trust service providers (including some *tScheme*-approved), voluntary approval schemes. Whilst the majority of these are U.K. based, input has also been taken from sources outside the U.K. Having in mind the relatively small number of respondents, they are not named in order to avoid any inference of specific viewpoints having originated from any particular contributor.

In addition the authors have reviewed all responses to DTI's consultation in March 2001, and the discussion paper in 2002, concerning implementation of Dir.1999/93/EC. In synthesising the totality of available material, the authors have also applied their own experience and expertise in the field.

The Response from Industry

Before reporting on the responses received from some thirty or so individuals from whom the authors took input, it should be noted that, in common with the intended scope of Dir.1999/93/EC, the study was not limited in terms of what might constitute an electronic signature. However, it became apparent that a significant proportion of respondents held the assumption that an electronic signature, under Dir.1999/93/EC, involves the use of PKI technology. The importance of this will be drawn out in the following sections.

Relevance of Dir.1999/93/EC

"*theoretically* it is quite relevant, but it has far less *practical* relevance"

The consultation identified a marked consistency in the views of the respondents on a number of significant issues. First and foremost, by far the majority of those whom the authors interviewed regard Dir.1999/93/EC as being theoretically quite relevant, but having far less practical relevance (some simply said it has ***no*** practical relevance or is entirely irrelevant ***in the U.K.***).

"It is fair to say that it is entirely irrelevant in the U.K."

There are many reasons behind this general perception of irrelevance.

One frequently-cited reason was that existing e-business is based on pre-established contractual relationships, not greatly affected by Dir.1999/93/EC. Because this is the case, there is no need for qualified certificates nor for SSCDs. This may change but not yet - any change will incur costs, and at present adoption of electronic signatures offers no benefits, just uncertainty.

Although one of the driving motivations behind Dir.1999/93/EC was to avoid the adverse effects of diverse legislative evolution and the implementation of licensing systems by Member States, there are across the EU, too many disparate and inconsistent implementations of this Directive (both legal and operational). The variability in Member States' legislations and practices leaves open any certitude as to the effects of electronic signatures, were they to be used as the principal means of authentication and integrity of cross-border e-business. These uncertain circumstances do not encourage the establishment of cross-border transactions built within the framework of this Directive, and may indeed have impeded their development.

Furthermore, concern has been expressed about the uncertainty Dir.1999/93/EC has created in relation to the legal effectiveness of non-qualified electronic signatures in other Member States. The study found that the general irrelevance of Dir.1999/93/EC to

e-commerce as it currently exists within the U.K. was felt by many respondents to have to do with the fact that the U.K.'s legal systems already confer the legal effectiveness of electronic signatures, as intended by Dir.1999/93/EC, without significant revision to existing or introduction of new legislation.

One respondent commented that whereas the provisions of Art.5(1) had been intended purely for a marginal part of the market linked to special acts (e.g. real estate, wills, tax matters, etc.) and Art.5(2) had been intended to cover the much higher-volume general need for electronic signatures, too great an emphasis had been placed in many legal and standardisation interpretations of Dir.1999/93/EC, which gave the impression that a '5 point 2' signature was somehow an inferior level of electronic signature which was not to be generally encouraged.

There is a complete lack of any significant 'Any-Any' activity in the marketplace, where Dir.1999/93/EC places its focus. (This Directive does not apply to closed systems, which some would regard banking systems to be so long as the services offered are only interoperable (technically and by the service definition), and bound by contract, between the subscribers to the bank's service). Furthermore, Dir.1999/93/EC has introduced uncertainty into the market, since many times it can be difficult to ascertain whether a system (such as a payment system) will be considered to be "closed" under the law of a particular Member State.

There are also problems with technological aspects of the implementation of Dir.1999/93/EC. One concern amongst respondents was that there is a lack of clarity about how conformance to the requirements of Dir.1999/93/EC can be achieved and that EESSI has contributed to further confusion in this regard. Then, concerning the technology presently available, there are too many problems with smartcard interoperability, e.g. PCs are generally not equipped with smartcard readers. Furthermore, smartcards need more user action (installation etc.) whereas it is generally easier for the user to download certificates onto their hard drive or install into their browser where users generally don't need to get involved The generally-held perception is that for the time being this is secure enough for most current applications (cf. electronic banking).

"the presentation of individuals [for registration] has no future"

Comment was made about the administrative costs of operating PKIs where the user community is truly unknown (i.e. are open to the public, as opposed to a closed system where the users are already known and identified), and even that many businesses which have implemented PKIs have found them to be costly to operate and offering marginal economic benefits because of this.

In addition, m-commerce is developing but its inherent technology does not readily enable compliance with the requirements of Dir.1999/93/EC and the standards for secure signature creation devices that are established by 'generally recognised' standards. In today's private-sector, mobile phones are the most widespread card reader and SIM cards the most common (potential) signing device. How such devices can be accommodated under Dir.1999/93/EC to allow signing functions that conform to Art.5(1) remains uncertain.

Thus, Dir.1999/93/EC has not been detrimental to the development of the internal market, but has been a brake on its expansion. The uncertainties about it have been another reason to put off doing anything about e-commerce. Many respondents thought that Dir.1999/93/EC (and the U.K. implementation) has had the effect of forcing business to think about electronic signatures – therefore a positive consequence has been greater debate and with it, awareness.

Some respondents also felt that legislative attempts to regulate a new industry in the absence of any market experience were premature.

It was however suggested that, beyond the EU, other observers are regarding the Directive and its attendant EESSI-developed standards with an attitude of "Oh no, not another set of standards and requirements".

This general view of Dir.1999/93/EC's irrelevance was not entirely universal. A number of respondents that had aspirations on providing electronic signature services that would be acceptable outside the U.K. saw Dir.1999/93/EC being very relevant to their operations, but they represented a relatively small proportion of those interviewed. This is discussed further when considering the U.K.'s implementation of Dir.1999/93/EC.

Some respondents felt that the European Commission's intervention had been appropriate in 1997/98 when the legislative activity of some Member States threatened to create significant barriers to the legal recognition of electronic signatures and provision of trust services within the Internal Market. However, they remained sceptical that Dir.1999/93/EC had actually achieved its objectives, given the current deepening divide between Member States and the polarised attitudes between those that favoured qualified electronic signatures and those preferring to allow the market to make its own decisions about what levels of assurance were appropriate. The study revealed a feeling that Art.5 arbitrarily imposed the legal traditions of strict requirements for form in some Members States upon the remainder.

Some respondents expressed a preference for EU law to be expressed in terms of the UNCITRAL Model Law on Electronic Commerce, i.e. simple legal recognition. One legal expert respondent pointed out that linking legal effect to suitability of purpose was unhelpful, since it provides no additional legal benefit by the time one arrives at a dispute.

Another respondent felt that Art.5(1) was not particularly beneficial even in civil law jurisdictions. He pointed out that the technology would still need to be proved in court, i.e. that the certificate had been issued by a CSP conforming with Annex II and that the device used to create the signature was indeed conformant to Annex III. This evidential burden essentially robbed Art.5(1) of any real benefit in legal proceedings.

Some also expressed the view that it was unhelpful to have provisions relating to the legal effect of electronic signature in the same legal instrument as provisions dealing with assurance related to technical use of cryptography.

U.K.'s implementation

There is broad agreement that the '*de minimis*' approach is appropriate. This view was frequently expressed empathetically towards HMG in that Dir.1999/93/EC may have been difficult to implement and that HMG has done so so as to impose a minimum burden upon U.K. industry. No real criticism was noted although some said that it was really too early to give an opinion about its real impact – it doesn't yet affect how business is being conducted.

Again, there was a consensus that there was, to date, no evidence that the *de minimis* approach is harmful to U.K. industry but again, many respondents noted the critical lack of any significant empirical evidence on which to base any objective assessment.

By comparison with other forms of implementation, supporting evidence that suggests the U.K.'s approach is preferable, comes from the number of German businesses that find the requirements of their own regulation to be too much and over-burdensome.

For the time being, the general view is that if this is not the right way, the market place will show that, but in the meantime, the risk of wasted investment through a complex, lengthy and inappropriate approach is minimised.

Shortcomings were raised in the issue of transactions where writing is still required; the respondents commenting on this aspect expressed a wish that HMG would amend relevant legislation as early as possible. These related to the transactions relating to land, consumer credit and health & safety reporting, all prime areas that could stimulate the market for electronic signatures.

In some limited cases, where service providers are aiming to provide services under a broad pan-European branding, there is some concern that the *de minimis* approach is acceptable to their peers in other Member States only because HMG is seen to be making a statement that the certificates and signing mechanisms provided by the U.K. trust service providers are in compliance with Dir.1999/93/EC by dint of compliance with U.K. legislation. Thus, the *de minimis* implementation works in favour of U.K. trust service providers although the fundamental mechanisms involved are not considered to be sufficiently rigid or exhaustive in themselves (by their peers in other Member States). In the absence of any explicit statement from HMG confirming the compliance of trust services established in the U.K. (which, so far as the authors are aware neither has been made nor should be anticipated) one is left to assume that those in other Member States believe that any challenge against the compliance of a UK provider would be made against that service under the U.K.'s legislation.

There was a sharp distinction between attitudes towards how Dir.1999/93/EC had been implemented and the extent to which HMG had actually acted to lead and encourage take-up of electronic signatures. It was suggested that HMG needs to look at business drivers and focus more on on-line activities that can deliver benefits.

"Without a government lead significant take-up [of electronic signatures] wont happen."

There was a notable level of comment suggesting that Government could do significantly more to support this fledgling industry, indeed that it had done far too little. This extended to comments about HMG's failure to establish a credible government-wide policy, to maintain a consistent approach, and educating businesses to help them understand the issues and potential benefits of electronic signatures. There was notable disillusionment that HMG seemed no longer to believe in the dual goals of making the U.K. the best place to conduct e-commerce and to have 50% of government services provided online by 2005.

In this vein, it was stated that education and awareness were of greater importance than the technology. Appropriate business practices and benefits needed to be better promoted, and demonstrated by government.

One particular example of failure in this regard, cited more than once, was that of the electronic VAT return system, where the application had a limited frequency of transactions (four times annually) and the authentication requirements are to be necessarily down-graded to encourage take-up. The Inland Revenue electronic return system received similar criticism. Neither system was seen as having offered particularly appealing incentives or frequency of use (and hence worthwhile gains in efficiency), although Government's efforts were acknowledged.

By way of contrast, clearly some respondents had had positive experience of HMG's attempts to encourage the take up of certification services to access Government services. A specific example given was farmers filing reports under the DEFRA scheme (cited as being one of the most successful initiatives, notwithstanding that participation was still relatively low).,. The example of actions taken by the governments of Canada, France, Germany, Italy were cited as positive examples where industry had been supported in developing the means to conduct business-government commerce electronically, using electronic signatures

Generally, it was felt that the incentives were not sufficient to encourage the effort of obtaining a certificate. It was thought that the process should be easier, i.e. the registration process should be capable of being completed entirely on-line, without interruption. The fact that the process had to be broken, e.g. to provide paper documents, or to receive PIN and password in the post, were viewed as significant impediments to the take up of certificates. Potential certificate holders simply lost interest and did not complete the process. The fact that for these services the opportunity to use electronic submission procedures could be exercised only infrequently and hence did not enable any economy of scale to be achieved through their frequent use was a further disincentive.

Only one service provider was capable, under the current rules, of providing a certificate through entirely on-line registration.

Use of electronic signatures

Very little evidence of the use of electronic signatures was found in the U.K. In particular, no respondent claimed to be using qualified electronic signatures or could foresee using them in the near future. None anticipated any immediate pressure from trading partners in other EU Member State, although few had any awareness of the e-invoicing Directive[1] and how that may affect their thinking and practices. Many respondents were unsure whether their "signing"/ contract formation techniques would even fall within the definition of an electronic signature under Dir.1999/93/EC. Government has been unsuccessful in persuading the citizenry that there is a benefit to them to be gained from using electronic signatures in their dealing with HMG. One respondent suggested that this was because HMG agencies had placed too much focus on benefits to themselves, rather than to businesses and citizens.

"Digital certificates didn't help one bit"

Nevertheless, some recognised that qualified electronic signatures might be demanded by the laws of other Member States, and so there may be a need to develop a capability to conform with such requirements. Whilst this growing awareness might be commended, the downside is that some anticipated, if absolutely necessary, acquiring the necessary services, from that Member State. This was perceived, under the present uncertainties, as the lowest risk option available to them. The attitude that U.K. certification services might be considered as inferior, and therefore electronic signatures based upon them, potentially unenforceable, is clearly detrimental to the development of trust services in the U.K. However, one trust service provider had actual experience of being asked to provide qualified certificates for public use outside the U.K., to meet requirements in another jurisdiction: the experience might have been successful had there not been additional (technical) interoperability problems. Other service providers could also foresee situations where the availability of qualified certificates in the U.K. would be required by U.K. businesses and/ or citizens for cross-border transactions, but did not see that as being imminent.

"Take-up has been painful"

The overwhelming response seemed to be that there was only minimal use of electronic signatures in the U.K. Most e-commerce was based on "click wrapped" agreements, which may or may not fall within the scope of Dir.1999/93/EC, or on e-mail transactions. The most significant electronic commercial transaction type mentioned was personal electronic banking; whilst this undoubtedly makes use of encryption and cryptographic techniques, there was currently little perceived need for transactions to be secured by certificate-based authentication or SSCDs.

One respondent simply questioned whether (in the U.K.) a single qualified certificate has yet been issued to the public. The predictable answer appears to be no, although some trust service providers have apparently investigated the possibility.

[1] Dir.2001/215/EC of the European Parliament and of the Council of 200205-07 amending temporarily Directive 77/388/EEC as regards the value added tax arrangements applicable to radio and television broadcasting services and certain electronically supplied services

Use of conformant solutions

Whilst there is a significant extent of product and systems that are claimed to be conformant with the requirements of Dir.1999/93/EC and with related standards (including those now 'generally-recognised') there has been relatively little investment of time and resources in having conformity determined by third-party assessments. This situation was observed not just in the U.K. but also in other Member States.

There is also little evidence of actual requirements (from the marketplace) for Dir.1999/93/EC-compliant solutions, so there is little driving providers towards formal assessment to establish the conformity of their solutions.

The legal effect of electronic signatures

There was no concern expressed about the legal effect of an electronic signature in the U.K. (with the exception of those who commented on certain legal requirements for writing). However, the acceptability in other Member States, particularly of non-qualified electronic signatures, is a matter of concern, both for U.K. industry and for the residents of these other countries. As an example, the authors understand there to be major confusion amongst businesses in Germany about whether they will be able to use non-qualified signatures for commercial transactions at all, given the potential implementation of the Electronic Invoicing Directive there.

There was concern about the legal effect, or lack thereof, of non-qualified electronic signatures in other Member States.

Trading advantages

The study did not reveal any trading advantages arising from the effects of the Dir.1999/93/EC. As stated in the foregoing, no-one felt there was undue pressure from other Member States (although, again, few had considered the e-invoicing Directive). There was, however, concern about the potential effect upon U.K. businesses trading within Members States that may require electronic invoices to be signed by qualified electronic signatures. The scope of this study did not permit any significant analysis of this area.

So far as use of electronic signatures in cross-border e-commerce is concerned, the European Union Member States are effectively separate islands. Until they coalesce by dint of cross-border e-trade, Dir.1999/93/EC will remain relevant within each Member State only in terms of its chosen implementation within that State. At the present its lack of harmonised implementation is a barrier to cross-border trade, but that is only a part of the story. Before this can even begin to happen there must be significant take-up of electronic signatures.

A few respondents thought that new laws which replaced existing statutory requirements for writing would be based on electronic signature principles and that public key

cryptography could conveniently provide strong evidence relating to the attribution of an electronic signature to a person, and the integrity of what was "signed".

A number of respondents referred to the "killer application" although none could define what it might be. It became clear from responses on this issue that there was effectively a vicious circle: citizens would see no benefit in investing in a certificate until there was an application or applications that made the cost worthwhile and made the signing and verifying process convenient; business would not provide such applications whilst there was only minimal deployment of certificates, and whilst there were cheaper forms of electronic "signing" or authentication which carried acceptable levels of risk. Additionally, so long as these methods continued to be acceptable to on-line providers, customers would see no reason to demand higher security. Most saw the driver for change coming from Government. Some saw Government as being the vehicle for achieving wide deployment of certificates. This could be via various schemes, e.g. entitlement cards, travel cards issued by the passport office or because of the requirements of the Government Gateway.

One respondent thought that an increase in online fraud or other crime would drive businesses towards the use of electronic signatures services as a counter-measure to the increased risk and losses being suffered.

A significant fillip to this could be further facilitation by HMG to help industry move into the e-age. The Prime Minister's commitment to have 50% of citizen to government services transacted online by 2005 could be the basis for realising this. It would seem that, without significant focus, this target is unlikely to be achieved with solutions that use electronic signatures.

Additional international perspectives

Some interesting specific observations regarding international aspects of business arose from discussion with respondents. One is that businesses outside the EU are asking for compliant products and services as a safeguard (when trading with partners within the EU). Other evidence indicates that systems are described as 'capable of complying with' rather then being 'conformant to' Dir.1999/93/EC.

A further observation is that some of those countries that will be shortly joining the EU during its enlargement have forged ahead with 'over-enthusiastic' implementation of this Directive within their own legislations, on the assumption that it is 'right' and that its provisions are all mandatory. Such an example is where the option of having a voluntary approval scheme has been implemented as a mandatory requirement by national governments where there is probably no need or benefit. In doing so they may have substantially de-motivated the marketplace and stifled the development of trust services and the uptake of electronic signatures.

Inhibiting factors

Overwhelmingly, the view was that the lack of demand in the market place was the major inhibiting factor to the take-up of electronic signatures. Service providers said this about the market place in general; businesses said it of their trading partners. Various reasons were suggested, probably none of them a single cause.

It was felt that potential users were confused about what they needed; there was lack of clarity in terms of legal requirements and in general, businesses have no understanding of the need to conduct a (business) risk assessment to help them determine what risks they may face and what degree of security they need in their use of electronic signatures. This view was not exclusively put forward by vendors.

It was recognised that some Member States favoured qualified signatures but (as yet) that did not appear to have had an impact in the U.K.

Others cited a lack of inter-working applications as a significant factor inhibiting growth of the market place, whilst also identifying a lack of user education and understanding as an impediment to the use of electronic signatures. Responsibility for this was placed partly at the feet of service providers who, it was said, put too much focus on the technology without explaining adequately the benefits. This attitude acted as a major turn-off.

A further factor was that certificates were regarded as being generally too expensive to use (i.e., not just the purchase price *per se*, but the incumbent costs of procurement, installation, personnel training) for the benefits to be gained. Consumers (in the widest sense) do not see a real benefit for the time and effort involved in applying these concepts. The line seems to be ‘if it ain’t broke, don’t fix it’!

Some respondents questioned rhetorically whether businesses have yet reached a stage where the idea of doing business without stronger authentication (integrity) and confidentiality is “unthinkable”. Such an attitude needs to evolve through an understanding of the benefits and efficiencies of using electronic signatures along with an understanding of how to perform a risk analysis to justify these choices. Once this becomes a matter of concern then demand will develop.

One respondent raised the issue of inadequately secure certificates and the potential for fraud and other crime. They felt that government complacency in relation to information security in electronic signatures did not mirror its concerns expressed elsewhere e.g. money laundering, computer crime and terrorism. This was perceived as another example of Government inconsistency.

Fulfilment of Dir.1999/93/EC's objective

The objective of Dir.1999/93/EC has been expressed as being: "*To ensure the proper functioning of the internal market in the field of electronic signatures by creating a harmonised and appropriate legal framework for the use of electronic signatures within the European Community*" [2].

"What internal market?"

No respondent felt that this objective had been achieved in practice. Many questioned the existence of any harmonised internal market involving electronic signatures and reinforced the point by indicating a simple lack of empirical evidence on which to judge success.

A valuable spin-off effect, noted by a small proportion of respondents, was that publication of Dir.1999/93/EC has increased awareness of electronic signature issues, especially the underlying technology. It was thought that this may have forced businesses to inform themselves about the benefits and disadvantages of electronic signatures, but that this Directive had failed to generate confidence in, or to have enhanced the take up of, trust services either in the U.K. or elsewhere in the EU. This comment should also be considered in light of previous remarks about technology being promoted more than business benefits.

A number of other reasons for the lack of achievement of this Directive's objectives were commented upon.

Firstly, alternative solutions are more straightforward, pragmatic and less troublesome. An example cited a number of times was the use of pin and password access and authentication to systems at large, allowing whatever transactional activity was then required.

Furthermore, Dir.1999/93/EC lacked clarity and national implementations have been inconsistent and confusing; This Directive was premature and had impeded the industry development of products and services through fear of conformance requirements foreshadowed by Annexes I-III inclusive. In addition, Art.5(1) does not actually deliver unequivocal legal effect for qualified electronic signatures, even in civil law jurisdictions.

Finally, differences in scope and implementation of the Supervisory Systems and Voluntary Approval Schemes implemented in the various Member State hinder inter-operability in procedural and other areas (this is discussed further below).

[2] Source: http://www.europa.eu.int/scadplus/leg/en/lvb/l24118.htm.

HMG use of electronic signatures

There were many comments about HMG use of electronic signatures, particularly in its dealings with citizens.

As far as the consultation process has determined (a small number of Government departments only were interviewed) there are few services requiring electronic signatures, none of which require qualified certificates, and the bulk of services are establishing lower assurance authentication requirements based upon other technologies. These are being applied as pragmatic solutions which enable rather than impede the roll-out of services. Nonetheless the citizenry remains cautious if not reluctant to adopt electronic interaction with Government. Established paper processes remain the simplest and most manageable.

Oversight

This broad term covers Supervision Systems (SS: ref Art.3(3)), Voluntary Approval Schemes (VAS: ref. Art.3(2)) - both of these are directed at service providers - and Designated Bodies (DB: ref. Art.3(4)) - concerned with the conformity of user products.

"I would have no idea who the supervisory body is"

It is clear, even amongst those close to these matters, that the U.K.'s position and established mechanisms for Supervision are not well understood by the business marketplace (and certainly, by extension, by lay persons whom Government would wish to be users of these technologies and concepts). Uncertainty as to the body or agency responsible for supervision, and the idea that *tScheme* is the U.K.'s supervisory system are both prevalent within and without the U.K. The authors note that during the 2001 consultation process many respondents at the time were confused as to the distinction between *tScheme* and both supervision and the role of a Designated Body. It appears that, despite the general awareness which has come about from the publication of this Directive, the period since has done little to eradicate these particular misunderstandings.

**"I fully endorse the self-regulatory approach -
it encourages development of the marketplace"**

A significant majority of respondents continue to favour the *de minimis* implementation adopted by HMG, although some expressed a preference for mandatory assessment for both services and products, rather than VAS. Some sought greater specification of how VAS should operate, in preference to supervisory systems, with the expectation that this would enhance compatibility and cross-border mutual recognition of voluntary approvals (although since VASs are to deal with 'enhanced' services, this, in the authors' view, leaves a vacuum at the level of basic oversight requirements).

TSPs in the banking and telecommunications sector especially called for minimum additional supervision, being already subjected to supervision by virtue of being within a regulated industry. In the banking industry in particular, apart from oversight from the

Financial Services Authority, the sector is subject also to measures from the European Central Bank to regulate trust services. There is, therefore, a danger of over regulation by different authorities with potentially differing regulatory systems.

More than one respondent expressed a dislike of the rigour of the German system but added "at least you know where you stand with it". Eradication of such uncertainty seems to be one of the keys to supporting cross-border e-business. Indeed, where respondents were located outside the U.K., there was a view that a compromise between the U.K.'s approach and the "very rigid interpretation" to be found in Austria and Germany was a desirable solution.

Complexity and lack of clarity

Many respondents expressed a view that Dir.1999/93/EC is indeed over-complex and too far-reaching. Moreover, many made a subtle differentiation between complexity arising from addressing many topics and complexity arising from varied interpretations all claiming conformity. There was a wide (but not uniform) consensus that what is required is more specific guidance for the current provisions (serving to limit a plethora of alternative interpretations and implementations) but not more provisions. Enough has been done in terms of the broad scope - the 'how' is what now matters.

There was also the suggestion that there is a general lack of understanding of what Dir.1999/93/EC really wants, or is trying to achieve, which leads to an unclear view of how to approach the implementation of this Directive. This, by implication, applies to Members States' governments.

A further point raised frequently (but not overwhelmingly) was the issue of the supposed technology neutrality of this Directive. Although Dir.1999/93/EC attempts to adopt a technology-neutral stance its language is clearly that of a linguistically-neutered PKI. This becomes increasingly evident by virtue of the standards published under the EESSI banner. A number of respondents made the observation that this language didn't do much other than confuse things where direct, technology-specific, terminology could have been more effective, and requirements might be clearer. There were suggestions that Dir.1999/93/EC should be limited in scope to the supply of PKI based services to the public. Therefore, any legal effect of electronic signatures should be dealt with in a separate directive (if necessary). Some also favoured the removal of any legal presumption in relation to the evidential value of the technical components (i.e. under Art.3(5)).

One particular comment was that since much of the focus of this Directive is around (pseudo-)PKI then Art.5(1) should be explicitly related to that technology, and technologies which offer lower inherent levels of assurance should be the subject of Art.5(2). Another respondent correctly pointed out that the definition of an electronic signature in Art.2(1) includes typing one's name at the end of an email, something that millions of people do every day. However, the majority of respondents held the assumption that an electronic signature, under Dir.1999/93/EC, involves the use of PKI technology.

A number of respondents shared a view that there is too much focus in Dir.1999/93/EC on the concept of a signature *per se*, which ignores contextual circumstances of commercial transactions, where the transacting parties actually shoulder the responsibility to ensure the good standing of the other, rather than relying simply on the certificate alone. Such a change of perspective might give greater utility to certificates, rather than have their use restricted by liability and other limitations as to use. These comments apply as much to the framework provided by this Directive as they do to the EESSI specifications which have been developed with the intention of helping adoption of the Directive. The contrary view was that certificate service providers needed to recognise that, in order for their certificates to have any real commercial value, they would have to accept responsibility for the information they were certifying, e.g. a certificate where virtually all liability is disclaimed is useless in a business context. In this respect there was support for the provisions on liability contained in Art.6, although it was considered that Art.6 was badly drafted and failed to reflect its original purpose. Comments made also suggested that certificates of equivalent assurance to qualified certificates were being issued, although they did not claim to be "qualified" because of the liability implications.

Turning to Secure Signature-Creation-Devices (SSCDs), exactly what is required to have such a device determined as being in compliance with this Directive's requirements (set out in Annex III) is unclear, since both Art.3(4) and 3(5) offer alternative solutions. Art.3(4) permits conformity to be determined by bodies designated by Member States and requires that such a determination shall be recognised by all Member States, whereas Art.3(5) grants a presumption of compliance when an electronic signature product **meets** [the generally-recognised] standard (authors' stress). Uncertainty arises in a number of ways - how is one to know which are the bodies designated in any given Member State? How would conformity be expressed? What does it take to 'meet' the standard? How are these articles related (the U.K.'s view, shared by certain other Member States, is that they are independent of one another)? How does a relying party ever establish whether these requirements are fulfilled? Hence, whilst some U.K. providers may be tempted to claim their compliance in accordance with their interpretation of one or other of these articles they have no guarantee, and in some specific Member State perhaps no confidence, that their claim would be accepted at face value.

Data Protection

Whilst some points were raised on this topic, no-one expressed real concerns. None of the respondents considered the requirements of Art.8(2) to be more than what one would expect of a quality service provider. On the other hand, some respondents felt that Art.8(2) was unnecessary and may be yet another inhibition to providing certification services. It was pointed out that data gathered during the registration process was not "sensitive" within the meaning of data protection law, and there was no justifiable reason for giving greater protection to data gathered by certification services than, for example, financial data gathered in the normal course of business. Others felt that data gathered in the registration process was valuable, and if CSPs could use it (without further restrictions than currently imposed by Data Protection Act 1998) then it may encourage more CSPs to develop, and perhaps to evolve, their businesses.

Liability

The complaint in relation to Art.6 and its U.K. implementation was mainly in relation to the reversal of the burden of proof. There was a notable lack of confidence as to how this would be handled in a legal dispute, given that it was outside the general experience of English courts. The prevailing view amongst lawyers was that its other provisions were confusing and unclear but probably did not substantially affect what was likely to be the situation in legal proceedings, had Art.6 not existed. Some expressed scepticism about the enforceability against consumers, in any event, of disclaimers and limitations which were likely to be "buried" deep in certificate policies or certification practice statements, not easily accessible to relying parties. One respondent suggested that the liability clause should be simply removed.

Most service providers choose not to make the claim of issuing qualified certificates, even though their systems may be technically compliant in nearly all respects, having concluded that there would be so many restrictions on use that the supporting value of the certificate would not have wide applicability or be worthwhile. There were also difficulties identified in placing a value on a transaction, and therefore in establishing maximum liability limits.

The overall view was that services and certificates equivalent in terms of assurance would be offered, but that service providers in the U.K. would not claim "qualified" because the liability aspects were unclear. One respondent thought that approval of a certification service by *tScheme* would give the same hallmark of confidence as calling the certificate "qualified" (however, to the authors' knowledge, there is nothing in the information published by *tScheme* which could be construed to imply this). The authors would note that whilst this might be so within the U.K., this may not be the case in other Member States, at least not until some broader harmonisation between VAS is achieved (such as is being pursued by ViTAS[3]).

EESSI Standards

Irrespective of their formal status and the manner of their preparation, this report will use the term 'standard' in a generalised sense to refer to the outputs of the EESSI programme.

One significant concern was that the EESSI process had been initially presented as being 'pre-standardisation', but that the publication in Commission Decision 2003/115/EC[4] (CD.2003/115) of references to "*generally-recognised standards*" had effectively usurped the process of moving CEN Workshop Agreements (CWAs) through a formal procedure to establish them as ENs (European Standards).

This was seen to be inappropriate and not in accordance with normal standardisation practices, and had denied national standards bodies their role in the formal standardisation process.

[3] Voluntary Trust-service Approval Scheme common interest group - see www.ViTAS-cig.org.
[4] Commission Decision of 2003-07-14 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC

Other comments reflected a frequent view that the ETSI Technical Specifications and CWAs had been written too much in isolation, that there had been insufficient synchronisation between them, that they covered too broad a range of areas, were too much in-depth, and finally that they were immature.

On the other hand, there was some limited support for the EESSI outputs, with the publication in CD.2003/115 of the three references being seen as having given clarity, removed a degree of doubt and indicated the acceptability of these standards as the basis for harmonisation and potential cooperation between oversight mechanisms.

"There is no business incentive - it needs to be customer-driven"

The more typical response was to question the relevance of EESSI standards in a marketplace where major players are very likely to dominate, and where any adoption of these new standards will be slow. Their take-up was not expected to happen without significant customer demand. There was also a view that they were set at too high a level, in too prescriptive a fashion.

Moreover, whilst some respondents took the view that the publication of references to three CWAs was good in principle, it tended to beg questions such as "But what are they?", "What do they mean?". A number of respondents remarked that despite publication of references to these *de facto* standards it was still too soon to give an opinion as to the value or contribution of CD.2003/115, since the marketplace "still doesn't know what they are yet".

Some respondents felt they needed more guidance at the EC level on conformance, but not more standards from EESSI. Furthermore, this guidance was not necessarily required to be normative (although the authors note than if it is not, there is then a question of how to assess against an optional and potentially variable specification). One respondent drew comparisons with the IETF PKIX group, whose outputs have been mainly Requests For Comment (RFCs). The main point made was that an RFC cannot achieve a recognised "Internet Standard" status until at least two interoperable implementations have been accomplished.

The EESSI standards were also criticised for focusing too much on the "high end", i.e. qualified signatures, rather than specifying "light touch" minimum assurance levels, which may have had more immediate commercial value.

A few commentators argued that whatever the current opinion as to the value of the EESSI standards, only a period of stability and availability will finally determine their worth.

"Technology self-gratification without any functional benefit"

Specific comments were made concerning the standard for Secure Signature Creation Devices (SSCDs), in that it was far too demanding, that the specified evaluation level EAL4+ (augmented) was too high and that business users would ameliorate their risks in other ways (rather than relying simply upon a 'super-secure' hardware token). Some also were concerned that the focus on SSCDs had been on smart-card implementations,

challenging the technology-neutrality of Dir.1999/93/EC. Some were further concerned that this might imply that other forms of SSCD, SIM cards, USB tokens etc may be not be regarded as conformant with Annex III.

There was a viewpoint was that theses standards should be developed by "industry, not by academics". The authors, in their separate capacities as experts within the EESSI standards development process, are inclined to observe that there is indeed substantial industry representation within the work-groups as a whole, and within the specialist teams, and that a high proportion of the participants are active participants. The difficulty has often been in securing a sufficient level of interest from a wider audience when these standards have been published for public comment, prior to their formal adoption.

International Aspects

Few of those interviewed had sufficient practical experience to offer views on this subject. Those who did have that experience expressed concerns that Dir.1999/93/EC posed serious problems for the acceptability of foreign electronic signatures, qualified certificates and SSCDs produced outside the EU. The most forceful view was that this Directive created a protectionist regime, which could probably only be resolved by action at the level of the World Trade Organisation. This was not seen as a realistic possibility, for the foreseeable future.

Others commented at a more pragmatic level about the difficulties of providing conformant services and products into the EU, that were intended to satisfy the requirements of Annex I or III. Art.6 posed a major impediment to the provision of "foreign" qualified certificates, in that it imposes certain statutory rules that cannot be replicated by contractual means, while Art.7 did not do enough to ameliorate that effect. Suggestions were that Dir.1999/93/EC could provide for reciprocal arrangements such as those in Arts.25 & 26 of the Data Protection Directive, or by drafting model contractual terms for service providers issuing qualified certificates in substitution for Art.6. The latter was felt perhaps to be adequate, given the view that the reversal of the burden of proof in Art.6 probably would not achieve its intended purpose in any event.

The view was expressed that it would be preferable if the FIPS-140 standard was recognised as appropriate for the evaluation SSCDs under Annex III, but there was also acknowledgment that a separate product certification for the European marketplace was acceptable so long as that certification was against international standards and enjoyed mutual recognition across all Member States and preferably beyond (e.g. in the form of a Common Criteria evaluation).

There were no specific suggestions from any of the respondents as to changes to Art.7, nor in respect of Recital 23. The authors themselves have refrained from making any observations in this regard in the belief that until such time as some harmonised criteria are established at least for supervision the European Commission neither has a basis for negotiation with any other nation states or economic groups, nor for determining what precisely 'enhanced' services might be enhanced with respect to. Nonetheless, the importance of Recital 23, the facilitation of cross border certification services with third

countries, the legal recognition of ***advanced electronic signatures*** originating in third countries, and the Commission's duties under Art.7(2) should not be overlooked

Changes to Dir.1999/93/EC

Some respondents felt that the Dir.1999/93/EC had so completely failed to achieve its objectives that to pursue a process of review was to perpetuate a myth, "like the Emperor's new clothes", although this is not interpreted by the authors as to suggest that no participation whatsoever in the EC's review of this Directive is necessarily a suitable approach to take.

Most comments focused on potential amendments to Art.5. The main concern was to ensure legal effect being given to non-qualified electronic signatures, particularly those that fulfilled the requirements of an advanced electronic signature (Art.2(2)) and were intended (by the signer) to be the equivalent of a 'paper-world' signature. Various means of achieving this were suggested:

- Σ Removal of Art.5(1) so that no specific legal effect would be given to any electronic signature. Instead, electronic signatures would have to rely on the evidential value afforded by the technical components used in their creation. (Some critics suggested that Art.3(5), that gives evidential value to signature products conforming to 'generally recognised' standards, to the identities of which have been published in the Official Journal, should also be removed);
- Σ The existing text of Art.5 (or indeed the entire Directive) could be replaced (in its entirety) with text similar to Art.9 of the Electronic Commerce Directive[5]: "*Member States shall ensure that their legal system allows signatures to be made by electronic means. Member States shall in particular ensure that the legal requirements applicable to signatures neither create obstacles for the use of electronic signatures nor result in such signatures being deprived of legal effectiveness and validity on account of their having been made by electronic means*";
- Σ If the wording of Art.5 as a whole is not revised as suggested above, then the terminology of the text should be amended to reflect the fact that PKI is the essential focus of this Directive, and relate Art.5(1) to refer specifically to PKI, leaving Art.5(2) to refer to other technologies, e.g. pin and password. Neither need be given greater legal effect, although the degree of assurance would differ in each case and would need to be taken into account by the parties to a transaction.

The intended effect of these options was to create a level playing field for all electronic signatures intended to be the equivalent of "paper world" signatures. The proponents believed that there were many options for businesses either for contract formation, "signing" or for access control: decisions on what is appropriate should be based on a risk assessment of the purpose for which the electronic signature (or alternative) is to be used. However, there was no consensus as to how Art.5 should be amended. Although

[5] Dir. 2000/31/EC of the European Parliament and of the Council of 2000-07-08 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

the concept of creating the distinction between PKI and non PKI electronic signatures seemed attractive, there are dangers that this will encourage the idea that somehow one is inferior to the other. A popular view was that a revised technology-neutral Art.5 should exist independently of, or replace the Directive, and that if regulation is necessary for PKI technology, then that should be contained in a discreet legislative instrument. Indeed, there were some who opposed the removal or amendment of Art.5(1) because a number of enterprises had invested substantially in developing solutions taking advantage of the provisions of this Article.

Some respondents had regard to the legal traditions in some Member States (notably Germany and Austria) that give specific legal consequences to conformance with formal requirements: therefore the abolition of Art.5(1) may be strongly resisted by those Members States.

At least one respondent commented that Art.5(1) did not actually deliver its perceived benefits in terms of legal certainty because of the opportunities to raise challenges in respect of the signature products themselves, e.g. how could a relying party prove that a claimed qualified signature conformed with Art.5(1)?

Concerning other aspects of Dir.1999/93/EC, one respondent suggested that the entitlement for national administrations to effect special conditions (through Art.3(7)) should be removed, so as to allow use of the same services and technologies between businesses and in their dealings with government.

Another comment made was that, with due consideration to security, multiple hosting of a user's key should be enabled so as to give the user the use of the same signing identity from multiple platforms (e.g. fixed PC, portable PC/PDA or mobile phone). The impact of this would not only be on Dir.1999/93/EC, but to standards presently requiring no key export and to technologies which generate and store keys. This would require, above all else, major adjustments to current thinking in the e-security field (whereas, the authors suggest, the average user would welcome this as a practical facilitation of their electronic signature capabilities)

Respondents also complained about ambiguity, and lack of practical relevance in many aspects of Dir.1999/93/EC. There were a number of suggestions for minor amendments, that are discussed later. Collectively, these complaints related to almost all aspects.

Future Dir.1999/93/EC review

A typical opinion as to when any further review should occur placed a dependency upon what changes the Commission's current review produces. There was a consensus that the review period had to allow the market to adapt to changes, and that measurable results had to be seen: there had been inadequate opportunity to date to see any positive effects of Dir.1999/93/EC, given delays in national implementations and the slow development of trust services.

With few exceptions, most respondees suggested a period of from three to five years before further revision is contemplated. Of the exceptions, some favoured short-term 'mini-reviews' (to test whether there was a need for a full review process), whilst one other suggested they be held only when legislative intervention is unavoidable, e.g.

because things have obviously gone seriously wrong or because preset goals are obviously not achievable.

Whether a 'mini-review' could be accommodated within the administrative structure of the European Community was a concern for some respondents.

Whatever the outcome of the current Commission review, any delay in concluding it or planned further review which did not give the marketplace a chance to get on with working with a stable Directive would be harmful to Europe as a whole.

Stimuli for market change

Analysis of the input to the study and the authors' own experience in the field suggest a number of potential stimuli for positive change in the marketplace. These are each discussed below, and with each the authors describe what they believe would be suitable changes that could address the issues and also identify specific courses of action that could work against the suggested stimulus or be counter to the interests of U.K. industry.

Clarity of legal effect of Advanced Electronic Signatures

Currently, Art.2(2) defines an advanced electronic signature but does not attribute any specific legal effect to it other than the legal validity (admissibility) afforded to a non-qualified electronic signature under Art.5(2). Art.2(2) is representative of many of the attempts in the late 1990's to identify the essential functional components of a handwritten signature. From a jurist's point of view, the elements Art.2(2) a) –d) do not necessarily reflect a strict legal analysis, but are sufficiently plausible to reflect the functional components that should be expected of a signature equivalent in the electronic world.

The one vital element that is conspicuous by its absence in Art.2(2) is the signer's intention to "sign". Signatures in the paper world stand as powerful evidence of this intention. Recent controversy over the dual use of electronic signatures for authentication as well as "signing" purposes have thrown considerable doubt over whether even a qualified electronic signature (without additional supporting evidence) can truly replace a handwritten signature as incontrovertible evidence of a signer's intention to indicate a legally binding commitment. Although a number of respondents cited the UNCITRAL Model Law and the U.S. Uniform Electronic Transactions Act as a preferable approach, none mentioned the question of proving an intention to "sign" (implied in the former and specified in the latter Model Laws). Indeed, this would be a substantial evidential burden to impose on a relying party and one that is not required when relying on a handwritten signature – the signature speaks for itself, unless, for example, there is a suggestion by the alleged signer that it has been forged or obtained by deception.

Additionally, how should any legal effect attributed to an advanced electronic signature be compared to that given to a qualified signature? Some might argue in favour of a permissive effect, rather than the mandatory effect of Art.5(1). However, this is likely to fall foul of the same criticisms currently levelled against Art.5(1), namely that it fails to deliver the legal certainty that was intended by its drafters. The most favoured solution to achieving parity between advanced electronic signatures and qualified electronic signatures is to remove Art.5(1) altogether.

There have been, both from respondents to this study and from other sources, calls for the removal of Art.5(1), which some regard as being an impediment to the growth of electronic signature usage. Objection to Art.5(1) is also driven partly from the fact that it

tries to resolve a need of civil law systems and by doing so establishes a difficulty for common law systems.

Possible change

The existing text of Art.5 could be replaced (in its entirety) with Art.9 of the Electronic Commerce Directive, to whit: "*Member States shall ensure that their legal system allows signatures to be made by electronic means. Member States shall in particular ensure that the legal requirements applicable to signatures neither create obstacles for the use of electronic signatures nor result in such signatures being deprived of legal effectiveness and validity on account of their having been made by electronic means*".

There are a number of likely implications of such a change:

- This would not force significant revision to Member States current implementations of Dir.1999/93/EC (if any): the Electronic Commerce Directive has been implemented in all Member States;

- The revised Art.5 would not impinge on Recital 21 of Dir.1999/93/EC, although some changes would be needed to Recital 20;

- The change should preserve Member States' rights to lay down different requirements for handwritten signatures (and indeed their electronic equivalents in appropriate circumstances). This potentially benefits the U.K. although it will inevitably still permit other Member States to require qualified electronic signatures as a matter of national law. In order to try to achieve some objectivity, a provision could be included to the effect that such national requirements should be proportionate, transparent and non-discriminatory (despite the fact that words are often considered to be impotent, it is the authors' experience that on occasions they do have some cautionary effect on government agencies);

- The revision would not therefore affect national laws in Member States that impose specific technical requirements for certain purposes, e.g. in response to the E-Invoicing Directive;

- The revision may have the effect of removing reliance on Art.5(1) in some Member States as a justification for requiring qualified certificates as being the only legitimate equivalent to hand written signatures, and in which case, the revision may slow down the deepening of the divide between Member States;

- The revision would remove the presumptions that currently appear to favour PKI-based solutions to the detriment of alternatives;

- The revision would contribute to the Commission's aim to make EC law more consistent.

The authors do not encourage the suggestion that Art.5 should be amended to create a two-tier legal recognition for electronic signatures, i.e. for those based on

PKI technology and those based on other technologies. Whereas there may be a technological argument as to the relative assurance that differing technologies may be capable of delivering, their selection and use within an information system employing electronic signatures is a matter for business judgement and should not be defined or constrained by a legal instrument.

Possible resistance

Resistance to any amendment to Art.5 may come from Member States and organisations that have already made substantial investment in the development of products and services designed to meet the requirements for a qualified electronic signature. Whilst this study would tend to indicate that U.K. businesses are unlikely to be in that category, the possibility cannot be ignored.

Technology neutrality

The negotiations of Dir.1999/93/EC were influenced by the UNCITRAL Model Law on Electronic Commerce, which was being adopted in a number of jurisdictions in North America and world wide. The very technology specific Utah Digital Signatures Law 1995 (as amended in 1996) was another notable influence at that time. Dir.1999/93/EC tried to encompass both the technology neutral approach of the Model Law, in terms of giving legal recognition to electronic signatures, as well as adapting some of the principles of the Utah Act to provide a regulatory framework for PKI-based services. It was also believed that within a relatively short period of time (from 1999), biometric technology would be available as an alternative to PKI-based electronic signatures. Dir.1999/93/EC was therefore intended to permit the development of new technologies. In fact, the language (and most of the content) of the Dir.1999/93/EC is heavily PKI biased.

The study received strong suggestions that Dir.1999/93/EC should be confined in scope to the supply of certification services, as set out in Recital 9. There was resistance to the concept (as expressed in Art.5(1)) that any particular use of technology should be accorded specific legal effect; in any event, it was considered inappropriate to include such provisions in a legal instrument that deals essentially with the regulation of a specific type of technology. A consequence of this would be that Art.2(2) and Art.5 should be removed in their entirety. A new legal instrument could be promulgated that would impose obligations on Members States to ensure the legal validity of electronic signatures, perhaps in terms similar to Art.9 of the Electronic Commerce Directive.

It is not considered necessary for Dir.1999/93/EC to allow scope for the inclusion of new technologies. Since any new security technology takes (on present experience) a decade or more to go from its theoretical origins to commercial maturity (or even suitability) such that it would be deserving of attention within the scope of Dir.1999/93/EC, there would be ample time to bring about any necessary revisions to this Directive to accommodate technological developments.

Possible change

Art.5 could be removed in its entirety and the remainder of Dir.1999/93/EC revised where necessary so that its scope is restricted to a *de minimis* level of regulation, being not more than what is essential to promote the development and deployment of electronic signature products and services in the Internal Market.

Possible resistance

Encouraging revision to the text of Dir.1999/93/EC, albeit with a *de minimis* objective, may simply stimulate further the obsession with strict and extensive regulation by those Member States unable to agree a baseline set of criteria. Apart from the potential for extended debate and diversion of resources, this could lead to further strict criteria, completely contrary to the initial objective.

Liability

Art.6 was plainly seen as a major inhibitor to the provision of qualified certificates to the public, although it was clear that there was a potential demand for certificates offering valuable assurance, both in terms of technical security and the registration process for the certificate subject. The liability provisions deterred certification providers from claiming qualified certificate status for their certificates, even though they may meet the requirements of Annexes I and II: this was to the detriment of users who were likely to have enhanced confidence in "qualified" certificates and inhibited the growth of the industry. The mandatory reversal of the burden of proof in Art.6 appears to have been ill-thought through: the resulting implementation in the Electronic Signatures Regulations 2002 is necessarily convoluted and complex as a result. Given the rules relating to discovery and case management in the post-Woolfe era[6], it is questionable whether this provision (in Art.6) will add any significant benefit in the U.K.

Possible change

Art.6 could be redrafted in any event, so as to:

- clarify what is meant by the phrase "*to the public*";
- clarify what limitations of liability or damages may or may not be attached to the issue of a qualified certificate;
- permit Member States to amend their rules of evidence and procedure to protect plaintiffs in disputes against CSPs in a manner most suited to their national legal systems.

[6] Since 1998, the Civil Procedure Rules have radically changed the way that pre-trial procedures are conducted. In particular, Judges are obliged to play an active role in case management, ensuring fairness between the parties in the preparation and filing of evidence for the trial. See the Lord Chancellor's website at www.lcd.gov.uk.

Data Protection

Trust service providers in the U.K provide services based on high levels of assurance: it is paradoxical to make the assumption that personal data is less well-protected by a trust service provider than by other commercial entities similarly handling such classes of data (this especially so when many TSPs are already subjected to rigorous regulation in this regard for other reasons). The responses suggested that there are no serious difficulties posed by Art.8.2, but the prevailing view was that CSPs should ***not*** be discriminated against by dint of stricter data protections requirements than other industries.

Possible change

Following the discussion above, Art.8(2) could be deleted.

Greater consistency in national implementations

The lack of consistency between Member States' implementations of Dir.1999/93/EC was perceived as a major impediment to the use of electronic signatures in the internal market. Effectively, this Directive was seen as having substantially failed in this respect. However, closer examination tends to indicate that the problem lies less with this Directive than with the underlying differences in the legal systems of Member States: Dir.1999/93/EC merely exacerbates these differences. This is compounded by the ambiguity created by the term "digital signature" (meaning a "digital identifier") and the failure by technologists and some lawyers to acknowledge the subtle but significant distinction between this term and an electronic equivalent of a paper world "signature".[7]

As e-commerce matures, it is likely that market forces will drive change and force greater consistency of law and practice amongst Members States. It is noteworthy that despite considerable difference in Members States legal traditions, nonetheless signatures have evolved and endured over centuries as a convenient and reliable form of evidencing consent and commitment to obligations in a commercial and legal context. It may be that it is not possible exactly to replicate a handwritten signature in the electronic world and that a new mechanism will have to evolve: what is clear is that the market will inevitably find its own solution. Over-prescriptive measures by governments will only delay the evolution and hinder the maturation of electronic commerce.

Possible change

As discussed above, Art.5 could be removed and Dir.1999/93/EC could impose upon Members States an obligation that any national laws prescribing requirements of form for electronic signatures should be proportionate, non-discriminatory and transparent.

[7] The former is a signature in the sense of being an identifier (e.g. music signature); whilst the latter, in law, has far less to do with identification but usually implies an acceptance of a commitment, with attendant legal consequences.

Clarity for Relying Parties

The study revealed that not only has Dir.1999/93/EC created considerable confusion for trust service providers and businesses through its lack of clarity, but that this has engendered a lack of confidence in relying parties. In addition, this Directive focuses on issuing certificates, using secure devices, building secure systems but virtually ignores the principal purpose of an electronic signature, i.e. promoting confidence in relying parties in an e-business transaction. Very little emphasis has been placed on issues concerning the secure verification of electronic signatures, without which the technology is almost worthless in a commercial context. Art.3(6) and the recommendations in Annex IV seem largely to have been ignored by both the Commission and Member States. It has not been suggested that further regulation in relation to secure verification is the way forward: indeed extending the scope of current regulation was strongly opposed by respondents. What may stimulate the up-take of electronic signatures (particularly for consumers) is the availability of verification systems that remove any responsibility from the relying party.

Some respondents felt that the future demand to complete more complex or high value transactions on-line may stimulate change. Of those cited, the demand to complete consumer credit transactions on-line is possibly the most likely driver for change.

Possible change

This does not necessarily require legislative intervention, but will involve substantial cooperation between vendors, trust service providers and businesses. This contemplates the availability of solutions that package not just the technology but also the liability, i.e. third party services that perform the verification for a relying party and that thereby assume responsibility, and therefore liability, for doing it properly - the entire process is transparent to the relying party - he doesn't have to install anything or initiate anything, he simply receives a confirmation that all is well or a failure indication. Inevitably, this will require cooperation from OS and browser vendors. Until such solutions are available "off-the-shelf" and offer a trustworthy, reliable, transparent service to end users, electronic signatures are unlikely to be attractive to business or consumers.

The demand to complete consumer credit transactions on-line does not require changes to Dir.1999/93/EC, but a change to the current requirements for writing in U.K. consumer credit law.

Harmonisation of oversight of Trust Service Providers

Dir.1999/93/EC Recital (4) states *"... divergent rules with respect to legal recognition of electronic signatures and the [approval] of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework ..."*.

The authors' observations and the comments of respondents to the study suggest that the manifest truth of this statement (i.e. that a "*clear Community framework*" would

eliminate barriers brought about by divergence) has not been borne out by Member States in their implementation of legislation, nor by the manner of implementation of national supervisory systems, nor by the actions of the ESC[8] (see Art.10).

Dir.1999/93/EC continues, introducing the notion of two mechanisms for overseeing the operation of CSPs. In Recital (11) it is stated (authors' emphasis): "*Voluntary [approval] schemes aiming at an* ***enhanced level of service-provision*** *may offer certification-service-providers the appropriate framework for* ***developing further their services towards the levels of trust, security and quality demanded by the evolving market****; such schemes should encourage the development of* ***best practice*** *among certification-service-providers; certification-service-providers should be left free to adhere to and benefit from such approval schemes*".

One then finds that Art.3(3) **requires** Member States to establish an "*appropriate system that allows for supervision*" whereas Art.3(2) has previously acknowledged that Member State **may** "*introduce or maintain voluntary [approval] schemes*".

This report has already described variances in how SS are implemented and the inherent difficulties that that can give in the recognition and authentication of certificates and signatures in cross-border e-commerce. Specifically, in the U.K. there is uncertainty as to which body is responsible for supervision and, somewhat more concerningly, confusion as to the role of *tScheme* in this respect.

It may also be said that Dir.1999/93/EC is unclear in this area, giving undue prominence to VAS (which are not a mandatory requirement, yet seem to have more focus put upon them than do SS). Thereby, Dir.1999/93/EC diverts attention away from one of the basic mechanisms which could have established harmonisation in one critical area. The fact that VAS are optional and intended to focus on enhanced levels of service-provision (ref. Recital (11)) does suggest that the original intention of Dir.1999/93/EC was to establish a basic oversight mechanism through supervision and leave the provision of more enhanced oversight mechanisms to be determined by the marketplace (by their voluntary nature).

So, whilst Dir.1999/93/EC requires notification of optional oversight mechanisms (i.e. voluntary schemes) it has no such requirement for the mandatory oversight process (supervision), which does little to help relying parties establish the status of certificates issued within the scope of this Directive.

Resolving these matters would establish a clear baseline at or above which the conformity of a service would have to be accepted by any Member State, thus giving an incentive to business to use electronic signatures for cross-border purposes. Creating a baseline, i.e. minimum requirements, would minimise the cost to fulfil the criteria and thus not overburden an immature industry that continues to struggle to establish a stable business case.

It is the authors' view that no additional requirements need be set for VAS - by their nature they are market-driven and respond to the perceived need of 'enhanced' services, the scope of which cannot easily be defined. Such non-mandatory mechanisms should

[8] The Electronic Signatures Committee, known far and wide as the 'Article 9 Committee - A9C' - ref Dir.1999/93/EC Art.9.

not be introduced through an instrument such as Dir.1999/93/EC and developments in this field should be left to the market, signs of which are already emerging in the creation of ViTAS.

Possible change

Dir.1999/93/EC could clarify, possibly through the ESC, minimum criteria for SS, compliance with which would constitute " *..a [**compliant**] system that allows for supervision*" (Art.3(3) - NB the present wording of the Article in this place in the text is '*... an **appropriate** system ...*'). Furthermore, all requirements in Notification (Art.11) could be amended to relate equally to both SS and VAS (there seems to be no reason not to assist relying parties by ensuring that information concerning voluntary schemes is equally promulgated).

In addition, the requirements of Art.11 could be extended to require the European Commission and/or each Member State to maintain an on-line, up-to-date, publicly-available and trustworthy register of all EU oversight mechanisms and the services they implement in response to Dir.1999/93/EC.

Whilst noting the existence of FESA[9], the authors have not explicitly suggested this body be involved in this process, since it is anticipated that its members would automatically be involved through their participation in the ESC.

At the same time as these changes the poor language of this Directive could be enhanced by the straightforward use of the word 'approval' in place of 'accreditation' in each and every instance of it except for Art.5(2) where the amendment should be either 'supervised' or 'supervised or approved'. Once this is accomplished a correct perspective of how a VAS should be established may develop.

Possible resistance

As discussed already under technology neutrality, encouraging revision to the text of Dir.1999/93/EC may simply stimulate further the obsession with strict and extensive regulation by those Member States unable to agree a baseline set of criteria. If UK industry can live within the present constraints of interpretability and disharmonious implementations, this may be preferable to further debate which may be extended and give reason for further pressure from those Member States whose administrations (not necessarily their own business communities) favour greater rigour. With the majority of UK service providers seeking *tScheme* approval it is perhaps better not to rock the boat.

Awareness of oversight in the U.K.

The fact that DTI has notified *tScheme* to the European Commission under Art.11 is little publicised, and of course Dir.1999/93/EC places no requirements upon notification of Member States' SS. The study's findings also indicate that there remains confusion

[9] Forum for European Supervisory Authorities for Electronic Signatures - see www.fesa.rtr.at.

amongst U.K. industry as to the roles and purposes of the various oversight functions and little awareness of the U.K.'s approach to implementing its Supervisory System.

Setting this out in a publicly-available manner would give interested parties in both the U.K. and other Member States a clear statement as to the U.K.'s established position, thus eliminating any misunderstanding as well as perhaps quelling the misinformation that emanates from certain sources.

Possible change

DTI could make publicly available a document that explained the purpose and scope of each of the three oversight mechanisms and then describe for each the responsible body, its contact details and its functional operation. Much of this information would be that already required and provided under Art.11 (Notification) of Dir.1999/93/EC but would be supplemented by description of how these bodies work and how they are accessible (e.g. how to apply to it, how complaints are handled, etc.). Clearly, cooperation with *tScheme* in the production of this would be appropriate.

Over-regulation

There were a number of comments expressing concern about the use of electronic signature technology by industries that were already regulated, i.e. that unless there was close cooperation between regulatory bodies, both domestically and across borders, there was a risk of over-regulation in some industries. This would have a significant financial implication for companies in terms of resources and cost of conformance. There was also a real potential for the emergence of conflicting requirements from different regulatory bodies.

Possible change

This was not perceived as a problem to be solved by any change to Dir.1999/93/EC, but it flagged up a priority need for regulatory bodies to consult and cooperate in the development of regulatory requirements in this area.

Conformity and Compliance

This report has already raised concerns as to what is required to have a secure signature creation device determined as being in compliance with Dir.1999/93/EC's requirements (set out in Annex III) is unclear, since both Art.3(4) and Art.3(5) offer alternative solutions.

There are two issues to be resolved - one is whether these two articles are intended to be alternative solutions to the same fundamental issue. The other is precisely what is required to demonstrate fulfilment of each Article. Setting this out in unambiguous terms would eliminate the uncertainty that presently exists, although the authors note that, in

the case of the responsibilities incumbent upon Designated Bodies, Commission Decision 2000/709/EC[10] addresses this in some depth.

It is the authors' view that it would be in keeping with the general view of U.K. industry and of Government that these two Articles remain as separate items within this Directive, on which basis the following changes are submitted.

Possible change

Art.3(4) could state (or refer to another source that states) how a designation of conformity is to be expressed, with particular regard to its accessibility to any relying parties wishing to have access to that information. This could include, *inter alia*: what information it should convey, in what format it should be presented, how the issuing body can be authenticated and for whom this information is intended. Such a statement could concern itself only with the expression of conformity, not any limitation as to the standards on which conformity may have been established.

In appointing its Designated Body, the U.K. could ensure that that body has the power to recognise and accept evidence based on compliance with standards and processes other than those covered by the 'generally recognised standards' referred to in CD.2003/115/EC.

Art.3(5) could state (or refer to another source that states) that, as a minimum, compliance should be determined by a third party assessment of the subject, applying the provisions of the appropriate part of the EESSI Guidelines for Conformity Assessments. Furthermore, it could address how (not withstanding the indications of the Guidance to which reference has just been made) compliance is to be expressed, with particular regard to its accessibility to any relying parties wishing to have access to that information, as described in the first paragraph of this change.

Greater support from HMG

The authors have found both empathetic attitudes towards the U.K.'s implementation of Dir.1999/93/EC, and a highly consistent view that this implementation is good for U.K. industry, whether looking inwards or to trading with partners established in other Member States. However, there has been notable criticism for government in a broad sense (rather than DTI specifically), generally identifying a lack of leadership in the use and application of electronic signatures and of helping industry and businesses in general understand what are the practical issues involved in them. Although this is an area incidental to the study's primary objective of eliciting credible input, the synthesis of which will help DTI construct a suitable contribution to the European Commission's review of Dir.1999/93/EC, it is pertinent to the present state of play within the U.K.

It might be asked "why should it be Government's role to stimulate the market?". If commerce at large cannot find a sufficiently strong case under present circumstances to bring about the growth in this fragile area, how would active Government adoption of

[10] Commission Decision of 2000-11-06 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.

electronic signatures necessarily act as a positive market influence? Of course, if the mechanisms that commerce might use to interact with Government were interoperable with other communities (of users) and could be used freely across domains then that may influence events, but this is really asking Government to fund the establishment of such a scheme, which in the authors' view is itself is unlikely to happen. One need only point to Finland to illustrate where even very enthusiastic government support has not had a very successful effect upon the marketplace. It is difficult to identify, anywhere in the world, a successful market in e-authentication services, which begs the question "Why is the UK going to be different?".

However, if one returns to the present Prime Minister's declared aim of making the U.K. the best place for e-business, business might reasonably expect some kind of positive input to help make this happen. Further dialog between Government and business therefore seems desirable.

Possible change

Given that this is an issue that is beyond the principal objective of this report the authors feel constrained to make only a limited suggestion as to how this issue could be addressed. There is no explicit change to Dir.1999/93/EC that would solve this matter, but the possible changes identified should address some of the concerns of U.K. industry and if not remove certain barriers or constraints, make their negotiation easier. Furthermore, the extent of changes that are actually applied to this Directive will need to be assessed when finally published, and one might anticipate a period of consultation prior to their publication and implementation.

At this stage HMG could engage with U.K. industry to establish ways in which advantage could be taken of the revisions and a new initiative taken to promote electronic signatures.

One suggestion submitted to the authors was to provide greater support to *tScheme* to allow it to conduct a general awareness programme, undertaken in concert with HMG's roll-out of services.

Co-ordinated development of Directive and standards

Input to the study has been critical of the extent of standardisation undertaken and the process in which it has been performed. In addition to this, the authors would argue that the ESC has insufficiently fulfilled its duty with regard to Art.10 and, furthermore, that what results it has produced have not been made available in a timely fashion, nor in any coordinated way regarding the work that has been undertaken under the EESSI. EESSI itself has proceeded with two bodies responsible for management of their own programmes, only loosely coupled by the fact that the EESSI Expert Team report of 1999-07-12 set out an initial road-map for standardisation.

The basic process of assigning specialists with a mix of skills may be an appropriate way to develop *de facto* standards, in order to short circuit the timescales involved in traditional standardisation. Where there is a relationship between the standardisation

requirement and a specific legislative instrument as is the case here, the process should permit close participation and exchange between national bodies and the drafting team(s). Any changes to Dir.1999/93/EC intended to lead to more harmonised implementation of it need to apply a more obvious co-regulatory approach henceforth. The provision of any further standards should focus on establishing the minimum level of requirement aligned to a common interpretation of Directive's intentions, which should itself use more careful and explicit text.

Possible change

The U.K. could take a leading role and promote a new approach to any further standards development which should:

- Ensure effective liaison between the ESC, responsible for determining a clear and common interpretation of Dir.1999/93/EC's text and requirements, and the standards editing team(s);

- Establish requirements, and draft standards, which set out only the minimum requirements for enabling cross-border e-commerce and use of electronic signatures;

- Put in place an effective management process with a single management body working closely with (preferably) one European standardisation body. (In EESSI so far there has been insufficient connection between EESSI, the ESC, and the management bodies responsible for the actual production of standards. The fact that there have been two management bodies and the incumbent overheads, including wasted time for the editing teams and participating experts is simply inefficient use of limited financial and expert resource);

- Adopt an approach to the formulation of texts that are intended to become de facto standards that allows for their maturation and proven application before they acquire any formal status, i.e. follow the IETF/RFC model;

- Ensure that the development programme and status of the final standards is fully promulgated such that all interested parties can determine the degree of their involvement.

Future Dir.1999/93/EC review frequency

Too-frequent review does not encourage the market place to have confidence in the stability of this Directive, nor to make a commitment to its provisions and those of their own Member State's implementation of it. A period of stability is therefore preferable, and this implies a longer time period between reviews.

Possible change

Establish a review cycle of five years, from the time at which any revisions become effective, possibly subject to the proviso that if the ESC so advised the European Commission, an exceptional earlier review could take place.

Miscellany

A few other much lesser potential changes have been identified. These are summarised below.

Possible miscellaneous/minor changes

In Art.2 the definition of "*signatory*" has received an inconsistent approach in the national implementations as to whether a signatory must be a natural person, or whether this definition can include legal persons. Once again, it may be that Member States should be free to determine according to their legal traditions whether signatures can only be made by natural persons. (This is to be distinguished from a person signing on behalf of a company or other legal person.) It has to be pointed out that whereas the legal issues in relation to automated "electronic signing" need to be resolved, this does not necessarily have to be achieved by a single legislative measure imposed uniformly across Member States: the essential issue is that regardless of the legal rationale at national level, there is a need for automated electronic signatures to be recognised in appropriate circumstances across borders.

Lack of clarity of a number of important terms creates problems for companies active in the market; as an example, it can often be difficult to determine when certificates are issued "to the public", and what is considered to be a "closed system". Greater clarity of such terminology is needed to provide legal certainty for companies offering authentication services.

Annex IV is generally perceived to fulfil no purpose. Given that the co-operation envisaged under Art.3(6) has not taken place, there seems to be no justification for making it mandatory: to do so may be to repeat the mistake of regulating prematurely. This annex could be therefore be deleted without detriment, particularly since it is not mandatory and such mechanisms have no place in an instrument such as this Directive.

Conclusions

The findings published in this report are based upon a series of focussed discussions with a group of respondents that was relatively small but broad in its scope. Nevertheless, although this group was not large in the general sense of obtaining representative views, the authors believe that they were able to obtain contribution to their study from a significant proportion of those players within the U.K. in this field who have an established level of expertise - this is not a large area of competence by comparison with other, more established, technical and legal domains. In addition some further input was taken from elsewhere within the EU.

Returning to the questions that this report is intended to address, the study has found that the failure of Dir.1999/93/EC to have any marked impact in the U.K. is due largely to:

- the general lack of demand for qualified signatures;
- the fact that most e-commerce is based on pre-established contractual relationships (excluding those transactions from the scope of Dir.1999/93/EC);
- the absence of wide deployment of certificates and the perceived lack of benefit from obtaining one by potential users.

In addition, the following are acting as inhibitors to the take up of electronic signatures:

- the wide-ranging variances between individual Member States' implementations of Dir.1999/93/EC;
- within the U.K., but apparently also within other Member States, the uncertainties regarding the need for qualified certificates supporting electronic signatures.

It has been concluded that there are no immediately obvious pressures for short term changes to this situation, although an apparent nascent demand for supporting qualified certificates from U.K. industry's trading partners in other Member States looks like it could have effect in the medium term (which the authors suggest should be taken as being between 6 to 18 months in this business / technology area). A further medium term effect may be the consequence of the publication by the European Commission of CD.2003/115/EC, in that procurers of trust services may cite conformity to these standards as a qualifying condition of supply. Again, the authors were given specific evidence of these standards being referenced now from procurers. Therefore, it is expected that one level of uncertainty may have been removed by the publication of this Decision.

As to whether the objectives of Dir.1999/93/EC have been achieved, the generally-held view is that they have not. There is no great indication that it has succeeded in giving legal recognition to electronic signatures that are intended to be the equivalent of hand

written signatures, nor that it has given rise to standards that will guarantee confidence in (and legal recognition to) electronic signatures. The general view is that the EESSI specifications have been set at too high a level of requirement. The consequence of this is that consumers do not perceive a benefit proportional to the cost of revising their business practices and infrastructure/assets to employ them.

A further conclusion of this study is that, whilst there are no doubt difficulties with Dir.1999/93/EC itself, many problems relating to national treatment of electronic signatures are rooted in the differences in legal traditions, established over centuries, in the various Member States. The consequence is likely to be that until new customs in relation to expressions of commitment (signing) evolve in the electronic environment, these problems are likely to persist. The authors also conclude that these customs are more likely to be driven by market forces than by legislative intervention. According to the study, premature or disproportionate regulation will simply have a "chilling" effect on the development of e-commerce.

Of note, and comfort to DTI, is that the U.K.'s *de minimis* approach to implementation of Dir.1999/93/EC received almost universal approval. This view was endorsed by respondents outside the U.K., although there are two qualifications that should be noted: firstly, there needs to be a clearer framework within which this approach is to be operated, which would give greater credence to the services of U.K.-established service providers, and secondly that some additional rigour might attain an effective compromise and equivalence with other Member States, without going to the extremes that certain countries have gone. The fact remains however that the U.K.'s approach has been regarded as supportive of U.K. industry as a whole and in some ways advantageous for it.

On the other hand, Government has been the subject of significant, sometimes stinging, criticism for its lack of consistency, commitment and leadership in the e-signatures field. In particular, the Government could do more to encourage business uptake by promoting awareness of potential gains from using electronic signatures. This extends to criticism of the U.K.'s poorly publicised procedures for implementing specific aspects of this Directive (most pointedly, the provisions for the various oversight mechanisms).

As to what sort of changes to Dir.1999/93/EC would be desirable, there is a choice of opinions and possible changes which range from the abandonment of Dir.1999/93/EC as a whole, through removal of Art.5 as Dir.1999/93/EC's central provision, through to more modest changes which seek to eliminate uncertainty through greater clarity and specificity undertaken along *de minimis* lines. The study identified a clear message that it would be undesirable for any changes to be made that would extend the scope of this Directive or that would introduce any further regulatory requirements.

Thus DTI should use its influence over the European Commission to try to achieve a *de minimis* approach to establishing specific criteria (for, e.g. supervisory systems), and that nothing is done to change a situation that is presently beneficial to U.K. industry. Such an objective should, however, take into account the possibility that certain Member States might try to use any opportunity for change to apply more demanding requirements.

In addition, DTI and, more particularly, Government in a broader sense could do more to promote and increase awareness of potential benefits of using electronic signatures.

About the Authors

Richard G. Wilsher (*RGW@Zygma.co.uk*)

Richard Wilsher is an independent Information System Security consultant with over twenty five years professional experience. He is a recognised expert in the fields of security, digital signature and public key infrastructure technologies, architectures and standards, security management and the European and global standardisation processes.

He has run his own independent consultancy, the Zygma partnership ltd., since 1993.

He has provided specialist support to DTI in the area of electronic signatures, with specific focus on the implementation of Directive 1999/93/EC, since 2000, in various capacities. Over this period he has had a leading role in the development of *tScheme*, the UK's independent voluntary approval scheme for trust services and is presently the Rapporteur for the common interest group on international harmonisation between voluntary trust-service approval schemes (ViTAS). Additionally, he has been involved in the EESSI work programme since its inception, including as a retained expert in a number of tasks, and is a frequent presenter at various international information security fora.

Jane Hill (*JH@JaneHill.com*)

Jane Hill is a barrister at the Chambers of Benet Hytner Q.C. in Lincoln's Inn, London. She has twenty years experience in private practice. Since 1996, she has specialised in electronic commerce and information security law and is recognised internationally as an expert in this field.

She has been appointed as an expert to a number of projects under the European Electronic Signatures Standardisation Initiative (EESSI); she is also an active member of the American Bar Association's Information Security Committee, chairing one of its working groups.

She has been an invited speaker at a wide range of international information security events.