Response to

DTI Consultation, March 2001

on

EC Directive 1999/93/EC, 13 December 1999

Classification: Rhye Proprietary; Public Domain

Version 1.0 – Final

Author: Peter SJF Bance MBCS CEng

Table of Contents

Author: Peter SJF Bance MBCS CEng

Author: Peter SJF Bance MBCS CEng

Document Overview & Background

On 12 December 1999, Directive 1999/93/EC was adopted by the European Parliament and the Council of the European Union regarding the implementation of a Community framework for electronic signatures. On 19 January 2000, this Directive was published in the Official Journal of the European Communities and summarily reviewed by the Department of Trade and Industry (DTI) in the UK.

In March 2001, the DTI published their *Consultation Document on the implementation of the EU Electronic Signatures Directive* for public review and comment. Responses were invited by 19 June 2001, and the required implementation date has been set as 19 July 2001.

This paper is an official response to the DTI Consultation Document, and is submitted by the Author on behalf of Rhye Internet Solutions Limited (see below). It is also available in other formats (RTF, PDF, Plain ASCII and HTML) from http://www.rhye.co.uk/papers/1999-93-ec/.

Note that further background information regarding the Directive and its history can be found within the text of the DTI Consultation – see later in this document for a reproduction.

Document Structure

This document is divided into the following chapters and sections:

- **Document Overview & Background** – details of the document's structure, intended audience, background information, etc.
- **Directed Comments: Consultation Questions** – addresses the questions explicitly posed in the DTI's Consultation Document in sequence; each response is formatted as a section unto itself.
- **General Comments: EC Directive** – general comments on EC Directive 1999/93, most simply providing clarification (or documenting the Author's understanding) of some of the more esoteric topics, and others raising potential issues in the Directive itself.
- **General Comments: DTI Consultation** – the Author's thoughts on the DTI Consultation document, and covers aspects not directly addressed by the *Directed Comments* chapter.
- ***Reference Chapters*** – plain-text reproductions of the EC Directive and DTI Consultation documents, provided in case access to the originals is unavailable while reading this document. These chapters also serve to provide an accurate context for this document.

***Note**: the Author's expertise in the field of European Law is limited, and therefore an assumption has been made: that implementation of EC Directives, once adopted by the Parliament and Council, is non-negotiable by Member States. As such, it is summarily assumed that the only flexibility in implementation is as explicitly set out within the Directive itself. If these assumptions are incorrect, the minutiae in this Response may be inaccurate, but the general opinions and concepts will still hold.*

Author: Peter SJF Bance MBCS CEng

Audience & Confidentiality

The primary audience for this document is the Department of Trade and Industry. This document has been created, however, with further propagation in mind, a possibility explicitly mentioned in the Consultation Document. For this reason, all content herein should be considered Public Domain and can be freely distributed. Please note, however, that proper acknowledgement must be included in any further distribution, as the content and presentation are also proprietary and protected by Copyright.

As requested, this document is being submitted to:

> Geoff Smith, Department of Trade and Industry: elecsigsconsultation@dti.gov.uk

and additionally copied for reference to:

> Managing Director, Rhye Internet Solutions Limited: directors@rhye.co.uk
> Thawte (Web of Trust – see below): weboftrust@thawte.com
> Web of Trust Notaries Community: thawtewot@listbot.com

Rhye Internet Solutions Limited

Rhye Internet Solutions Limited (Registered in England Number 3411130), a private company with broad and deep experience in the IT field, provides Internet, intranet and extranet consultancy services to large clients in both the Public and Private sectors. Past and present customers include:

- COI Communications (HM Government Agency)
- Johnson Matthey
- BZW
- Glaxo Wellcome (now part of Glaxo SmithKline)

The Company's primary specialisation since mid-2000 is network security, particularly relating to Internet-facing systems services. For further information or a more detailed portfolio, please feel free to contact us:

- **Web Site**: http://www.rhye.co.uk/
- **E-mail**: enquiries@rhye.co.uk
- **Postal Mail**: PO Box 646, Tring, HP23 5FB

The Author

Peter SJF Bance MBCS CEng is the Technical Director of Rhye Internet Solutions Limited. His 10 years' experience in IT (particularly in the field of network security) qualifies him to provide an expert Response to the DTI Consultation under discussion. Relevant qualifications and outside interests in the context of this Response include:

- First-class Bachelor of Science with Honours in Computer Science
- BrainBench – Certification in Internet Security (Master level)
- BCS – Professional Member and Certified Information Systems Practitioner

- Engineering Council – Chartered Engineer (CEng)
- Authorised Notary for the Thawte Web of Trust (see next section)

For further information or a detailed Curriculum Vita, please feel free to contact Peter:

- **Web Site**: http://www.minstrel.org.uk/
- **E-mail**: Minstrel@minstrel.org.uk or peter.bance@rhye.co.uk
- **Postal Mail**: c/o Rhye Internet Solutions Limited (see above)
- **Telephone/Facsimile**: 07092 082 939

Please note that contact is preferred via e-mail.

The Thawte Web of Trust

As mentioned above, the Author is a Notary within the Thawte Web of Trust scheme. Full detail of the scheme, its aims and its workings can be found at http://www.minstrel.org.uk/thawte.html and in pages linked to from there.

In essence, the Web of Trust (WoT) is an identity assertion mechanism that allows Thawte (a South African Certificate Provider, now part of VeriSign) to issue qualified personal certificates to users worldwide in the knowledge that their identity has been verified by at least three independent parties.

Since the scheme is extremely pertinent to this EC Directive, certain aspects of this document have been written with the WoT in mind – in particular, its relevance to the Directive is highlighted in the *General Comments* chapters.

Revision History

13 June 2001 – version 1.0 prepared for submission to Department of Trade and Industry.

No further changes to this response are anticipated unless additional clarification is requested.

Directed Comments: Consultation Questions

Question 1 – Supervisory Regime

QUESTION 1: Do you agree that the implementation of a supervisory regime should be based on a de minimis approach and subject to review in two years' time?

This proposed approach would certainly be the quickest to implement in the United Kingdom, would involve the least amount of effort, and would have the added advantage of allowing free and gradual growth of CSP services to take place. As suggested in the consultation document, the supervisory responsibilities of the DTI and tScheme should be minimal, and mainly oriented toward the provision of information.

The fundamental security principle at play here is that the primary responsibility for determining whether to trust a person, agency or company lies with the *trusting* party. By definition, trust cannot be imparted without full knowledge of the trusted party, the implications of trusting them, and the mechanisms/systems used to signify that trust.

This means that the onus must be on the industry itself to:

- Acquaint themselves with the concepts of digital signatures
- Become aware (at least at the conceptual level) of the mechanisms used to signify and grant trust
- Ensure they have obtained sufficient information to impart trust – simply trusting a third party because Internet Explorer says everything is fine is *not* acceptable

Historically, such trust mechanisms have worked well using a hierarchical (or chaining) approach – Network Solutions' PGP, the Thawte Web of Trust and X.509's inherent chaining functionality are good examples. A typical chain could be described along the lines of:

> **Citizen A** trusts **Citizen B** (they know each other well)
> **Citizen B** trusts **Agency X** (s/he is an employee)
> **Agency X** trusts **Company Y** (e.g. open customer-supplier relationship)
> **Company Y** trusts **Company Z** (e.g. industry partners)
> Therefore, **Citizen A** trusts **Company Z**

Hence, it follows that if tScheme (or any other 'supervisory' agency) presents itself as being qualified to *recommend* CSPs to be trusted, then they (tScheme et al) *must* provide sufficient information about themselves (members, qualifications, processes, etc.) to allow the industry to trust *them*. Alternatively, if the DTI states that tScheme is a trusted supplier, then the DTI itself must be proven trustworthy, through provision of similar information.

***Note**: in this context, a discussion of Digital Signatures, the word 'trust' has a far more important (even legal) meaning than its use in the vernacular.*

Author: Peter SJF Bance MBCS CEng

Question 2 – Designated Body

QUESTION 2: Do you believe that the UK should have a designated body and if so who should it be and how should they assess compliance with Annex III of the Directive?

There should certainly be a 'designated body' of some form that will be responsible for the assessment of Secure Signature Creation Devices against the criteria set out in Annex III of the Directive. However, it is not the Author's belief that this should be a UK-specific organisation. Indeed, it is debatable whether any Member State in the EC or even the Council itself could or should appoint such a body.

If a UK-specific 'designated body' *is* appointed, however, there are a number of factors to be considered:

- Academic, non-profit and even commercial organisations already exist in the UK, Europe and overseas that are extensively involved in this kind of work – it is important to avoid a huge replication of effort if the output of said organisations could be reused.
- The United Kingdom is not leading this field – indeed, the Author's personal experience indicates that very few of the world's cryptographic experts are even European. Therefore, it is critical that international input is accepted in any assessment or judgement of CSPs and/or cryptographic devices.
- To ensure that administrative, governmental and commercial politics do not affect the working of such a critical organisation, a 'designated body' should be:
    - Independent (i.e. not restricted, limited or controlled by any third party)
    - Non-proprietary (i.e. not managed by any vendor)
    - Non-commercial (i.e. non-profit)
    - Qualified (i.e. including members with expertise in the field of cryptography)
- The consultation document mentions CESG as an obvious 'designated body' in the UK. In the Author's opinion, however, this would not be a good choice – aside from the immediate concern that CESG is an agency of Government (and perhaps, therefore, would be seen as biased), the agency is not known as a major player in the security industry; their qualifications would have to be better publicised than they are at present.

Given the above points, the tScheme organisation appears to fulfil many of the criteria. Although its current membership includes many commercial organisations, their goals and principles are reasonably clear – the organisation itself should still be able to act in an independent manner, although this may need to be the subject of regular review. The group's adherence to industry standards should provide a sound platform for any recommendations it makes.

Although assessment of devices against the Annex III guidelines is not currently part of tScheme's remit, it would not be too onerous a task to extend it thus. In the Author's opinion, however, an extension of this kind should coincide with an extension of tScheme's membership – there needs to be at least a small contingent of leading cryptographic experts included in any assessment team; if such experts *are* already involved via one of the commercial tScheme members, those experts should be individually named to provide further reassurance.

Author: Peter SJF Bance MBCS CEng

It is important to state that the EC Directive is quite clear on the subject of discrimination – it must be ensured that (other than in the Public Sector, which has been granted a freer rein) no CSP, potential CSP or device is discriminated against in the market if it does not possess a 'tScheme Mark'. CSPs and device publishers may not wish to be assessed by the group, but should still be allowed to compete fairly – see my response to Question 4 for further discussion on this topic.

As for how compliance should be assessed, one fundamental mitigating factor must be considered – the *only* way an encryption algorithm and its implementation can be considered secure is if the source code is disclosed and reviewed by the Internet Security community at large. It is not enough for a supplier simply to state that a particular industry-standard encryption algorithm has been used, as the specific *implementation* of that algorithm can be subject to security flaws. Indeed, this problem *has* occurred in commercial applications in the past.

Similarly, it is also unsatisfactory for an Annex III compliance judgement to be based purely on sample data – however many thousands of 'good' examples are reviewed, there will always be the potential for one 'bad' example to occur in the future – this potential renders a Secure Signature Creation Device useless. Again, the only way to protect against this is for expert and independent cryptographic analysis to take place on the source code, whether the device is software- or hardware-based.

There is also the possibility that a back door of some kind could be intentionally or accidentally embedded within a Secure Signature Creation Device. Without an Open Source policy in the device's development, no analyst could possibly make a safe judgement. Again, there have been real examples of this occurring in commercial applications.

Question 3 – Article 3.5

QUESTION 3: What do you believe will be the impact of Article 3.5 and is there any further action the Government could take?

Article 3.5, urging Member States to 'trust' the recommendations of an 'Electronic-Signature Committee' (discussed in Article 9), is a potential cause for concern. Given the information presented in response to the previous two questions, it would be inadvisable for such recommendations to be accepted without full background information, either through publication of the assessment process and results, or by full disclosure of the Committee's qualifications and membership. A simple statement along the lines of 'this product complies to such-and-such a standard' is not sufficient in this context.

A few actions could be taken by the Government to ease concerns on this matter:

- If a 'designated body' (see previous response) exists, representatives from that body should be part of the 'Electronic-Signature Committee', and thus be privy to sufficient information to accept or reject, on behalf of the body, recommendations made by the Committee.
- Failing this, and again given the existence of a 'designated body', any recommendations from the 'Electronic-Signature Committee' should be subject to full review, even audit, but the body before the recommendation is passed to industry.

Author: Peter SJF Bance MBCS CEng

- In the last resort, especially if a 'designated body' is not appointed, the Government should obtain and publish full background information on the recommendations put forward by the 'Electronic-Signature Committee', so that industry itself can choose whether or not to accept such recommendations.

Question 4 – Article 3.7

QUESTION 4: Do you agree with our analysis of the meaning of Article 3.7 and the proposed course of action to ensure compliance with it?

The e-Envoy reference URL mentioned in the Consultation Document (www.e-envoy.gov.uk/frameworks/authentication/contents.htm) produces an error (404 – File Not Found), and so the Author does not feel qualified to prepare a complete response to this question. However, it should be pointed out that online Government services are already digressing from this Article, and so the issue should be addressed quickly before further non-compliance occurs.

The specific example that has come to the Author's attention is the Online VAT Return submission facility provided by Customs and Excise (and presented as part of the 'Government Gateway' initiative). This facility *requires* a certificate to be obtained from *ChamberSign* or *EquiFax* (both of which are actually reselling Thawte certificates); it further requires specific vendor components on client machines and even particular Operating Systems to be used – this conflicts **directly** with Article 3.7, which states:

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

Such insistence on certificates from a particular CSP (especially one in which there is currently a lack of confidence in the industry) or systems/software from particular vendors cannot be justified in the context of this Article.

It should also be noted that Article 3.7 permits additional requirements to be demanded of certificates *only* in the Public Sector. Care needs to be taken that this is not inadvertently or deliberately extended to the Private Sector by any 'designated body'.

Question 5 – Article 5.1(a)

QUESTION 5: Do you agree with the proposed regulation to implement Article 5.1(a)?

Article 5.1(a) should certainly be implemented in law. A related point, although this is almost certainly outside the scope of this Directive, is that the Author would very much like to see a more general change in legal requirements as to the form of legal documentation. In this electronic age, and given the strength of today's signing devices, there are many instances where a digital signature should be accepted as an alternative to 'writing and signature'. However, this is likely to be a matter for the legal profession and Justice system rather than Government legislation.

Author: Peter SJF Bance MBCS CEng

Question 6 – Article 6

QUESTION 6: Do you have any comments on the proposal to implement Article 6 and that this should be achieved by regulations under the European Communities Act?

No further comment – the DTI's analysis of Article 6 is consistent with that of the Author, and Article 6 implementation should proceed by whatever means is most appropriate.

Question 7 – Article 8.2

QUESTION 7: Do you agree with the proposal to implement Article 8.2 and thereby place specific data protection requirements on certification service providers?

The requirements set out in Article 8.2 should certainly be implemented as an extension to the Data Protection Act. Furthermore, it is the Author's belief that the measures described in this Article should be applied to *all* treatment of citizens' personal data, and not limited to the actions of Certificate Service Providers. The Data Protection Act is not currently strict enough to protect the individual; from recent conversations the Author has had, it is a common belief that these requirements are *already* incorporated in the Data Protection Act.

Question 8 – Impact of Directive in UK

QUESTION 8: Do you have any views on the likely impact of the Directive in the UK and how it may assist in promoting trusted and secure electronic transactions?

In general, implementation of this Directive will be transparent to the majority of industry, given the 'light touch' approach being taken by the Government. Indeed, this is as it should be. The greatest impact is likely to be on the Government itself, particularly in the implementation of Article 3.7 (see the response to Question 4, above).

In the Author's experience, a great many citizens *already* possess qualified certificates that fulfil the requirements set out in Annex I, as the S/MIME mail-encryption standard is popular as a means to protect and sign private and commercial communications. Implementation of this Directive will mean that many existing certificate holders will be able to take advantage of electronic services without further expense or inconvenience. On a related note, many commercial organisations are already investigating, implementing and using PKI systems from leading International vendors; once the Directive is implemented, the usefulness of these PKI implementations will be greatly extended.

As one might expect, the Directive will be of particular importance in the IT industry, where protection and verification of data is frequently a fundamental requirement. Electronic signing and encryption are fundamental to many online services.

As suggested in the Consultation Document, the profile and usefulness of advanced digital signatures will be greatly increased by their use for authentication to G2B or G2C services, especially when electronic voting is available, but this can only take place once the problems highlighted in the response to Question 4 above are urgently addressed.

Author: Peter SJF Bance MBCS CEng

General Comments: EC Directive

This chapter presents the Author's thoughts and opinions on the content of EC Directive 1999/93/EC. As mentioned in the Document Overview, the assumption is made that Member States are not able to make amendments to the Directive itself, so this chapter is provided only for reference and clarification.

The chapter is divided into sections for ease of reading, each addressing a particular Article, Annex or other section within the Directive.

General

One major concern the Author has about the EC Directive as a whole is that, although it appears to encourage the use of many different technologies, it appears to have been written almost specifically to recommend the X.509 standard (see the comments on Article 6 below).

There are several other popular standards and technologies in use in industry, not least of which is PGP (and particularly OpenPGP). PGP actually has a number of advantages over current implementations of X.509:

- Encryption and signing key strengths are typically higher than existing X.509-enabling devices.
- It is more flexible, as it can be used to sign or encrypt any data, whereas X.509 implementations are generally limited to e-mail and HTTP protocols.

There are other advantages to OpenPGP – its creator, Phil Zimmermann, has written a succinct and powerful article on this very topic – it can be read at:

http://openpgp.org/technical/whybetter.shtml

In this article, Phil describes OpenPGP's trust model as a 'proper superset of the centralized trust model we most often see in the X.509 world', and suggests (as the Author has elsewhere in this document) that the mechanics of trust are the primary responsibility of individual end-users or entities.

The Author has used PGP for many years, and found it to be far more useful than X.509-related technologies (e.g. S/MIME, SSL, etc.) – S/MIME in particular is unusable if you are unwilling (or unable) to run specific proprietary software on a particular machine.

Unfortunately, with the EC Directive in mind, PGP is likely to be excluded from use as a digital signature enabler in e-Commerce, as the majority of the requirements and recommendations in the Directive simply do not apply. This is a shame, and the Author would have liked to see allowance for technologies that do not work according to the same model as X.509.

Opening Paragraph

As mentioned in this document's *Overview*, the Author has an interest in Thawte's Web of Trust scheme. Item (11) appears to be directly relevant to this scheme:

> "(11) Voluntary accreditation 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 accreditation schemes"

The Web of Trust is a 'voluntary accreditation scheme' in this context, and provides Thawte in particular with the confidence to issue qualified certificates to individuals in the knowledge that identities have been verified.

Item (13) is extremely important, particularly with respect to discussions regarding a 'designated body':

> "(13) Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme"

Unfortunately, this Item could be open to several interpretations. In the Author's view, it leaves Member States free to decide on their own supervisory regimes *as long as* they do not impose limits on CSPs by insistence on accreditation.

In Item (23):

> "(23) The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial"

the phrase "could be beneficial" is surprisingly non-committal. The Author is certain that mutual recognition of certification services across internal and external borders *would* be extremely beneficial to all concerned.

Item (27) discusses review of the Directive:

> "(27) Two years after its implementation the Commission will carry out a review of this Directive so as, inter alia, to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in this Directive; it should examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject"

Author: Peter SJF Bance MBCS CEng

In this industry, two years is a very long time – it is often said that one year in IT is equivalent to 5 years in other industries! Although the Commission will not review the Directive for two years, the Author feels it is important that the UK implementation of the Directive is reviewed far sooner.

Article 3

3.3 again discusses supervision:

> "3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public."

It is unclear from this exactly what supervision the Directive suggests or allows, although it does appear to apply *only* to CSPs registered in a particular Member State. Placing this in the context of other Articles and the Opening Paragraph, the Author would conclude that this Article allows only for a 'light-touch' supervisory regime to be adopted by Member States, much as the DTI is recommending.

Article 4

4.2, which discusses the circulation of electronic-signature products, has the potential for great impact:

> "2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market."

Legislation already in place in several Member States will need to be amended to allow this to take place. Historically, export of high-encryption products has been a complex matter – whilst this has been most evident in US Export regulations, it is certain to be an issue internally to the EC as well. It remains to be seen exactly which products will become most popular in the context of the Directive, but hopefully they will be Open Source and based on industry standards, and so the issue may not arise.

Article 5

5.2 discusses the legal effects of electronic signatures:

> "2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
> - in electronic form, or
> - not based upon a qualified certificate, or
> - not based upon a qualified certificate issued by an accredited certification-service-provider, or
> - not created by a secure signature-creation device."

The Author is not a member of the legal profession, but the wording of this clause appears vague; it could be open to abuse or subject to multiple interpretations in court. If this is the case after proper legal analysis, this should be clarified in the UK implementation of the Directive.

Author: Peter SJF Bance MBCS CEng

Article 6

6.3, a fundamental clause in the Directive, discusses limitation of the usage of qualified certificates:

> "3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate. provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it."

Similarly, 6.4 extends this premise to financial limitation:

> "4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties."

From a technical standpoint, these requirements may limit the available technologies. Currently, it would seem that only X.509 certificates can support the 'extensions' required to support these clauses and similar requirements laid out in Annex I. There are a number of other electronic-signature products in existence (and common use) that would be explicitly excluded from commercial use by these requirements. Whilst inclusion in a certificate of actual limitation data is not required, the *ability* to include it is.

Article 7

Article 7 discusses the international aspects of the Directive:

> "1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:
> (a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or
> (b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or
> (c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.
> 2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council shall decide by qualified majority.

Author: Peter SJF Bance MBCS CEng

> 3. Whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority.
> Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements."

This Article as a whole is a cause for concern, but in particular 7.1. It implies that for CSPs in third countries to be able to issue qualified certificates to citizens in Member States, they *must* subject themselves to accreditation of some kind. In the Author's view, this conflicts with the overall spirit of the Directive – it introduces prejudice against CSPs not established within Member States. Indeed, many of the world's leading CSPs (or Certification Authorities, CAs, as they are more commonly known) are *not* established in Member States: for example, Thawte are based in South Africa, and VeriSign are based in the US.

Article 8

Clause 8.3 discusses the use of pseudonyms in qualified certificates:

> "3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name."

It is unclear to the Author whether CSPs would be required to retain information relating to an individual's *real* identity when a pseudonym is used in a certificate. If they are not, such certificates could almost certainly not be used for important electronic transactions; they should be limited to enabling e-mail encryption and signing only.

It may be that this is already covered by 'national law' as mentioned in the Clause.

Article 9

Clause 9.1 mentions the instigation of an Electronic-Signature Committee:

> "1. The Commission shall be assisted by an "Electronic-Signature Committee", hereinafter referred to as "the committee"."

As discussed earlier in this document, it is important that the membership and qualifications of this Committee are published to Member States, as crucial decisions and recommendations could be made by, or on the advice of, this Committee. Indeed, it would also be advantageous if at least one member of any UK-appointed 'designated body' were part of this Committee.

Article 11

Article 11 discusses information that should be relayed to the Commission and other Member States:

Author: Peter SJF Bance MBCS CEng

> "1. Member States shall notify to the Commission and the other Member States the following:
> (a) information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);
> (b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);
> (c) the names and addresses of all accredited national certification service providers.
> 2. Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible."

11.1(a) is directly relevant to the Thawte Web of Trust discussed earlier – however, it is unclear whether the Commission and Member States should be informed of the scheme. Thawte are based in South Africa, and hence would not be classed as a 'national voluntary scheme', although there are a great many Web of Trust members in this country.

In the Author's opinion, it would serve the EC well if they *were* notified of the Web of Trust and the benefits it presents. It should be borne in mind that *all* CSPs currently used by the Government Gateway issue certificates in the name of Thawte, and official recognition of the Web of Trust could simplify the processes even further.

11.1(b), in its use of the phrase '… of **the** national bodies …' implies that it is expected that accreditation and supervisory bodies will be appointed. This is in direct conflict with earlier Articles. A similar issue exists with the reference to Article 3.4.

11.1(c) – again, it is unclear whether the names and addresses of CSPs from third countries, but *operating* in the UK (e.g. VeriSign, Thawte, etc.), should be passed to the Commission and other Member States.

ANNEX I – Requirements for Certificates

As discussed earlier in this document, requirements (i) and (j) may have the direct effect of limiting the technologies that will comply:

> "(i) limitations on the scope of use of the certificate, if applicable; and
> (j) limits on the value of transactions for which the certificate can be used, if applicable."

The words 'if applicable' used here imply that it is not *required* for that data to be contained within a qualified certificate if is not relevant to the transaction or other activity being undertaken. With this in mind, the Author would have preferred these requirements to be presented separately – their inclusion in this list of requirements, which is prefaced with "**must** contain", is not ideal – far greater flexibility would have been achieved if text akin to the following had been used:

> "Qualified certificates *must* contain:
> (a) an indication that the certificate is issued as a qualified certificate;

> ...
> (h) the advanced electronic signature of the certification-service-provider issuing it.
>
> In addition, if applicable, the certificate *may* contain:
> (i) limitations on the scope of use of the certificate; and
> (j) limits on the value of transactions for which the certificate can be used.

ANNEX II – Requirements for CSPs

Again prefaced by the word "must", this Annex raises several important questions:

> "(e) ... administrative and management procedures which are adequate and correspond to recognised standards;"

It is unclear here which 'recognised standards' the administrative and management procedures must correspond to. Whilst the Author is not fully versed in such procedures, there are almost certainly different standard procedures recognised at the national, European, global and even academic levels. Clarification should be made, perhaps in a summary of assumptions in the UK implementation of the Directive.

Item (j) is related to the controversial topic of 'key escrow':

> "(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;"

This explicitly rules out the possibility of a CSP storing private keys, which is as it should be. However, and given certain existing legislation, the Author would like to see this provision extended to encompass private keys used for decryption as well. Whilst in many applications the two are the same, and so no issue exists, there are a few (and perhaps more in the future) where different certificates are used for encryption/decryption and signing/verification. In these instances, private key escrow is unacceptable, as it undermines the usefulness of encryption.

A later requirement is extremely unclear in many ways:

> "(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in redily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;"

[The Author has read *readily* for *redily*]

1. Unless it is a legal term, the phrase 'durable means of communication' is extremely vague. The Author presumes that paper is meant, although realistically many forms of digital storage are actually more durable than paper.
2. '… may be transmitted electronically, must be in writing …' this strikes the Author as a strange phrase – if the definition of 'writing' in this context is, again, on paper, then electronic transmission would not be relevant. If it does not refer to paper, then it is unclear why the requirement is stated at all.
3. '… re[a]dily understandable language.' – the language that will be best understood by any individual is dependent on their existing knowledge. CSPs may find it difficult to provide the right level of information in the right terms for everyone.

The final requirement in Annex II raises further questions:

> "(l) use trustworthy systems to store certificates in a verifiable form so that:
> – only authorised persons can make entries and changes,
> – information can be checked for authenticity,
> – certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
> – any technical changes compromising these security requirements are apparent to the operator."

There is an implication of CSP audit here – who will be responsible for determining whether Annex II requirements are met? Since privacy and propriety issues are undoubtedly involved when looking at CSPs' internal systems, is it sufficient for that CSP to provide a statement of compliance? It should also be noted that **no** system can be classed as 100% secure, and it is almost impossible to implement a system where *all* changes are notified to the operator. Again, perhaps this Clause should have been separated from those prefaced by "must" and terms like "to the best of the CSP's ability" or "to industry security standards" used instead.

Annex III – Requirements for Secure Signature-Creation Devices

One key question regarding this entire Annex is how compliance will be assessed should there be no 'designated body'. Again, will a compliance statement from the CSP be sufficient, or should products be Open Source?

1(c) raises an ever-present security problem:

> "(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others."

It is extremely difficult to persuade all users that their signature-creation-data (more commonly referred to as a 'private key') is critical, and should be protected at all times. Where such data is protected with a password, strong passwords are rarely used, and in any case are frequently written in obvious places near users' machines. Taking this requirement literally, this should not be a problem, as long as the signature-creation-data *can* be protected, but it should not be assumed that this would always be the case.

The precise meaning of the final Annex III requirement is unclear:

> "2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process."

On the face of it, this appears a sensible statement – signed data should obviously not be altered. However, depending on the technology in use (S/MIME, PGP, etc.) it is frequently the case that data being signed **is** altered during the signing process itself. For example, PGP alters certain characters in the first column of signed data when they are encountered; additionally, almost all signature-creation devices are capable of 'opaque-signing', where the signed data cannot easily be read until verification is performed.

The signed data is always returned to its original form when the signature is *verified*, however. The requirement would have been better (and more clearly) written as:

> "2. Where a secure signature-creation device alters data to be signed during the signing process, it must return it to the original form on signature verification..."

The second part of the requirement appears superfluous – prior to the signing process, data will be in its original form anyway, and so it is outside the scope of any signature-creation device.

Annex IV – Recommendations for Secure Signature Verification

It is interesting that the signature verification process is not subject to requirements under this Directive, and only recommendations are made. In the Author's experience, secure-signature creation and verification devices are fundamentally linked, and in most cases form part of the same software application. Without an appropriate verification process, signing data at all is pointless.

Once again, there is the question of how Annex IV compliance should be assessed, although in this case it is a recommendation only, and so compliance is not strictly necessary. The Author believes, however, that most of Annex IV should be at least *viewed* as requirements, and assessed at the same time as Annex III compliance.

There are two recommendations in this Annex that raise questions:

> "(a) the data used for verifying the signature correspond to the data displayed to the verifier;"

It is unclear which data is being referred to here – the 'data used for verifying the signature' would be a combination of the signature itself and the original data that was signed, which the verifier would obviously have access to anyway. It is difficult to conceive of a system where signed data is not presented to the verifier before verification takes place.

> "(g) any security-relevant changes can be detected."

In the Author's opinion, this recommendation should not be qualified with the term 'security-relevant'. In order for a secure signature creation and verification process to be reliable and useful, **any** changes to the original data should be highlighted on verification. Even trivial changes such as the addition of a carriage-return in the data should be pointed out to the verifier. In most cases, given the cryptographic algorithms in question, it will only be possible to report that *something* has been changed, in which case point (g) is moot anyway.

General Comments: DTI Consultation

This section presents general comments, opinions and observations relating to the DTI Consultation Document itself. Once again, for ease of reading, it is divided into sections that approximately correspond to the structure of the Consultation Document.

General

It is surprising that such a short consultation period has been provided – the EC Directive was adopted at the end of 1999, and yet the Consultation did not start until March 2001, with a deadline of mid-June. Three months is a very short time considering the scope of the Directive's implications.

Item 6

> "6 Member States cannot make the provision of certification services subject to 'prior authorisation' (Article 3, paragraph 1). The Government will not do so."

It is possible that this has already taken place, and a great deal of work may be necessary to reverse the situation. See discussion earlier in this document regarding the 'Government Gateway.

Item 9

> "... In effect, this establishes a benchmark for the content of certificate – drawing on the widely-used x509 standard for digital certificates – and the performance of the supplier in terms of competence, viability and integrity."

This clearly states that the UK implementation of the EC Directive will be based around the X.509 standard. See the Author's earlier comments regarding alternatives.

Item 15

> "15 In a high risk scenario, it is possible to envisage a much more active supervisory regime..."

The precise definition of a 'high-risk scenario' should be clarified, lest unnecessary supervisory activity takes place which conflicts with the spirit of the Directive.

Item 18

> "18 The classical 'regulatory' skillsets are available in many parts of Government. For the more rigorous approach to supervision, the most obvious candidate to undertake this role would be OFTEL (noting the proposal to merge this organisation into a more broadly-based OFCOM). The need to challenge CSPs on elements of the Directive which are based

Author: Peter SJF Bance MBCS CEng

> on cryptographic technologies would probably require the import of specialist skills. These are available commercially but it might be more credible if this specialist function were performed by the Communications and Electronic Security Group – the Government's technical authority on information technology security."

As noted, any supervisory activity by OFTEL/OFCOM would require specialist skills to be available which are unlikely to be part of the body's portfolio at the moment. The suggestion that CESG would have more credibility in such a supervisory capacity is, from the Author's experience, inaccurate. Within the Public Sector, this may be the case, but taking the industry as a whole, it is not. Additionally, CESG are unlikely to be viewed as sufficiently independent (see earlier in this document).

Item 21

> "21 At this stage, given the uncertainty of the market, the Government propose to provide by regulation the de minimis option outlined above..."

The *de minimis* approach is certainly the most appropriate when considering implementation of this Directive. However, the reason for this is not 'uncertainty of the market' – the potential uses of electronic signatures and their positive impact on industry is perfectly clear.

Item 43

> "43 The Directive requires that Member States treat qualified certificates originating from non-EU service providers as legally equivalent to EU certificates if they meet one of three criteria. These are that they are accredited by a an accreditation scheme in a Member State, their certificate is guaranteed by a service provider from a Member State or the service provider is in a country which is subject to a bilateral or multilateral agreement."

A point of principle in relation to this – it is the Author's belief that the trust mechanisms implemented as part of this Directive should be beyond international administrative politics. For example, if a country is subject to economic sanctions, the Author sees no reason why certificates and signatures originating from that country should be affected in any way. The reliability and credibility of trust hierarchies should be based on process and technology alone.

Item 47

> "Articles 9-15
>
> 47 These articles concern the management of the implementation of the Directive."

This is true, but they should still not be ignored completely by the consultation. In particular, see the earlier points in this document regarding the appointment of an 'Electronic-Signature Committee' – this will have a fundamental impact on the Directive's implementation in Member

Author: Peter SJF Bance MBCS CEng

States. Note also that Article 11.1(b) appears to conflict with other sections of the Directive, insisting by implication on accreditation and supervisory bodies – see earlier in this document.

Author: Peter SJF Bance MBCS CEng

Reference: EC Directive 1999/93/EC, Full Text

Extracted from original EC Directive document located at http://europa.eu.int/comm/internal_market/en/media/sign/Dir99-93-ecEN.pdf – white space added by Author for readability.

DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 13 December 1999
on a Community framework for electronic signatures

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,
Having regard to the proposal from the Commission(1),
Having regard to the opinion of the Economic and Social Committee(2),
Having regard to the opinion of the Committee of the Regions(3),
Acting in accordance with the procedure laid down in Article 251 of the Treaty(4),

Whereas:

(1) On 16 April 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on a European Initiative in Electronic Commerce;

(2) On 8 October 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on ensuring security and trust in electronic communication – towards a European framework for digital signatures and encryption;

(3) On 1 December 1997 the Council invited the Commission to submit as soon as possible a proposal for a Directive of the European Parliament and of the Council on digital signatures;

(4) Electronic communication and commerce necessitate " electronic signatures" and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation 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 regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market;

(5) The interoperability of electronic-signature products should be promoted; in accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured; essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods(5) and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods(6);

Author: Peter SJF Bance MBCS CEng

(6) This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;

(7) The internal market ensures the free movement of persons, as a result of which citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; the availability of electronic communication could be of great service in this respect;

(8) Rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically;

(9) Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures;

(10) The internal market enables certification-service-providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers; in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorisation; prior authorisation means not only any permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect;

(11) Voluntary accreditation 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 accreditation schemes;

(12) Certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law; whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services;

(13) Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme;

(14) It is important to strike a balance between consumer and business needs;

Author: Peter SJF Bance MBCS CEng

(15) Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient;

(16) This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised;

(17) This Directive does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures; for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;

(18) The storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures;

(19) Electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in the public procurement, taxation, social security, health and justice systems;

(20) Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of hand-written signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to hand-written signatures only if the requirements for hand-written signatures are fulfilled;

(21) In order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved; national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence;

Author: Peter SJF Bance MBCS CEng

(22) Certification-service-providers providing certification-services to the public are subject to national rules regarding liability;

(23) The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial;

(24) In order to increase user confidence in electronic communication and electronic commerce, certification-service-providers must observe data protection legislation and individual privacy;

(25) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law;

(26) The measures necessary for the implementation of this Directive are to be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission(7);

(27) Two years after its implementation the Commission will carry out a review of this Directive so as, inter alia, to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in this Directive; it should examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject;

(28) In accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty, the objective of creating a harmonised legal framework for the provision of electronic signatures and related services cannot be sufficiently achieved by the Member States and can therefore be better achieved by the Community; this Directive does not go beyond what is necessary to achieve that objective,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Scope

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.

It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

Article 2

Definitions

For the purpose of this Directive:

1. "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. "advanced electronic signature" means an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

3. "signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;

4. "signature-creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

5. "signature-creation device" means configured software or hardware used to implement the signature-creation data;

6. "secure-signature-creation device" means a signature-creation device which meets the requirements laid down in Annex III;

7. "signature-verification-data" means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;

8. "signature-verification device" means configured software or hardware used to implement the signature-verification-data;

9. "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;

10. "qualified certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;

11. "certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;

12. "electronic-signature product" means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;

13. "voluntary accreditation" means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is

Author: Peter SJF Bance MBCS CEng

not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

Article 3

Market access

1. Member States shall not make the provision of certification services subject to prior authorisation.

2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive.

3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.

4. The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated.

A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.

5. The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.

6. Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer.

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

Article 4

Internal market principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not

Author: Peter SJF Bance MBCS CEng

restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.

2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market.

Article 5

Legal effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
(b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature-creation device.

Article 6

Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:
(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;
unless the certification-service-provider proves that he has not acted negligently.

2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that

Author: Peter SJF Bance MBCS CEng

certificate. provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.

4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties.
The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.

5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts(8).

Article 7

International aspects

1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:
(a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or
(b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or
(c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council shall decide by qualified majority.

3. Whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority.

Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements.

Article 8

Data protection

1. Member States shall ensure that certification-service-providers and national bodies responsible for accreditation or supervision comply with the

requirements laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on tile protection of individuals with regard to the processing of personal data and on the free movement of such data(9).

2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

Article 9

Committee

1. The Commission shall be assisted by an "Electronic-Signature Committee", hereinafter referred to as "the committee".

2. Where reference is made to this paragraph, Articles 4 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof. The period laid down in Article 4(3) of Decision 1999/468/EC shall be set at three months.

3. The Committee shall adopt its own rules of procedure.

Article 10

Tasks of the committee

The committee shall clarify the requirements laid down in the Annexes of this Directive, the criteria referred to in Article 3(4) and the generally recognised standards for electronic signature products established and published pursuant to Article 3(5), in accordance with the procedure laid down in Article 9(2).

Article 11

Notification

1. Member States shall notify to the Commission and the other Member States the following:
(a) information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);
(b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);
(c) the names and addresses of all accredited national certification service providers.

2. Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible.

Article 12

Author: Peter SJF Bance MBCS CEng

Review

1. The Commission shall review the operation of this Directive and report thereon to the European Parliament and to the Council by 19 July 2003 at the latest.

2. The review shall inter alia assess whether the scope of this Directive should be modified, taking account of technological, market and legal developments. The report shall in particular include an assessment, on the basis of experience gained, of aspects of harmonisation. The report shall be accompanied, where appropriate, by legislative proposals.

Article 13

Implementation

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 19 July 2001. They shall forthwith inform the Commission thereof.
When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the main provisions of domestic law which they adopt in the field governed by this Directive.

Article 14

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities

Article 15

Addressees

This Directive is addressed to the Member States.

Done at Brussels, 13 December 1999.

For the European Parliament
The President
N. FONTAINE

For the Council
The President
S. HASSI

(1) OJ C 325, 23.10.1998, p. 5.
(2) OJ C 40, 15.2.1999, p. 29.
(3) OJ C 93, 6.4.1999, p. 33.
(4) Opinion of the European Parliament of 13 January 1999 (OJ C 104, 14.4.1999, p. 49), Council Common Position of 28 June 1999 (OJ C 243,

Author: Peter SJF Bance MBCS CEng

27.8.1999, p. 33) and Decision of the European Parliament of 27 October 1999 (not yet published in the Official Journal). Council Decision of 30 November 1999.
(5) OJ L 367, 31.12.1994, p. 1. Regulation as amended by Regulation (EC) No 837/95 (OJ L 90, 21.4.1995, p. 1).
(6) OJ L 367, 31.12.1994, p. 8. Decision as last amended by Decision 99/193/CFSP (OJ L 73, 19.3.1999, p. 1).
(7) OJ L 184, 17.7.1999, p. 23.
(8) OJ L 95, 21.4.1993, p. 29.
(9) OJ L 281, 23.11.1995, p. 31.

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:

(a) an indication that the certificate is issued as a qualified certificate;
(b) the identification of the certification-service-provider and the State in which it is established;
(c) the name of the signatory or a pseudonym, which shall be identified as such;
(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
(e) signature-verification data which correspond to signature-creation data under the control of the signatory;
(f) an indication of the beginning and end of the period of validity of the certificate;
(g) the identity code of the certificate;
(h) the advanced electronic signature of the certification-service-provider issuing it;
(i) limitations on the scope of use of the certificate, if applicable; and
(j) limits on the value of transactions for which the certificate can be used, if applicable.

ANNEX II

Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:

(a) demonstrate the reliability necessary for providing certification services;
(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature techology and familiarity with proper security procedures; they must also apply

Author: Peter SJF Bance MBCS CEng

administrative and management procedures which are adequate and correspond to recognised standards;
(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in redily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;
(l) use trustworthy systems to store certificates in a verifiable form so that:
- only authorised persons can make entries and changes,
- information can be checked for authenticity,
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

ANNEX III

Requirements for secure signature-creation devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
(a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
(b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

ANNEX IV

Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:

(a) the data used for verifying the signature correspond to the data displayed to the verifier;
(b) the signature is reliably verified and the result of that verification is correctly displayed;
(c) the verifier can, as necessary, reliably establish the contents of the signed data;
(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
(e) the result of verification and the signatory's identity are correctly displayed;
(f) the use of a pseudonym is clearly indicated; and
(g) any security-relevant changes can be detected.

End of document

Author: Peter SJF Bance MBCS CEng

Reference: DTI Consultation on EC Directive 1999/93/EC, Full Text

Extracted from original DTI Consultation document available at http://www.dti.gov.uk/cii/ecommerce/europeanpolicy/esigncondoc.pdf – white space added by Author for readability, and [footnotes] moved to bottom.

March 2001
Responses by 19 June 2001
Department of Trade and Industry

CONSULTATION ON EC DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND COUNCIL ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES

Department of Trade and Industry

Consultation Document on the implementation of the EU Electronic Signatures Directive.

Introduction

1 On 19 January 2000, Directive 1999/93/EC on a Community Framework for Electronic Signatures (commonly known as the Electronic Signatures Directive and referred to hereafter as "the Directive") was published in the Official Journal of the European Communities (OJ No,L13, 19.1.00, p12).

2 The background to the Directive was that from the early 1990s onwards legislation had been passed in several jurisdictions covering the use of on-line authentication techniques based on public key cryptography (digital signatures and the supporting digital certificates). The passing of such laws in Europe, in 1997 in Germany and Italy, opened up the prospect of a patchwork of incompatible laws governing the provision of electronic signature [1] services and the legal recognition of this key e-commerce enabling technology. The Commission proposed action to prevent this happening. The objective of the Directive was "to facilitate the use of electronic signatures and to contribute to their legal recognition" (Article 1 the Directive). At heart, it is concerned with promoting user trust and confidence in the process of authentication in the information age.

3 In short, the Directive works to promote the proper functioning of the internal market by ensuring that electronic signatures are not denied legal admissibility on various grounds and establishing benchmarks for the signature creation devices and certificates which are used to support such signatures. The Directive creates a framework whereby all parties can be assured that the benchmarks are met and thus that the provision of products or services in the single market is not constrained. It is not intended to affect the law relating to the conclusion and validity of contracts, requirements of form nor law governing the use of contracts.

4 This consultation paper has been produced to seek views on the implementation of both the obligations on Member States and also those areas where Member States have discretion whether to act. The Directive has to be implemented by 19 July 2001. As explained below, the Electronic Communications Act of 2000 implemented some of the key requirements of the Directive and there was extensive consultation on that legislation.

Author: Peter SJF Bance MBCS CEng

5 The consultation paper follows the format of the Directive in respect to the key requirements. The full text of the Directive is annexed to this paper as Annex A. Defined terms are in italics.

Article 3 Market Access

Prior authorisation

6 Member States cannot make the provision of certification services subject to "prior authorisation" (Article 3, paragraph 1). The Government will not do so.

Voluntary accreditation schemes

7 Member States may introduce or maintain voluntary accreditation [2] schemes aiming at "enhanced levels of certification service provision". These schemes must have objective, transparent, proportionate and non-discriminatory conditions and cannot limit the number of accreditations for "reasons which fall within the scope of this Directive".

8 The Government took powers under Part I of the Electronic Communications Act 2000 (the ECA) to establish a statutory voluntary approvals regime. The tScheme has been established by the Alliance for Electronic Business [3] (a consortium of industry bodies concerned with the promotion of electronic business) in response to and as alternative to the Government implementing the powers taken under Part 1 of the ECA. The tScheme therefore exists as a non-statutory voluntary approvals regime for trust service providers (which would include the service providers covered by the Directive). Government is working in partnership with the tScheme but it is clearly private sector-led. The Government has no plans therefore at present to introduce a voluntary accreditation scheme and notes that the conduct of the tScheme appears to fulfil the broad objectives for schemes which might be introduced by Member States in accordance with the Directive.

Supervision

9 Member States must ensure "the establishment of an appropriate system that allows for supervision of certification service providers which are established on its territory and issue qualified certificates to the public". "Qualified certificate" means a certificate which meets the requirements of Annex 1 and is provided by a service provider who meets the terms of Annex II. In effect, this establishes a benchmark for the content of certificate – drawing on the widely-used x509 standard for digital certificates – and the performance of the supplier in terms of competence, viability and integrity.

10 "Supervision" is not a defined term in the Directive and the preamble does not clarify its meaning to any great extent. The preamble (recital 13) says that private sector supervisory systems are not excluded but that providers are not obliged to apply to be supervised "under any applicable accreditation scheme".

11 The concept of supervision has featured significantly in discussions between Member States about the implementation of the Directive. The approaches proposed range from the stringent – with detailed rules supplementing the terms of Annexes I and II – to light touch regimes. There is clearly a strong feeling in some Member States that the value of qualified certificates as a basis for the use of electronic signatures in transactions depends on the certainty that Annexes I and II are applied with rigour.

Author: Peter SJF Bance MBCS CEng

Equally, other Member States are placing greater faith in accreditation arrangements to ensure that the objectives of the Directive are met.

12 The issue is how to take this forward in the UK. There are two questions: what should be the nature of the supervisory regime and whether legal backing should be given to the supervisory function; who should take on this role of the supervisor.

The nature of a supervisory regime

13 As indicated above, this is an area where the Member State has discretion. The UK supports the objectives of the Directive and would not wish to implement supervision in a way which would undermine confidence in the use of qualified certificates. Nevertheless, the Government's guiding principle on the use of regulatory powers is to "fit the remedy to the risk". The problem in this case is that both the nature and the scale of the risk are, at this stage, unquantifiable. The risk would be to the confidence by society generally in these forms of authentication and, in particular, the risk to relying parties if qualified certification did not fulfil the expectations of the Directive. It is by no means certain that a large number of suppliers will issue qualified certificates and it is not clear how many will do this outside of the co-regulatory framework of the tScheme. The risk, and hence the remedy, would be entirely different if the market was serviced by a small number of large, reputable organisations working in a co-regulated environment compared with several hundred small or micro service providers. It is worth considering the types of supervisory regime which might be appropriate for these extreme scenarios.

14 In a low risk scenario, supervision may be de minimis. This would involve the supervisor observing the market and recording those service providers of which he becomes aware either through observation or the provider volunteering information. The supervisor would give such publicity as he considered appropriate to any activities of certification service providers of which he became aware which did not comply with the Directive.

15 In a high risk scenario, it is possible to envisage a much more active supervisory regime. If there was sufficient grounds to suspect that the terms of Annex II were not being complied with to any significant extent (evidence of non-compliance with Annex I being more easily determined) or qualified certification was brought into disrepute in other ways, then powers might be taken to:

- Require notification that qualified certificates were being issued, with penalties for non-reporting (if this were done after the commencement of business, it would not breach the disbarring of prior authorisation);
- Require documentation to be maintained supporting claims of compliance with the Annexes and penalties for the failure to do so;

16 In such a regime, direct auditing of the documentation or the commissioning of independent audits would probably be occasioned by a trigger event such as an observation of malpractice or a complaint by the public. Such a regime would be resource intensive and a fee regime would need to be established and notified at the time such a regime was established.

17 In deciding the way forward, we also need to bear in mind the impact of tScheme. The scheme is voluntary but is committed to accommodating the specific requirements of qualified certificate issuance into its approval

Author: Peter SJF Bance MBCS CEng

profiles. If tScheme is successful, and the majority or all of the issuers of qualified certificates are tScheme approved, this will lead to confidence in the issuance of qualified certificates in the UK.

Who should be the supervisory body?

18 The classical "regulatory" skillsets are available in many parts of Government. For the more rigorous approach to supervision, the most obvious candidate to undertake this role would be OFTEL (noting the proposal to merge this organisation into a more broadly-based OFCOM). The need to challenge CSPs on elements of the Directive which are based on cryptographic technologies would probably require the import of specialist skills. These are available commercially but it might be more credible if this specialist function were performed by the Communications and Electronic Security Group – the Government's technical authority on information technology security.

19 A more radical approach would be to ask tScheme to undertake this function. The Directive says that service providers should not be obliged to apply to be supervised under any applicable accreditation scheme. There is a strong argument that those organisations who have consciously chosen not to subscribe to tScheme and its values should not be compelled to become linked to the Scheme, simply because they have chosen to issue qualified certificates.

20 Nevertheless, it is possible to envisage a role for tScheme, or other bodies that may come forward, in assisting or leading on the supervision function if it were closer to the de minimis model described above.

Conclusions and what action should Government take?

21 At this stage, given the uncertainty of the market, the Government propose to provide by regulation the de minimis option outlined above. This will be subject to review in two years (and thus will fit well with the timetable for the review of the Directive) and the regime will be reassessed in the light of the development of the use of qualified certificates in the UK. This review will require a dialogue with the relevant stakeholders and a formal consultation on whether the role of the supervisor should be changed.

22 It is proposed that a supervisory regime be established to take receipt of representations on the performance of CSPs and publicise information about the appropriate issuance of qualified certificates. At this stage, it would seem most appropriate to maintain the supervisory function within the DTI but to ask tScheme to assist in the observation and commentary on market practices. We believe that this would most clearly meet the Government' s guidelines on Better Regulation.

QUESTION 1: Do you agree that the implementation of a supervisory regime should be based on a de minimis approach and subject to review in two years' time?

Secure Signature Creation Devices

23 The Directive places emphasis on the security of the signature creation device and Annex III sets out in broad terms what properties are required to be considered a "secure signature creation device". (SSCD). This mirrors the benchmarking of the certification process and the two – SSCD and Qualified Certificate – used together meet the quality requirements of the class of Advanced Electronic Signature [4] which should be seen, in certain

circumstances, as being equivalent to a hand written signature (see discussion of Article 5.1 below).

24 The Directive deals with how Member States may ensure that SSCDs meet the terms of Annex III. Article 3.4 permits Member States to designate appropriate public or private bodies to determine the conformity of such devices with the terms of Annex III. Such designated bodies have to meet certain criteria laid down by the Commission in consultation with the Member States. This process has been finalised and the criteria – which deal in broad terms with the competence, integrity and independence of such bodies – have been laid down [5]. Article 3.5 goes on to describe a process whereby the Commission can publish the references to Standards for electronic-signature products and that Member States shall presume that there is compliance with the requirements laid down in Annex II point f (the requirement that certification service providers use "trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them") and Annex III (the requirements for secure signature creation devices). Thus there are effectively two routes for a device to meet the terms of Annex III.

25 The two questions in relation to the implementation of the Directive are whether the Government should appoint a designated body under 3.4 and whether any specific action should be taken to ensure that the Government can give due weight to the need to acknowledge compliance under 3.5.

Designated body

26 The Government seeks the views of all interested parties on whether the UK should appoint a designated body.

27 As background to this decision, the following factors should be taken into account. There is wide scope for how the designated body might perform its task of assessing against the compliance of devices with Annex III. It could simply take the terms of the Annex as a template and judge evidence in support of the individual components against that template. Or the designated body could refer to standards. A Standard is under preparation within the joint CEN/ETSI European Electronic Signatures Standardisation Initiative (EESSI) – an attempt by European business to provide standards to support the Directive and promote interoperability amongst authentication products and services. This Standard has proved controversial and at the time of the consultation it was not clear whether the Standard would be agreed or when it might be approved under the process described in Article 3.5.

The draft Standard is effectively based on the Common Criteria approach of drawing up a standard profile for assessment by a third party. If such a standard were agreed and the designated body did not use it or other standards with the same objective, it might leave the UK open to the criticism that the assessment regime for these products was not in keeping with the spirit of the Directive and lacked sufficient rigour.

28 The most obvious designated body might be CESG who could manage the process alongside the existing UK assessment scheme under the Common Criteria for product security evaluations. Another possible approach would be to ask tScheme to extend their remit and to specifically take on the task of the designated body. The scheme could use the Standard or develop its own profiles in the light of the Standard to run assessments by appropriate third party assessment bodies (these might well be the existing Common Criteria/ITSEC

Author: Peter SJF Bance MBCS CEng

approval bodies but might also be the assessment bodies who are being appointed to carry out tScheme profile assessments).

29 Another important factor in the Government' s decision will be the cost. There are very few manufacturers of these products in Europe (although manufacturers from outside the EU can apply to any designated body). The Government would need to be assured that any costs it bore in setting up such a designated body would be justified by a level of approvals which would meet the ongoing costs of maintaining such a body. It is this sort of consideration which is leading many Member States to be cautious about the possibility of establishing a designated body. The Government would therefore particularly welcome the views of the manufacturers of such products to establish whether the creation of a designated body is feasible.

30 A designated body does not need to be appointed and, in any case, not before the deadline for implementation and does not require the Government to take new powers. If it were decided to appoint a designated body this could be done by an administrative act.

QUESTION 2: Do you believe that the UK should have a designated body and if so who should it be and how should they assess compliance with Annex III of the Directive?

The presumption of compliance

31 We do not believe that we need to make legislative changes to implement 3.5. The UK is bound to accept that compliance with appropriate standards created under Article 3.5 will have the effect of assuring compliance with Annex II point f or Annex III. For Annex II, we believe that this will compel the UK to accept that those service providers subject to supervision under the Directive (see above) will be deemed to have met the terms of Annex II point f if they meet the relevant standard (and again one is in preparation by EESSI). For standards relating to Annex III, we believe that, when presented with an advanced electronic signature, the UK will need to accept as confirmation of the validity of the signature creation device, either a current approval from an EU designated body or confirmation that the terms of the relevant standard have been met. There are at present no plans to introduce independent assessment regimes for either standard referred to in Article 3.5 (although it is possible that the existing product evaluation scheme could be extended to provide such assessment). Advice will need to be prepared for those parts of the public sector who are likely to accept digital signatures in the course of their business on what the recognition of such standards will mean in practice.

QUESTION 3: What do you believe will be the impact of Article 3.5 and is there any further action the Government could take?

Signature Verification Devices

32 Article 3.6 requires Member States to work together with the Commission to promote the use of Signature Verification Devices according to the recommendations in Annex IV.

The Commission have not made proposals on how such promotion might be undertaken. Accordingly, we make no proposals in respect of this requirement.

Public Sector requirements

33 Article 3.7 allows Member States to make the use of electronic signatures subject to possible additional requirements - relating only to the specific characteristics of the application used. Several Departments are looking at the use of PKI technologies for internal purposes and in relation to the more sensitive transactions with citizens and businesses. The Office of the eEnvoy have set out its views on how authentication techniques might be used in relation to on-line Government Services. (www.e-envoy.gov.uk/frameworks/authentication/contents.htm) These principles will inform the way that authentication is used at the "Gateway" portal for one-stop citizen and business access to Government services. The Office of the eEnvoy, in conjunction with the Communications and Electronic Security Group, are also developing guidance on the use of public key infrastructure within Government.

34 The Government will need to ensure that any "additional requirements" will need to meet the terms of Article 3.7 and advice will be prepared on how such requirements should be imposed and how they might be notified to the Commission under the terms of Article 11.1(a). In particular, this guidance will need to make clear that such requirements may "not constitute an obstacle to cross-border services for citizens". In this context it is important that Departments understand the meaning and value of qualified certificates and advanced electronic signatures originating from other Member States.

QUESTION 4: Do you agree with our analysis of the meaning of Article 3.7 and the proposed course of action to ensure compliance with it?

Article 4 Internal Market Principles

35 This article requires that each Member State should not restrict the provision of certification services originating from other Member States and should allow electronic signature products which meet the terms of the Directive to circulate freely. None of the proposals in this paper appear to create any internal market problems. No further action is planned in relation to this requirement.

Article 5 Legal Effect of Electronic Signatures

36 The key elements of Article 5 - the legal admissibility of electronic signatures - has been met by Section 7 of the Electronic Communications Act. This covers both Article 5.1(b) and 5.2 which deals with the electronic signatures in legal proceedings.

37 It is the Government' s view that the first part of Article 5.1 will need to be implemented in UK law. This states that:- "Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure signature creation device a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data:"

38 We propose to provide under regulations made under section 2(2) of the European Communities Act that where a person in relation to data in electronic form uses an advanced electronic signature which is based on a qualified certificate and is created by a secure signature creation device, any legal requirement for a signature in respect of such data is satisfied. This would not alter the substantive English, Northern Irish or Scots law on when writing

is required for a transaction. Its practical impact should be limited given that requirements as to form usually specify both writing and signature. Implementation in Scotland and Northern Ireland would be a devolved matter to be dealt with by Scottish and Northern Irish Ministers, the Scottish Parliament and the Northern Irish Assembly.

QUESTION 5: Do you agree with the proposed regulation to implement Article 5.1(a)?

Article 6 Liability

39 Article 6 requires Member States to impose a minimum level of liability on certification service providers who provide qualified certificates to the public. Article 6(1) requires that where:-

- a certification service provider either:-

    - issues a certificate as a qualified certificate to the public; or
    - guarantees a qualified certificate to the public

- and a person reasonably relies on that certificate for any of the following matters:-

    - the accuracy of all information contained in the qualified certificate at the time of issue
    - the inclusion in the qualified certificate of all the details referred to in Annex I of the Directive;
    - the holding by the signatory identified in the qualified certificate at the time of its issue of the signature identification data corresponding to the signature verification data given or identified in the certificate; or
    - the ability of the signature verification data to be used in a complementary manner in cases where the certification service provider generates them both

- and as a result that person suffers loss,

then the certification service provider must be liable in damages in respect of the loss “unless the provider proves that he had not acted negligently”.

40 We believe that this will require that the claimant will need to establish that the service provider issued or guaranteed a qualified certificate to the public, that the claimant reasonably relied on it and that such reliance was for any of the specified purposes and that damage was caused by such reliance. The final words of Article 6(1) make it clear that the onus is on the service provider to prove that he had not acted negligently. We have looked at the obligations imposed by Article 6.1 against the existing requirements of the English, Northern Irish and Scots law of tort and delict and contract. We have concluded that existing law does not provide a comprehensive solution to the requirements of the Directive and therefore provision will need to be made which would ensure that in the circumstances set out in Article 6.1 a certification service provider is liable unless he proves that he has not acted negligently and that this liability is not dependent on the existence of a duty of care.

41 Article 6.2 requires that where:-

Author: Peter SJF Bance MBCS CEng

- a certification service provider issues certificates as qualified certificates to the public;
- a person reasonably relies on that certificate; and
- that person suffers loss as a result of any failure by the certification service provider to register the revocation of the certificate,

then that certification service provider must be liable in damages in respect of the loss unless the certification service provider proves that he has not acted negligently.

Again provision will need to be made to ensure that in the circumstances set out in Article 6.2, a certification service provider is liable unless he proves that he had not acted negligently and that this liability is not dependent on the existence of a duty of care.

42 Provision will also need to be made to implement the requirements of Article 6.3 – that certification service providers can indicate limitations in the qualified certificate on its use and shall not be liable for loss as a result of the use of the certificate which exceeds that limitation. Likewise, provision will need to be made to implement the requirements of Article 6.4 – that certification service providers may indicate a limit on the value of transactions for which the certificate can be used and shall not be liable for any loss to the extent that loss results from the use of the certificate in relation to a transaction the value of which exceeds that limit.

QUESTION 6: Do you have any comments on the proposal to implement Article 6 and that this should be achieved by regulations under the European Communities Act?

Article 7 International Aspects

43 The Directive requires that Member States treat qualified certificates originating from non-EU service providers as legally equivalent to EU certificates if they meet one of three criteria. These are that they are accredited by a an accreditation scheme in a Member State, their certificate is guaranteed by a service provider from a Member State or the service provider is in a country which is subject to a bilateral or multilateral agreement.

No further action is proposed to meet this requirement.

Article 8 – Data protection

44 Article 8.1 requires Member States to ensure that certification service providers and national bodies responsible for accreditation or supervision comply with the requirements of Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This Directive has been implemented by the Data Protection Act 1998.

45 Article 8.2 goes further however and requires member states to ensure that a certification service provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate.

Author: Peter SJF Bance MBCS CEng

Article 8.2 further requires that data may not be collected or processed for any other purpose without the explicit consent of the data subject.

46 Provision will need to be made to ensure that these stricter requirements concerning data protection apply in relation to certification service providers referred to in article 8.2.

QUESTION 7: Do you agree with the proposal to implement Article 8.2 and thereby place specific data protection requirements on certification service providers?

Articles 9-15

47 These articles concern the management of the implementation of the Directive.

Conclusions

48 It is difficult to envisage what impact the Directive will have on the use of authentication in the EU and in the UK in particular. In particular it is difficult to see where and how the concept of the advanced electronic signature will impact on UK electronic transactions. It is possible that the concept of the qualified certificate will gain currency and will assist in the growth of the electronic authentication and provide clear co-ordinates for arrangements on the mutual acceptability of certification with other jurisdictions. Some of these uncertainties may be resolved by Governments adopting these benchmarks for G2B or G2C services. The benchmarking of the provision of certification clearly chimes with developments in the UK especially the idea of approving service providers embodied in Part 1 of the ECA and being given substance by the work of tScheme.

49 Against this background the above proposals are designed to meet the requirement of the Directive with the lightest possible touch.

QUESTION 8: Do you have any views on the likely impact of the Directive in the UK and how it may assist in promoting trusted and secure electronic transactions?

Consultation

50 We invite comments as soon as possible and by no later than 19 June 2001. It will not be possible to take into account responses received after this date.

51 Comments should be sent to Geoff Smith at DTI either by: by e-mail (preferably as a Word document or text format) to (elecsigsconsultation@dti.gov.uk) or in writing to:

Information Security Policy Group
Communications and Information Industries Directorate
Department of Trade and Industry
Bay 226
151 Buckingham Palace Road
London SW1W 9SS

Clearly stating who you are and, where relevant, who you represent. You are free to comment on any aspect of the implementation of the Directive but it

would be helpful if you could address the questions referred to in the body of the text above and summarised at Annex B.

52 Should you wish any part, or all, of your comments to be treated in confidence you should make this clear in the response. In the absence of such instructions, responses will be assumed to be open placed, in the Libraries of the of the Houses of Parliament, published by Ministers (including publication on the DTI website) or shared with others. In the event that there are a large number of responses and a range of views on the proposals outlines above, it would also be out intention to publish a summary of the response to this consultation exercise.

DTI
Communications and Information Industries Directorate
March 2001 URN 01/750

[Annexes omitted – repetition]

[Footnotes]

[1] The use of the term “electronic signatures” enables the law to reflect a broader set of approaches to electronic authentication and not simply to focus on digital signatures based on the cryptography.

[2] The Directive uses the term “accreditation” to describe the process described as “certification” in the UK – that is the third party assessment of suppliers. The tScheme is more closely aligned to the process of certification in that it controls the use of an approval mark. Agreement to grant approval is based on independent assessment of the tScheme profiles by bodies that are accredited by the UK Accreditation Service.

[3] For more information on tScheme go to WWW.tscheme.org.

[4] The use of the term Advanced Electronic Signature in the Directive is worth comment. As a defined term it exists as four broad performance characteristics. In this form, the concept only clearly features as a requirement on the way in which a certification service provider signs a qualified certificate. The only other specific reference to Advanced Electronic Signatures is in Article 5.1 which requires the additional criteria of meeting Annexes 1, II and III. This has led some jurisdictions to coin new expressions – such as “qualified signature” – for this special class of Advanced Electronic Signatures.

[5] Commission Decision (EC) 2000/709 (OJ L289, 16.11.00, p42)

End of document

Author: Peter SJF Bance MBCS CEng