Signature Directive Consultation

Ross Anderson and Caspar Bowden

Foundation for Information Policy Research

1 Executive Summary

At the request of the European Commission, the Foundation for Information Policy Research (FIPR) compiled this response to theEU Draft Directive on Electronic Signatures (COM1998 297 final). It was prepared following extensive input from trade associations, companies, academics, individuals and the DTI (a progress report of the 21/8/98), a discussion at the FIPR Advisory Council, and a public consultation exercise during September – October 1998.

On the basis of these consultations, FIPR believes that the proposed Directive will be an important step towards facilitating electronic commerce through harmonised cross-border recognition of electronic signatures. Many member states are already taking steps to remove obstacles in their national laws to the use of digital signatures; however the Directive is likely to accelerate the process and also to bring important harmonisation benefits. FIPR therefore supports the draft directive and seeks to help the European Commission in identifying and dealing with possible points of conflict.

The draft Directive requires Member states to ensure that "electronic signatures" which are based on a "qualified certificate" issued by a certification service provider which fulfils certain requirements are, on the one hand, recognised as satisfying the legal requirement of a hand written signature, and on the other, admissible as evidence in legal proceedings in the same manner as hand written signatures.

Our consultation exercise has identified a number of issues arising from it, which the Commission might care to consider while finalising the text of the directive, and while coordinating this activity with work in the fields of consumer protection, data protection and the regulation of trade and financial services.

In the following sections, we describe the feedback that we received from our respondents, raise some discussion points, and make some recommendations. In the final section, we set out suggested changes in the draft of the Directive.

2 "Identity" vs "Authorisation" Certificates

Many of the issues raised by respondents concern the question of whether certificates are more like passports or more like credit cards - in other words, whether they certify the identify of the certificate holder or his authorisation to perform some function, such as by using a payment system.

The limited utility of "identity" certificates for trust management has been brought out in many technical discussions and compared with "authorisation" (or "capability") certificates which bind a private key to some specific capability or permission.

> 'A keyholder's name is one attribute of the keyholder, but...rarely of security interest. A user of a certificate needs to know whether a given keyholder has been granted some specific authorisation....The certificate holder should be able to release a minimum of information in order to prove his or her permission to act.' (SPKI requirements 11/3/98).

It is thus widely believed that identity certificates may not be the best technical or commercial solution for e-commerce, and under the draft Directive's proposals, qualified certificates bind a "signature creation device" (commonly envisaged to be a private key embedded in either a smartcard or a piece of software such as a browser) to "the unmistakable name of the holder or an unmistakable pseudonym", and thus appear at first sight to fall into the identity certification camp.

Many respondents therefore argued that the Directive should positively accord legal recognition to "authorisation" certificates as well as "identity" certificates. To a great extent it does so already, as Annex 1 (c) requires that a qualifying certificate bind the holder's name or pseudonym to *'a specific attribute ... such as the address, the authority to act on behalf of a company, the credit-worthiness, VAT or other tax registration numbers, the existence of payment guarantees or specific permits or licences'*. It is not wholly clear what else 'authorisation certificates' will entail, although we received a number of suggestions.

Four possibly problematic applications bear mentioning from the many that have been brought to our attention:

- SET certificates bind a key to a credit card number rather than to an individual. Yet the banking industry would very much like SET signatures to have legal force. Some bankers claim that this can be achieved using contract law, by forcing all SET users to sign paper contracts with their card issuers. However bank-customer contracts have been set aside as unfair in the past in a number of countries.
- Firewire certificates may be very widely deployed in consumer electronics equipment and bind a private key to an equipment serial number. They will be used in the prevention and detection of copyright offences, and industry would like them to have evidential value in prosecutions.
- The adoption of EDIFACT security mechanisms in applications such as messaging between doctors and hospitals in Britain's National Health Service is complicated by legacy systems which often compel the signature on, say,

a lab report to be generated in an EDIFACT translation system shared by all the staff at a pathology laboratory; it is thus the laboratory's signature rather than that of any individual. Doctors wish to be able to rely on such signatures not just for safety reasons but also in medical negligence claims. More generally we will need to make provision for the signatures of legal persons such as companies, as well as of individuals.

– In electronic publishing systems, such as one being developed for the British National Formulary (the list of all drugs that doctors may prescribe), digital signatures are not affixed to individual entries but, for performance reasons, are combined using a hash tree whose root is signed. It is desired that this signature should still be considered to provide non-repudiation for all the leaves of the tree. The issues here are twofold: firstly, the multiple levels of indirection between the leaf and the root, and secondly that the ultimate root signer may not be the publishing company, but the software vendor who certifies the publishing company's root key (this is also an issue for SET and for systems such as Authenticode).

Under Article 6, only signatures based on qualified certificates (from an Annex II CSP) are positively accorded legal effect (although other signatures should not be denied effect solely on grounds of being electronic, non-qualified, or non-accredited). This appears to be rather confusing and its effect for applications such as those mentioned above should be clarified. We recommend, for example, that Article 2 should be redrafted to include delegation: when someone has a qualified certificate, and uses the corresponding private key to sign a certificate delegating a power of attorney for some matters to a key held by their lawyer or spouse, then signatures created using this key should clearly have effect.

We also recommend that the Directive should not limit itself to certificates issued by CSPs who do *'deal directly with the public'* as very many proposed applications will be restricted in some way. For example, there have been talks in the UK about the General Medical Council (the registration and disciplinary body for doctors) running a healthcare CA. However, the GMC does not issue certificates to the public and would thus fall outside the scope of Article 2 (6). Furthermore, the operation of this CA may be outsourced to a facilities management company which might also certify keys for nurses, physiotherapists and other clinical professions whether directly or via a GMC-led consortium. Similarly, it is proposed that the UK banks will issue SET certificates to their customers, but that the certificate manufacture and revocation list management will be performed by a jointly owned technical company. The directive does not speak clearly to such arrangements; the simplest resolution might be clarification that all these parties are CSPs for the purpose of the Directive. However, then the prescriptions of Annex II become quite excessive. We will return to this below.

Two of our respondents strongly agreed with the Directive's focus on *'authentication linked to identity of a physical legally responsible person':* "The possibility of holding a person accountable for his acts and taking him to court is central in our society. We are not just living in a sea of role holders." However this was a minority view.

Several respondents pointed out that while corporate persons may be identified uniquely by their country of registration and registration number, there are very serious difficulties in identifying natural persons. Names are rarely unique, addresses change, and so there might be pressure to use a unique national identification number. But this introduces cultural factors, or privacy risks, or both, that may be unacceptable culturally in many member states. For example, the UK and Ireland have no identity cards and the concept is unacceptable to many people; while in Germany, which has identity cards, the use of the identity number is too tightly constrained by data protection law to be usable in general purpose public key certificates. For all these reasons, the requirement in Article 2 (1) (b) that signatures be capable of identifying the signatory appears to be excessive, as is the requirement in Annex 1 that certificates contain the unmistakable name or pseudonym of the holder. For many practical purposes, the requirement in Annex 1 (f) that each certificate contain a unique identity code will be sufficient.

Some respondents argued that many business applications would seek to leverage off existing systems in which identification was not necessarily unique: operators of systems such as loyalty cards and frequent flyer programs do not find it economic to determine which of 'Caspar PS Bowden', 'CPS Bowden', C Peter Bowden' 'C Paul Bowden', 'C Bowden' and 'Christopher Bowden' correspond to the same individual. Strong identification requirements would be extremely onerous in such applications. In the banking world, attempts to move from account-based to name-based systems have caused severe problems (we heard of one case in which a man's mistress's bank statement was sent to his wife's address following such a system change).

Some respondents argued that for ordinary business correspondence, signature certification via third-parties was unnecessary, or unjustifiably complex and costly. Trust between parties can be developed directly, through a commercial relationship, and existing mechanisms to deal with fraud and default are adequate. Implications include that signatures backed by a public key fingerprint on a letterhead or business card should be valid. Others take the view that strengthened non-discrimination provisions would be adequate here.

More than one respondent pointed out that large volumes of electronic transactions already take place without digital signatures, as is indeed the case in the paper world:

> 'The concept that a signature is vital for every message exchanged is totally artificial. A great volume of business correspondence is already transmitted by one electronic method or another without hazard (without even the need for encryption) and business interests themselves from experience find methods for correcting the few cases where difficulties arise. Simplicity is preferable to the expense of complexity.'

A significant issue is whether national laws passed to implement the draft directive might undermine existing electronic commerce, by casting doubt on existing 'signature' methods (such as a typed name at the bottom of an unprotected ascii email) which the courts currently consider to be valid. If this were to happen, the net effect of the draft directive could be the opposite of that intended; it could do serious harm to the development of electronic commerce in the European Union.

We would therefore suggest a two-pronged approach. Firstly, member states should not introduce legislation that undermines the validity of existing electronic writings (including those writings without particularly strong protection mechanisms, such as a name typed at the bottom of an email message). Such writings should continue to enjoy a rebuttable presumption of validity. Secondly, where member states are amending existing laws that specify manuscript signatures for particular purposes, such as mortgages, guarantees and tax returns, it should be open to them to specify that signature mechanisms or services should meet such minimal technical standards as are specified by the Commission under Article 3 (3), for which adherence to an accreditation scheme would be prima facie evidence of compliance. This is probably close to the intended effect of Article 5 but that article might perhaps be clarified.

There are also issues relating to whether the draft directive is general enough to deal with likely future trust architectures, such as XML in which keys, timestamps, copyright management data and other security objects may be embedded in electronic documents in quite general ways. If different member states deal with these technical issues in different ways, there is still scope for quite serious barriers to trade. So the Commission may have to be fairly active in maintaining the standards published under Article 3 (3).

3 Issuance of Certificates

Qualified certificates are defined as containing *'the identifier of the certification service provider issuing it'*, with the implication that (a) certificates are issued by a CSP, and (b) certificates are certified by a single CSP.

In this model, the validity of certificates issued by a CSP generally depends on authorisation by a "higher-level" authority. Signatures are verified by validating the certificate of the issuing authority, through a formal hierarchy or tree, until the "root" is reached. But as noted above, in a number of fielded systems, this "root" is a public key which is embedded in mass market software or hardware. The software or hardware vendor may either auction off the privilege of having one's key signed by this root, or make it available only to its marketing partners. There is an obvious risk of conflict between member states, who will wish mass market software sold in their countries to include all authorised CSPs, and vendors who will wish to use their control of root keys as a continued source of revenue. We were informed of one CSP in a member state that went out of business after failing to persuade one of the browser vendors to include its key in the browser distribution. We note that a similar issue has already arisen in relation to conditional-access gateways to pay-TV systems, and the regulatory framework necessary to promote competition and inhibit artificial barriers to entry have been addressed by the Commission and by national regulators.

Several respondents expressed concern on these grounds, and acknowledged the inconsistency with policy on pay-TV gateways: "the possibility for unfair market dominance certainly exists, and both the Commission and national governments must have adequate powers to regulate competition in this area."

Another model of certification permits the holder to create a "self-signed" certificate, which may subsequently be submitted to other parties (including CSPs), and accumulate a number of certifying signatures from these parties. Signature verification requires validation along a chain through a "web" of "trusted introducers".

It is not clear whether the web-of-trust model of certification is ideal for e-commerce applications; although it may give evidence of identity, it is less clear that it can support authorisation directly. However, some respondents believe that there are two reasons to accommodate it. Firstly, there may be many applications in which one wishes to give weight to a user-created certificate, such as if a user creates a delegation certificate authorising (for example) his attorney to control his bank account. Secondly, the most widely used software for generating and verifying digital signatures on arbitrary user generated messages is PGP; and export restrictions hinder the emergence of any competitor with the necessary world-wide deployment and availability. Some respondents felt that in many applications, PGP will remain the preferred solution. Other respondents disagreed, and believe that a legal binding between a public key and either an identified person or a set of authorisation attributes is necessary.

It has also been pointed out that, in an ideal world, different keys should be used for different applications, and the use of an identity key for banking transactions is less than ideal. We will return to this in the section on revocation; meanwhile we will note in passing that it may be an argument against the web of trust. If a key is certified by multiple principals, then it must be very clear on which of them one is placing reliance for a particular transaction. This can make the system design much more complicated than one in which each application has its own key material and certification infrastructure. Attempts to deploy shared infrastructure in the past (such as multifunction smartcards) have been notably unsuccessful.

There was much discussion of the relative merits and extent of standardisation of PGP and S/MIME. S/MIME proponents pointed to a broad degree of compatibility with present products, and unsuitability of the web-of-trust model for business use. PGP proponents pointed to the prospect of broad compatibility following agreement of an open IETF standard, that it can equally support hierarchical trust models, and the incomplete state of the S/MIME v3 standard. The ISO 9735 standard for EDIFACT was also mentioned as likely to become important in future. Overall, though, there was strong support though for the draft directive's aim of technological neutrality.

A third model of certification is where public keys are certified using existing, non-electronic mechanisms. One early example of this is the 'Global Trust Register', a directory available in both paper and electronic form which contains the fingerprints of many of the world's most important public keys. This approach to certification attempts to rectify the worst shortcomings of the first two approaches. Likely future examples include the established directories of doctors, lawyers, etc which could easily include public key fingerprints. There are also people who include a public key fingerprint on their business card or letterhead. It would clearly be a bad thing if the Directive were to render invalid a signature made using a key whose owner had publicly certified it by such out-of-band means. It was noted that an exclusion of out-of-band certification might also lead to technical challenges to whichever out-of-band means were used to distribute the root public keys of authorised CSPs.

One respondent suggested that in order to accommodate non-electronic verification of certificates, the term "device" should be selectively replaced by "means" (as in "signature verification means"). We strongly support this proposal; it addresses a number of other difficulties such as how an X.509 certificate might be considered to contain a "signature verification device" as in Annex I.

Finally, there is an inconsistency in the Directive in that Article 6 (1) (a) and (c) refer to the date and/or time of certificate issue while Annex 1 refers to the "operational period". There is a possibility for confusion here as in the banking sector; for example, the issue date of a credit card frequently predates its operational period by some weeks. We suggest that all references should be to the "operational period" and let this be defined more precisely, if need be, by the contract between the user and the CSP.

4 Recognition, Accreditation and Non-discrimination

The German digital signature law sets out a number of criteria for CSPs. High technical security standards will impose high entry costs, which in turn will lead to certification services being provided by a small number of large organisations rather than by a large number of small firms. Many respondents argued that this is a bad thing. Firstly, large certifiers may abuse their position for anti-competitive purposes; this has been raised in the context of both pay-TV and browser vendors. Secondly, it would be more natural (and help public acceptance) if CSPs were organisations that people trust, such as the family lawyer or doctor, rather than a distant impersonal body such as the passport office or the phone company.

In many applications, local certification makes sense. For example, Europe's largest employer – Britain's National Health Service – manages personnel at the level of the individual hospital or medical practice rather than having a single central staff function. It would therefore be much more convenient to manage keys and certificates at this level rather than centrally, and this is what existing encryption pilots and projects do. The prospects of 11,000 small certifiers alarmed some interests in government, which suggested one large centralised TTP, but this now appears to have been rejected, both on economic grounds and for reasons of professional control and confidence. Similar issues have already arisen in the context of the control of electronic tachographs, and one may also expect them to arise in other professional and commercial applications.

A frequently proposed compromise is to have a small number of large certifiers who manufacture the actual signatures, while a larger number of small registration authorities interact with the consumer. This is the arrangement that UK banks are developing for SET certification; the user will deal with his bank, which will outsource the certificate manufacture to a central, jointly-owned facility. This facility will be invisible to the user, whose contractual relationship will remain with the bank. It is also a possible solution in health care, where a central CA operated by professional bodies could be supported by local CAs or registration authorities in hospitals, clinics and medical practices.

The draft directive could cause problems here by prescribing liability relations with the banks' central facility rather than the customer's bank, and with the doctors' professional association rather than with the doctor responsible for a given patient's care. The obvious solution is that, on a literal reading of Article 2 (6), all the certifiers – both central and local – qualify as CSPs. However, in that case the small certification or registration operations run in small banks or family medical practices would not meet the technical requirements of Annex II (e.g., to employ persons with expertise in electronic signature technology). Our suggested resolution is to leave the definition of CSPs broad, but to redraft Annex II so that small certification and/or registration functions operated in small to medium sized enterprises can meet its requirements.

More generally, legal (and threat) models of accreditation satisfactory for business-to-business e-commerce, are not necessarily appropriate for business-to-consumer and professional-to-citizen applications, although they are often assumed to be, resulting in significant distortion of existing trust relationships. They may also frustrate new developments sought on technical grounds. An example is cross-certification by CAs, which is desirable in many applications and not difficult technically, but which raises interesting liability issues.

The draft directive gives some relief. Article 6 (2) allows CAs who perform suitable due diligence to avoid responsibility for incorrect information supplied by the certificate subject, and Explanatory Memorandum III-7 states that *'The legal recognition of electronic signatures should be based upon objective, transparent, non-discriminatory and proportional criteria and not to be linked to any authorization or accreditation of the service provider involved.'* The Preamble (10) states *'whereas the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorization of the service provider involved.'*

Yet Article 3 (2) states that *'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.'* Article 5 (Legal effects) does not contain a reference to non-discriminatory recognition, merely that a signature should *'not be denied legal effect...on the grounds that...(it) is not based upon a certificate issued by an accredited certification service provider.'*

The combined effect of these provisions is confusing. There appears to be no explicit prohibition of discriminatory linkage of (voluntary) accreditation to recognition, corresponding to the that contained in the Memorandum and Preamble. The UK is contemplating legislation which would counsel the courts to presume a lower burden of proof for signatures based on certificates from voluntarily licensed CSPs, than for unlicensed, thus creating market pressure in favour of licensed certificates. The adoption of such measures by some but not all member states is bound to raise barriers to the internal market.

The primary purpose of the Directive (the prevention of internal market barriers) could be seriously undermined if national licensing were the only effective route to ensure recognition without legal uncertainty, especially during the phase of rapid growth expected before the Directive is adopted and implemented. If licensing was also conditional on voluntary acceptance of other national policy goals (such as third-party key escrow), these barriers could become entrenched. Clarification of the effect of "non-discrimination" provisions on the burden and standard of proof, and other auxiliary national licensing conditions, should be incorporated into the Articles. Our specific suggestion is to redraft Article 5 so that member states must recognise not just signatures based on a qualified certificate, but also signatures generated in accordance with the standards recognised by the European Commission under Article 3 (3).

5 Revocation

The revocation of certificates is of great importance to commerce. Over the years, banks have developed complex worldwide systems for revoking stolen credit cards, with 24-hour emergency numbers, national and worldwide blacklists, and multiple levels of stand-in processing to reduce communication costs. Proposals for the revocation of public key certificates have not evolved to this level, but some systems (such as SET) will piggy-back on the existing credit card infrastructure.

In the single-issuer model of X.509, the power to revoke a certificate rests with the issuer, and revocation of the issuer-certificate of a CSP revokes the validity of all certificates at lower levels, if verification is performed hierarchically. The propagation of revocation information is thus critical; and improper revocation of a high-level certificate causes drastic denial of service.

In the web model, revocation may also be under the control of a certifier (e.g. a CSP) or the certificate holder. A certificate may be regarded as selectively valid according to the extant trust chains which can be verified. Revocation propagation must be well defined, but a web of trust can be made resilient to single points of failure.

More recent implementations and proposals introduce a number of new mechanisms ranging from designated revokers through reconfirmation services. (These are not supported by Annex II (b) which should be amended appropriately.) It is becoming increasingly widely realised that the risks of permitting an arbitrary number of people to rely on a certificate for value are severe; in the language of the credit card industry one should ideally have a zero floor limit for internet transactions. In the absence of this (and even perhaps in its presence), banks will insist on recourse against the merchant. Otherwise there is a risk of attacks, whether for profit or purely disruptive, in which a credit card is simultaneously used at a large number of online merchants.

Some respondents thought that revocation issues, being technically unresolved, should be relegated to a separate Annex or to future standards promulgated under Article 3(3). However, revocation could become extremely complex, especially if the prevailing model were a multifunction user smartcard, issued by the government, which operated as a national identity card yet also held applications such as an electronic purse, a transport ticket, prepayment for utility meters and road tolling; specifying it in regulations would be inappropriate. Others took the view that Annex I should require that the certificate contain details about revocation policy. But this would exclude fielded systems whose certificates contain no such details. On balance we suggest that a revocation policy statement should be an optional feature of certificates, and the situation kept under review.

6 Liability

A closely related set of issues concern liability. The Directive seeks to make member states ensure that certification service providers which issue qualified certificates are liable to persons who rely on the certificate, in limited respects.

The curious situation that arises here is that 'open' certificates that the certificate subject may present to as many people as he wishes – such as passports, university degrees, driving licences and professional registration documents – are not instruments which normally give rise to any liability by the certificate issuer. Those instruments which do commonly give rise to liability – such as the electronic analogues of credit cards, share transfer forms, cheques, bills of lading and other negotiable instruments – are typically used in closed systems because of the requirement to provide safeguards against multiple spending. However, this appears to mean that in many cases they may not be accorded any specific legal effect by the directive, which might miss its main opportunity to influence liability issues.

A number of respondents made the point that businesses are not generally interested in identity but in ability to pay (the hotelier is interested in whether you have a credit card, not in whether you have a passport). Governments on the other hand are interested in identity because they operate many systems which can be defrauded by people who can successfully pretend to be more than one individual. Therefore, it is argued, the whole push for licensed CSPs is simply an attempt by governments to get industry to assume some of their costs by constructing a PK infrastructure of a kind that businesses does not really need at all.

We do not accept this completely. The most convincing example which we have found of an identity certificate being of importance in commerce is in applications for consumer credit. There may in the future be others, e.g. special offers which are intended to attract new customers and limited to one per person. However, in general, names are of much less interest to business than to government.

One respondent suggested a hybrid approach similar to the multifunction smartcard mentioned above: CSPs only certify identity, according to announced policy, and with strictly limited liability, while separate registries then add on authorisation certificates for each application. Another argued that the certification of identity and authorisation were fundamentally different and should be carried out by different organisations (the state and the private sector). On the other hand, many business respondents want their users to have keys that are not shared, and that are deployed rapidly off the back of existing customer management systems using certificates that are proprietary and low cost. There are both marketing and technical security reasons for having different keys (and if need be different smartcards) for different applications.

One respondent suggested that we should separate the issue of evidentiary acceptability from that of liability. In an ideal world we would support this; in practice some deal on liability may have to be made for the Directive to be accepted by the EU.

However, the most significant input we got from respondents on the issue of liability did not concern contract matters, such as value limits on the transactions for which a certificate was designed, but:

– matters of tort such as liability for defamation of someone who was wrongfully blacklisted;
– data protection issues such as liability for improper release of a name corresponding to a pseudonym ('What is the cost of infringing the privacy of a patient?');
– consumer credit issues such as whether liability disclaimers on a certificate could be used to defeat legislation such as the Consumer Credit Act in the UK which makes a credit card issuer jointly liable with the merchant for goods purchased from the merchant with the card.

We suggest that Article 6 be amended to clarify these issues.

7 Data Protection

A number of respondents expressed concern over more general tensions between the licensing of CSPs and data protection. For example, if the Directive's emphasis on unique names were to encourage governments, businesses or healthcare providers to set up identity numbering systems in countries where these have previously been culturally unacceptable, then this will seriously erode customer trust and could damage trade, industry and healthcare operations. One respondent expressed an even more general concern, namely that the directive would be a centralising force and would foster the creation of central databases of personal information generally; another feared that if the number of CSPs were to be small then cross-referencing such databases would be made somewhat simpler.

Specific concerns range from bank 'signature cards' to number and/or smartcard systems for health insurance in a number of member states. For these reasons, and because of the cost of compliance with data protection law, many businesses (especially in the healthcare sector) prefer to operate with de-identified data. The provision in Article 8 (4) that pseudonyms must be capable of defeat by law enforcement agencies has the potential to greatly complicate their operations. We recommend that such escrow provisions not be made mandatory but be a matter for member states.

Respondents have also remarked that the provisions of Article 8 (4) contain a loophole in that member states can avoid reporting the disclosure of a data subject's pseudonym by failing to close the investigation against him. We recommend that in any case the reporting of pseudonym disclosure become mandatory after a fixed period of time, possibly 3 years.

8 Consumer Rights

Many respondents commented that the Directive needs to take more account of consumer rights. Contracts between a member of the public and large organisations such as banks and software vendors have a tendency to be unfair because of the disparity in bargaining power, and mitigating the worst effects of this is widely accepted as a proper function of government at local, national and community level. Concern has been expressed that the Directive may have the effect of undermining this function.

In many previous cases of dispute, such as those between individuals and banks over 'phantom withdrawals' from automatic teller machines, the banks' defence has been to claim that their systems were infallible – that any dispute by a customer of a debit entry on a bank statement that was claimed to be for an ATM withdrawal must be mistaken or mendacious. Such sweeping claims by the banking industry have been undermined in the UK and the Netherlands by the conviction of criminals for ATM fraud, and in Germany by court appointed expert witnesses exploring vulnerabilities in the Eurocheque card system. However many banks wish to return to the status quo ante and each new technical development (such as the introduction of smartcards) tends to be seen as an opportunity to revive claims of technical infallibility.

In general, creating binding legal presumptions of certificate validity, without practical experience of large-scale usage, has the potential to cause great unfairness and injustice in many cases.

Previously, the Commission has tended to side with the consumer, and a recent report recommended that the sworn statement of a consumer that a transaction had not been made should be awarded equal weight to a claim by a bank's experts that it must have been. However, the current draft Directive appears to go in the other direction; provided a signature is supported by a qualifying certificate, there will be a strong presumption of validity. This is disturbing given firstly, the banks' record on consumer disputes; secondly, the fact that most electronic commerce implementations to date have a history of serious security bugs; and thirdly, that the certifiers proposed for the financial industry in a number of countries are far from being neutral between banks and customers but are rather consortia owned by the banking industry.

A single case of a person wrongfully convicted because of a bug, an operational blunder or a technical security breach (as has happened in at least one member state in the context of disputed cash machine withdrawals) could fatally undermine confidence in the system.

The best solution known to us is to limit the liability of the end user by legislation, the best example being perhaps 'regulation E' which governs electronic banking in the USA and has facilitated it by limiting customers' liability to \$50 except in cases of gross negligence. As the US is the EU's chief competitor in electronic commerce, Europe can afford no less. We therefore recommend the addition to Article 6 of a requirement that CSPs offer their users insurance against loss or theft of their private keys, or system failure or abuse arising otherwise than through the user's misconduct or gross negligence, on reasonable and non-discriminatory terms.

9 Evidence

The issue of disputed transactions leads naturally to the issue of evidence. In criminal trials especially (though also in civil matters), the defendant's right to examine and test all the evidence against him is strongly upheld in most member states. In the absence of such a right, claims of system infallibility place an intolerable burden of proof on the defendant. This causes difficulties for the prosecution when defendants demand the right to have their expert witness examine systems whose owners are not prepared to cooperate. Differing transparency traditions in different member states have the potential to inhibit trade, as evidence generated in one state may be relatively fragile in another.

One possible benefit of digital signatures is that, carefully implemented, they could greatly reduce the amount of the system that could have contributed to the creation of an item of evidence, and thus the transparency requirements and the scope for evidentiary challenge. However, some respondents were of the opinion that these benefits will not be fully realised without some official guidance.

The problem is how to accept electronic signatures as strong evidence without placing on defendants in both civil and criminal cases an impossible burden of proof, in the cases when misleading evidence is generated by some as yet obscure technical failure, or by the corruption of CSP staff, or by a failure which CSP staff discovered after the fact but decided to cover up for business confidence reasons. Some respondents take the view that the dilemma is insoluble; we tend rather to the view that experience will teach the courts how to deal with such cases provided that the first few cases are approached with a reasonably open mind. We therefore suggest amending Article 5 to direct member states that their implementations of this directive should not exclude challenges to specific signatures whether based on technical, operational or procedural arguments.

10 Agency

One respondent expressed concern about whether, under the proposed Directive, natural persons would be able to sign on behalf of organisations. Another respondent raised the problem of how we determine the extent to which someone who presents a business card from a given company can bind that company. The current business infrastructure does not generally attempt to solve this problem (although banks print books of the authorised signatures and powers of their officers and circulate these books to correspondent banks). If the future electronic trust infrastructure tries to impose a general solution for this problem, then it might give rise to substantial costs and complexity.

There are many possible scenarios, such as when an individual officer has full signing powers, where some quorum or authorised set of officers can sign, where an authorisation is restricted (as when an engineer can sign 1m ECU for lab equipment but may not sign at all for stationery), where a time-limited delegation has been arranged, where someone acts as an agent, and where an organisation is bound by a letter from its attorneys.

Furthermore, if individual as opposed to corporate keys can bind the company, then considerations of revocation and control generally would suggest that each company have its own CSP infrastructure. This would conflict with the desire of some member states to have few, large CSPs rather than many small ones.

Some respondents suggested that these matters should be clarified in Article 5. However, on the grounds of simplicity and consistency throughout the Directive, we suggest that Article 2 (2) be expanded to explicitly include natural persons signing on behalf of organisations, corporate seals that may be used by different persons at different times but which are kept under an organisation's control (for example, by virtue of being implemented as tamper-resistant processors locked in a data processing centre), and limited function signature means such as those used to implement delegation and dual control functions.

We finally recommend that the Commission monitor technical developments and seek to implement necessary changes in the regulatory regime through the standards process of Article 3 (3) where possible.

Appendix - suggested amendments

Here we summarise the amendments suggested in the above discussion.

1. Recital 9: replace 'exclusively' with 'primarily'
2. Article 2 (1) (b): delete
3. Article 2 (2) Insert the clause ', acting either for himself or for an entity that he is authorized to represent,' between the words 'who' and creates'
4. Article 2 (3) Insert after 'signatory' the words "or by persons authorised by the signatory"
5. Article 2 (3) and (4): replace 'device' with "means" (and make corresponding changes later in the text)
6. Article 2 (6): delete the words 'to the public'
7. Article 5 (2): add after 'electronic signatures' the words 'which satisfy the technical standards published in accordance with Article 3 (3) or'
8. Add to Article 5 the following new paragraph 3:
   '3. Member states shall also ensure that electronic means of authentication which currently have legal effect but which fall short of the definition of an electronic signature in Article 2 (1), are not rendered invalid by the implementation of this Directive.'
9. Add to Article 5 the following new paragraph 4:
   '4. Member States shall ensure that parties are afforded contractual freedom to agree among themselves on the terms and conditions on which they will accept data that is electronically signed, subject to applicable data protection and consumer protection law.'
10. Add to Article 5 the following new paragraph 5:
    '5. Member states shall ensure that their implementations of this directive do not exclude legal challenges to signatures based on qualifying certificates whether these arise on technical, operational or procedural grounds.'
11. Add to Article 6 the following new paragraph to be inserted between paragraphs 2 and 3:
    'Member states shall require certification service providers to offer their users insurance against loss or theft of their private keys, or system failure or abuse arising otherwise than through the user's misconduct or gross negligence, on reasonable and non-discriminatory terms.'
12. Add to Article 6 at the end of the current article 4:
    '... to counterparties to the transactions. However member states shall ensure that the certification service provider retains full liability for other claims, including those arising for defamation and for violations of data protection and consumer protection law.'

13. Article 7 (1) (b): replace 'same extent as its own certificates' with 'degree stated in the certificate'
14. Article 8 (4): replace 'shall ensure' with 'may require'
15. Article 8 (4): add 'or after a period of 3 years'
16. Annex I (b) delete
17. Annex I (d) replace 'device' with 'means'
18. Annex I (e) and (h) should be optional; there should be a second list headed 'Qualified certificates may contain' with these two items. The item currently numbered (h) should have prepended to it 'the certificate revocation policy, and any other'
19. Annex II: we suggest that these requirements be rewritten to acknowledge the likelihood that many small certifiers will not have expert staff on the premises and will not use expensive equipment. The most realistic requirement on such certifiers is that they carry insurance, or if one must be more specific, that they use products conforming with approved standards and in whose use they have been adequately trained. Failing a rewrite, we suggest deletion of items (b), (d) and (e), and the last seven words of (i).
    In any case, item (b) should have the word 'operate' replaced with 'provide', and item (f) should have the last clause replaced by 'guarantee the confidentiality of these keys during the process of generation and afterwards'.

28th October 1998