Towards a european framework for digital signatures and encryption

Vinje, Thomas; Julia Barcelo, Rosa

Published in:
Computer Law and Security Report

DOI:
10.1016/S0267-3649(97)82130-9

Publication date:
1998

Document Version
Publisher's PDF, also known as Version of record

ELECTRONIC COMMERCE

"TOWARDS A EUROPEAN FRAMEWORK FOR DIGITAL SIGNATURES AND ENCRYPTION"

THE EUROPEAN COMMISSION TAKES A STEP FORWARD FOR CONFIDENTIAL AND SECURE ELECTRONIC COMMUNICATIONS.

Rosa Julià-Barceló and Thomas Vinje

The growth of electronic communication depends on the ability of electronic messages to be confidential and secure. The need for confidentiality and security exists in a great variety of electronic communications, including, for example, electronic contracts (both business-to-business and business-to-consumer), electronic tax declarations, and electronic medical records. As described below, the main technological tools for ensuring the confidentiality and security of electronic communications are digital signature methods and encryption.
On 8 October 1997, the European Commission took a step towards establishing a European framework for digital signatures and encryption by issuing a Communication entitled "Ensuring Security and Trust in Electronic Communication: Towards a European Framework for Digital Signatures and Encryption".[1] The Communication is divided into three sections. First, it deals with the elaboration of a framework governing the entities that issue the certificates establishing the basis for digital signatures (so-called certification authorities) and the legal recognition of digital signatures. Second, it addresses encryption, including export control measures and law enforcement requirements. Finally, the Communication discusses the legal basis for a Commission initiative in these areas and the scope and timeframe of such an initiative.
After providing an introduction to the relevant technology, this article will provide a brief description and analysis of the main topics discussed by the Communication, focusing particularly on digital signatures and certification authorities.

AN INTRODUCTION TO THE TECHNOLOGY

Both 'digital signatures' and 'encryption' are based upon cryptographic technology. Indeed, a digital signature is essentially an *encrypted* message accompanying an electronic document. However, as described below, digital signatures and encryption have different functions and usually are based on different types of cryptographic techniques.

'Encryption'

As used in the Communication, 'encryption' is the term employed to describe the symmetric-key systems used to achieve the *confidentiality* of electronic communications. By exchanging messages encrypted using symmetric cryptosystems (described below), communicating parties seek to ensure that they (and only they) will be able to read the content of the messages.

With symmetric-key systems, both sender and recipient use the same 'key' to encrypt and decrypt messages: the sender encrypts a message with the symmetric key and sends it to the recipient, who possesses the same key and who will use it to decrypt the message (i.e. return it to plaintext). In order for the communications to remain confidential, the key must remain secret. This means the parties must have a secure way to exchange the key. As the Communication notes, this is cumbersome in an open environment where many participants do not know one another.

Although the Communication uses the term 'encryption' to describe only systems using symmetric-key systems, it is also possible, as described below, to achieve confidentiality of communications using asymmetric cryptography.

'Digital signature' technology

Whereas encryption, as that term is employed in the Communication, is used to achieve confidentiality, digital signature technology is used to achieve integrity and authenticity of the data, i.e. *security* of electronic communications. By using digital signature technology, the recipient of an electronic communication can be confident that the sender of the communication is actually who they purport to be (this is often referred to as the 'authenticity' function of digital signatures). The communicating parties can also ensure that the communication received is the one that actually was sent (this is often referred to as the 'integrity' function of digital signatures).

Digital signature technology is based on *asymmetric* cryptosystems, where different keys are used for encryption and decryption. With asymmetric systems, each party is allocated two different keys. One key is used to transform certain data into a seemingly unintelligible form. That data is attached to an electronic document, and it effectively constitutes the 'digital signature' itself. Another key is used to verify a digital signature by returning that data to its original, intelligible form. In other words, the sender of an electronic communication 'signs' it digitally by attaching to it certain data encrypted using one key (much like the author of a traditional paper document signs it by affixing his handwritten signature to it). The recipient of the electronic document ensures the validity of the digital signature by decrypting the data using another key.

The key used for creating the digital signature — the signature key — is called the *'private key'*, because it is available only to the signer. Unless the key has been stolen or otherwise compromised, nobody else has access to this private key, and hence nobody else can digitally sign a message in the same way.

The second, signature verification key is called the *'public key'* because usually it is made available to the general public, for example through a directory of public keys. This key, when applied to digital signatures created by the key holder's individual private key, will decrypt those signatures — and *only* those signatures. Thus, the public key will *not* recognize the digital signature of any other person.

Because a particular public key can verify only digital signatures created using its holder's private key, and because (absent compromise of the key) the sender of a message is the only possessor of the private key, the recipient of a message who successfully verifies its accompanying digital signature using the sender's public key can be confident that the message is *authentic*, i.e. that it was sent by the person who purported to send it. Moreover, after applying the public key to the encrypted message, the recipient can compare the resulting text with the plaintext included in the message. If they are the same, the recipient can also be confident about the *integrity* of the message (i.e. that the message has not been altered in transit).

In most public key techniques, a one-way algorithm (a so-called hash algorithm) is applied to an electronic message to produce a condensed version of it. This condensed version of the message (the 'message digest') is then 'signed' (encrypted) with the sender's private key. In effect, this encrypted message digest is itself the 'digital signature'.

Because the hashing method is a one-way function, the message digest cannot be reversed by the recipient to obtain the full message itself. Therefore, the encrypted message digest (the digital signature) is accompanied by the full text of the message in unencrypted form. Upon receipt, the recipient processes the unencrypted message text with the same hashing algorithm as was used to create the message digest, and compares the resulting message digest with the original one the sender sent along with the message (which, of course, the recipient has decrypted using the sender's public key). If the unencrypted message was altered in any way during the transit, the two digests will be different, thus revealing that alterations were made.[2]

With respect to the authenticity of a message, the recipients can be confident about the identity of the sender only if they are confident that the private key remains in the sole possession of the person with whom they believe they are communicating and that the party with whom they are communicating is actually the one he purports to be. Thus, the key system must allow the recipient of an electronic communication to ensure that the private key has not been compromised. For example, a pharmacy must be able easily to check whether a physician's private key has been stolen or otherwise compromised before filling an electronic prescription issued by that physician. Moreover, it is often important for the system to allow a recipient of an electronic communication to ensure not only that the party with whom the recipient is communicating is really the one they are believed to be, but also that they have certain characteristics. For example, a pharmacy may need to establish that the holder of a particular key is actually a physician before accepting his digital signature on an electronic medical prescription. As described below, both of these objectives can be established through the activities of certification authorities.

It is common practice to include the public key along with an electronic communication. However, this approach does not provide sufficient confidence about the integrity of the private key. Although the recipient *can* use a public key accompanying the communication to decrypt the signature, the only way to gain real confidence in the digital signature is to retrieve the public key from a trustworthy database and to decrypt the digital signature using that public key. The fact that a public key is included along with a communication, and that it can be used to decrypt the digital signature, does not, after all, mean that the private key remains in the sole possession of the proper key holder.

As described below, this highlights one of the more important functions of certification authorities, namely the establishment and maintenance of key databases. By issuing certificates to key holders and by creating and updating key databases, certification authorities play an essential role in establishing a trustworthy system whereby message recipients can verify the integrity of the private key and the characteristics of the key holder.

Thus, the digital signature fulfils the same basic authenticity and integrity functions as the manual signature. Indeed, with a well-structured and managed public and private key system using secure algorithms and sufficient key lengths, it is virtually impossible to tamper with a digital signature, so the digital signature is actually far more reliable than the manual signature.[3] A system of commerce based on electronic documents and digital signatures thus has the potential to provide more security than ever before.

As noted above, asymmetric cryptography can be used not only to achieve authenticity and integrity through digital signature technology, but also confidentiality. Indeed, electronic communications accompanied by digital signatures are often encrypted using the public key of the recipient. Thus, the recipient — and only the recipient — can use his private key to decrypt the communication.

The role of certification authorities

As noted above, the trustworthiness of digital signatures, and thus their value in electronic commerce, lies in the *reliability*

of the keys. In an open environment, the requisite reliability of keys can be achieved mainly through the establishment of a legal regime governing independent 'certification authorities' who provide (1) the necessary assurances of identity by issuing certificates binding public keys to the identity of their owners and (2) the requisite confidence that keys have not been compromised through the establishment of a trustworthy database maintaining an up-to-date list of valid keys.[4]

In order to provide confidence to communicating parties about the identity and characteristics of a key holder, the certification authority must obtain and verify certain information for the certificate. For example, a physician applying for a certificate must provide an adequate demonstration of his personal identity and of his status as a licensed physician. After obtaining and verifying such information, the certification authority creates a certificate containing, *inter alia*, the party's public key,[5] the identity of the key owner, a serial number, and the identity of the certification authority. Then, a hash function is applied to this information and it is signed by the certification authority with its private key. This 'signature' is then attached to the same information in unencrypted form in order to form the complete certificate. Thus, the certificate has two parts: the unencrypted, full-text information, and the digital signature of the certification authority.

Such certificates enable communicating parties to achieve confidence about the identity and status of the parties with whom they communicate as follows: when Party A enters into a transaction with Party B by sending Party B a message digitally signed by Party A, he also sends along with the message the certificate issued by the certification authority. Because the certificate contains Party A's public key, signed by the certification authority, and because the certification authority's public key will always be available in a public database, Party B can use the certification authority's public key to verify the certificate sent along with the message by Party A, thus enabling Party B to verify Party A's message.

As noted above, the second main function of certification authorities is to provide confidence that keys remain valid. To do so, they must establish a reliable key database, including a certificate revocation list. This is a list indicating certificates that are no longer valid because, for example, the private key has been stolen or otherwise compromised. Thus, when someone receives an electronic communication purportedly signed by a particular person, he can confirm, by reviewing the certificate revocation list, that the certificate remains valid.

ESTABLISHING A LEGAL FRAMEWORK FOR CERTIFICATION AUTHORITIES

At present, certification services are offered in Europe by only a few private companies active in the field of computer security and whose establishment and operation is not subject to any legal framework.[6] Because certification authorities will have a vital role to play in establishing a reliable system for electronic commerce based on digital signature technology, the growth of this sector will depend on the adoption of an appropriate, albeit not overly bureaucratic, legal regime that will generate trust in the activities of certification authorities.

To the extent the legal regime engenders more trust in certification authorities and the use of digital signatures, for example by providing greater evidentiary value to electronic documents accompanied by digital certificates, electronic commerce in general will be encouraged. Moreover, cross-border electronic commerce will flourish only if certificates issued in one Member State are recognized in all other Member States and if the legal regimes governing the activities of certification authorities are reasonably harmonized.

The creation of an appropriate legal regime governing the establishment and operation of certification authorities would have other favourable consequences. It could provide a basis for the growth of electronic commerce in a global context, beyond the borders of Europe, and provide appropriate consumer protection in the context of certification services.

The Communication addresses three especially timely questions with respect to certification authorities:

- How can the EU-wide legal recognition and trustworthiness of digital certificates be established?
- Should the legal framework governing the establishment and operation of certification authorities be based upon a licensing system or a non-licensing system, or both?
- What liability regime should govern the activities of certification authorities?

How to achieve the EU-wide recognition and trustworthiness of digital certificates?

The Communication suggests that the establishment of an EU-wide legal framework providing certain basic requirements for the establishment and operation of certification authorities would provide the basis for requiring the mutual recognition of certificates among Member States. In other words, once such a common legal framework is established, a certificate issued in one Member State would have to be recognized in all other Member States. The Communication provides some examples of fields where common requirements could be specified, including:

- security of the certification authority and compliance with data protection legislation;
- reliable identification of certificate applicants (to ensure that applicants are properly identified);
- minimum insurance coverage (to cover cases where the certification authority is liable, for example, for misidentifying a certificate applicant);
- technical obligations (for example, to ensure that the applicant's private and public keys employ adequate, up-to-date, encryption technology), and
- qualifications and security-testing of personnel.

It would seem that the areas identified by the Communication for possible inclusion in a Community legislative instrument governing certification authorities are, in general, appropriate matters for such legislation to address — although it would be wise also to consider legislation for achieving interoperability between certification authorities. Moreover, the goal of establishing a harmonized regime setting minimum criteria for the establishment and operation of certification authorities, and the application of the mutual recognition principle to certificates issued by authorities complying with such a regime, is a laudable one. In addition, the Communication seems to suggest the establishment of a flexible regime that would permit room for experimentation in this new area, avoiding the creation of heavy bureaucratic obligations.

Should this legal framework be based on a licensing system, non-licensing system, or both?

One of the key questions to be addressed in connection with creating a harmonized regime for the establishment and operation of certification authorities is whether certification authorities would have to be licensed, and whether a Member State requiring licensing would have to accept certificates issued by a non-licensed authority in a Member State having no licensing obligation. As the Communication indicates, some Member States are now in the process of introducing voluntary schemes for the establishment and operation of certification authorities, while others regard mandatory licensing schemes as essential to the building of trust in certification authorities and digital signatures.[7]

The Communication accepts that licensing regimes might be appropriate. However, it also accepts the possibility of non-licensing approaches. Indeed, it says: "Licensing is only one of the possible trust-enhancing methods Member States may apply to promote the use of legally valid digital signatures. Non-licensed, but highly regarded private or public organizations may as well be considered as a trusted CA."

Thus, the Communication concludes that the EU regime governing certification authorities should allow for "the coexistence of licensed and non-licensed CAs". It is not clear precisely what this coexistence would entail, but it seems that a Member State with a licensing system would have to accept certificates issued by non-licensed authorities from Member States without licensing systems. However, authorities in all Member States would have to comply with the minimum criteria governing certificate authorities' establishment and operation provided for in the EU legislation.

The Communication's 'coexistence' approach would seem to be a wise one. Given the infancy of this area of business, flexibility should be provided for experimentation. For example, it might be appropriate to limit licensing obligations only to those certification authorities providing services to the public (as suggested for the UK) and for closed user groups to be exempted from any licensing requirement. The fundamental goal should be to establish a balance between imposing sufficient legal obligations on the establishment and operation of certification authorities to engender trust in the use of digital signature technology, while allowing scope for technology and business practices to develop.

Which liability regime should apply?

The Communication says, correctly, that having "clear liability rules would contribute to the acceptance of CA services". However, the Communication fails to define clearly the standard it envisions for liability. In addressing liability issues, one should distinguish among the following actors: (1) the certificate-holder; (2) the certification authority; and (3) the third party who receives (and relies upon) the certificate.

With respect to the certification authority's potential liability to the certificate holder, who presumably will have a contractual relationship, the Communication seems to indicate that the certification authority's standard of liability will depend on the terms of the contract. The Communication goes on to indicate that a "catalogue of requirements" could form the basis of the contractual duties, providing both minimum and maximum liability of the certification authority. However, the Communication does not indicate which requirements this 'catalogue' might contain, nor whether this catalogue would be binding by law, nor whether the legal regime governing certification authorities might prohibit the contractual exclusion of liability in certain circumstances, perhaps as a matter of consumer protection. For example, should a certification authority that fails to publish the revocation of a certificate after proper notice by the certificate holder of the theft of his certificate be able to exclude liability for damages incurred by a certificate holder when his certificate is then used by a thief?

With respect to extra-contractual liability, both between the certification authority and third parties who rely on a certificate and between certificate holders and such third parties, the Communication is silent. It would seem appropriate for any regime governing the operation of certification authorities to address this issue, and to establish a liability regime creating an appropriate balance between these actors.

Under usual tort rules, the person who suffered damage in reliance on a certificate would bear the burden of demonstrating the lack of due care of the certification authority. However, given the very specialized technological aspects involved in issuing and maintaining a certificate, this burden could be exceedingly difficult to meet. Therefore, a solution that establishes a reversal of the burden of proof might be appropriate. Under this approach, the certification authority would have the burden of proving its lack of negligence. Perhaps such a reversal of the burden of proof would likewise be appropriate in the context of contract cases between certification authorities and certified parties.

This approach is likely to be adopted by the United Nations Commission on International Trade Law (UNCITRAL) in a new model law on certification authorities to complement the Model Law on Electronic Commerce.[8] The UNCITRAL draft also proposes a liability presumption, as is provided in the Product Liability Directive for defective products, which can be rebutted by the certification authority by showing it has fulfilled certain requirements (for example, by demonstrating it acted with diligence in ascertaining the key holder's identity).

The German Digital Signature Act does not provide a special rule on liability; therefore, general rules will apply.[9] To the contrary, the UK's Public Consultation Paper suggests that certification authorities should be subjected to a strict liability regime attenuated only by liability caps on compensation.[10]

One specific issue should be mentioned concerning the obligation of the certificate holder, namely the obligation to maintain the secrecy of the key and immediately to notify the certification authority of any key compromise. Although some authors have criticized the notion that the certificate holder should bear the risk of loss until such time as it has notified the certification authority of a key compromise,[11] this would seem to be the only workable method of allocating this risk. It would seem inappropriate to impose any liability upon the certification authority until it has received such notice, though it would, of course, be useful for certification authorities to educate certificate holders about the importance of carefully maintaining certificate and key integrity. In addition, technological measures, such as smart-

cards provided with biometric devices, might reduce the risks associated with key and certificate loss and theft.

LEGAL RECOGNITION OF DIGITAL SIGNATURES

Digital signatures cannot play their proper role in facilitating electronic commerce unless they are legally recognized. In other words, digital signatures must be legally equivalent to hand-written signatures before they can become an effective business tool.

Unfortunately, as the Commission points out in its Communication, digital signatures are not yet accorded appropriate legal recognition. EU Member State laws currently impose requirements of handwritten signatures and 'written documents' as conditions of contractual validity, enforcability and evidentiary admissibility and weight.[12] These requirements vary from EU Member State to Member State, both in their terms and their specific purposes.

In many legal systems it is common to find a requirement that certain contracts or administrative acts must be in written form and must be authenticated by hand-written signatures. Under this approach, for example, certain contracts are invalid or unenforcable unless they are documented in writing and accompanied by a hand-written signature, often for consumer protection purposes.[13] In others, documentary evidence to which signatures are affixed is accorded more evidentiary weight than other forms of evidence,[14] and it is unclear whether digital signatures will qualify for such favourable treatment. Moreover, even in countries where documentary evidence is not formally accorded privileged status, courts are not always willing to accord the same evidentiary value to electronic documents accompanied by digital signatures as to their conventional counterparts accompanied by hand-written signatures.

Because digital signatures can provide at least the same degree of confidence as to the authenticity and integrity of a document as can their hand-written counterparts, this is an anachronistic situation. As the Communication notes, "in order to achieve as wide as possible acceptance of digital signatures, national legal systems may need to be adapted to ensure that they offer the same recognition and treatment to digital signatures as conventional signatures".

In our view, to facilitate the development of electronic commerce, EU harmonization legislation should establish the legal recognition of digital signatures. The Communication seems to embrace this proposition, indicating that the Commission intends to undertake an ongoing assessment of the need to provide for the legal recognition to digital signatures at Community level.[15] In pursuing this course, the Commission is following in the footsteps of several international organizations that have suggested steps be taken to accord appropriate legal recognition to new authentication and integrity mechanisms (e.g. UNCITRAL, Tedis Programme, Council of Europe, and Working Party 4 on Facilitation of International Trade Procedures of the United Nations Economic Commission for Europe).[16]

As the Communication correctly points out, any such legal regime should be sufficiently flexible to anticipate future technological developments. While it should accord today's digital signatures the same recognition as conventional signatures, it should adopt a technologically neutral approach that would apply also to new means of providing authentication and integrity. Indeed, the law should not provide for the technology-specific recognition of current digital signature technology, in part because that technology might one day no longer provide adequate security. Technological progress might lead to a situation where the current form of public key cryptography discussed above no longer ensures integrity and authenticity (for example, because computer capacity rises to the point where it is possible rapidly to discover a private key from the public key or because certain encryption algorithms no longer provide security because the mathematical problems underlying them are resolved). Moreover, specifically legislating for today's technology would discourage the development of new technologies.

Thus, the European Commission and the Member States should immediately begin the process of identifying, analysing and cataloguing their various legal requirements whereby digital signatures and electronic documents are disadvantaged vis-à-vis their traditional paper counterparts. Then they need to undertake the difficult task of devising a new, harmonized, approach to such requirements that is no longer formulated in the terminology of the traditional world of paper documents and that will accord appropriate legal recognition to digital signatures and their technological descendants. This standard should identify the requisite level of authenticity and integrity required for particular *types* of documents (whether traditional or electronic) and establish technologically neutral standards according to which *any* manner of providing the requisite authority and integrity will be accorded equal legal recognition.[17]

One important question arising in this context concerns the role of certification authorities. As the Communication also acknowledges, the legal effects of documents signed with digital signatures may be implicitly linked to the trustworthiness of certification authorities. Indeed, to the extent certification authorities, for example, ensure the connection between the public key and the key holder, they enhance the value and trustworthiness of digital signatures.

However, should the new legal standards (mentioned above) governing the requisite level of authenticity and integrity demand for every type of document the involvement of a certification authority? For example, should the law require, as some have suggested, that an electronic document will qualify as a 'written document' for evidentiary or other purposes only if it is accompanied by a digital signature that has been recognized by a certification authority that has fulfilled certain requirements governing its establishment and operation? In our view, such a condition would seem misplaced, at least in certain contexts. For example, companies that regularly do business with each other electronically might well choose to do so by privately exchanging keys and avoiding the expense and burden of using a certification authority. It would seem inappropriate to deny equal legal recognition to digitally signed electronic documents exchanged in such circumstances. Perhaps the law might provide that digital signatures certified by a licensed certification authority would be accorded *prima facie* legal recognition, but it would allow those relying on other digital signatures to prove their validity by establishing the security and reliability of the system and signature in question.

Electronic documents accompanied by certified digital signatures provide a much higher degree of authenticity and integrity than do most conventional documents accompanied by handwritten signatures. Thus, requiring an electronic document to be accompanied by a digital signature certified by a certification authority before that document would be accorded legal recognition would impose a much higher burden on digital signatures than has traditionally been imposed on conventional signatures. For many, perhaps most, electronic documents, it would seem inappropriate to impose such a high standard of authenticity and integrity.

Indeed, requiring an electronic document to be accompanied by a digital signature certified by a certification authority would seem to be akin to requiring a hand-written signature to be notarized. In so far as not all conventional documents need be notarized in order for them to be valid or enforceable, why should electronic documents require the affixation of a digital signature certified by a certification authority in order for them to be recognized? Perhaps an appropriate solution would be to require the involvement of a certification authority only in cases where the involvement of a notary would be required in the context of a conventional document and where communications are made with public authorities such as tax and social security authorities.

In any event, a functional, technology-neutral approach should be taken that provides courts with flexibility to accept new technological forms of providing authenticity and integrity. However, this approach is specifically formulated, it should ensure (at least over the near term) that an electronic document will be accorded the same legal recognition as a traditional paper document accompanied by a handwritten signature if it is accompanied by a digital signature and a certificate issued by a certification authority established and operated according to the requisite standard.

'Public' electronic documents might be deemed to fall within a special category, and perhaps they would be legally recognized only if accompanied by a certificate issued by a licensed certification authority. Although notaries are unlikely to welcome this prospect, one might ask whether certification authorities indeed have a vital 'notarial' role to fulfil in the digital future, and whether certification authorities might take over much of the role of notaries in the electronic world. If so, how can we ensure that the licensing requirement is not used to limit the number of certification authorities, and thereby to restrict competition among certification authorities?

REGULATION OF ENCRYPTION

We now turn to the other main topic addressed by the Communication, namely encryption. Because encryption has been the topic of considerably more debate and commentary than have digital signatures, we will comment only briefly on this section of the Communication.

As the Communication correctly recognizes, the development of electronic commerce and many other applications of the Information Society will depend on the ability cost-effectively to maintain the confidentiality of electronic communications.[18] The Communication provides several examples where this requirement of confidentiality is particularly clear, including tele-shopping and tele-banking (where consumers must be assured that personal data such as credit card numbers are kept confidential); sensitive business communications such as project bids, research results, and the like (where companies must be protected against industrial espionage); and health care telematic applications (where patients must be protected against the unauthorized disclosure of their medical records). As noted above in the section introducing the technology, *symmetric* encryption systems are currently the main way of achieving the confidentiality of electronic communications.

As most readers will already know, a lively debate has been under way regarding the regulation of encryption, and the Commission takes a clear and enlightened position with respect to the main issues in this debate. In particular, the Communication addresses the following issues:

- Export control measures.
- Domestic control measures.
- Key escrow and key recovery systems.
- Privacy considerations.

Export Control Measures

As the Communication notes, certain export controls have been imposed on encryption in an effort to deny foreign opponents the benefits of strong cryptography. Internationally, such controls have been imposed under the so-called Wassenaar arrangement,[19] which replaced the COCOM list. Exports of certain encryption technologies are controlled within the European Union under the Dual-Use Regulation of December 1994.[20] As pointed out by the Communication, in so far as the Dual-Use Regulation permits controls on shipments of cryptography products from one Member State to another, it can lead to distortions in the functioning of the Single Market.

With respect to policy actions to be taken in the export control area, the Communication does not suggest any actions with respect to the Wassenaar arrangement, probably because the Commission did not wish to be seen to be exceeding the bounds of its authority in sensitive national security matters. However, the Communication does, fortunately, suggest that the Dual-Use Regulation should be liberalized.[21] In particular, the Communication suggests the progressive elimination of intra-Community controls on commercial encryption products.[22]

Domestic Control Measures

Compared with export controls on encryption, domestic control of encryption is, as the Commission notes, relatively rare. Among EU Member States, only France has a comprehensive cryptographic regulation. However, intense debates are under way in several European countries (and the United States) concerning the possibility of adopting such legislation. As noted by the Communication, national law enforcement authorities and national security agencies favour domestic encryption controls because they fear that the widespread use of encrypted communications will diminish their ability to fight crime and prevent terrorism.

The Communication notes that proposed domestic control mechanisms could make the use of encryption (or at least certain forms of encryption) illegal unless it has been authorized. Alternatively or additionally, supply and import of encryption products and services (or *certain* products and services, such

as those employing strong encryption) could be placed under an authorization scheme. The main aim of such regimes is to ensure that encryption available to users either is relatively weak (i.e. practically useless) or subject to legal access by governments through key escrow or similar schemes.

The Communication is refreshingly blunt in its assessment of such domestic control mechanisms. Basically, it points out that such mechanisms would be futile and counterproductive. They would not prevent criminals from using effective encryption technology, but "could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks".[23] Moreover, such regulations could, by establishing different rules governing the use and sale of encryption technologies, create obstacles to the functioning of the Single Market — and this provides an important constitutional basis for Commission initiatives in this area. In addition, the formulation of laws regulating encryption will have a direct effect on privacy and freedom of speech and association. We can only hope that the Member States will realize the wisdom of the Commission's hands-off approach to encryption regulation.

Key escrow and key recovery systems

Key escrow and key recovery systems are among the methods that have been suggested for policing the use of encryption in connection with illegal activities. Under a key escrow system, a copy of the relevant key would be provided either directly to a law enforcement agency or to a so-called 'trusted third party' that could be required to release the key to government agencies under certain circumstances. Under a key recovery system, information about the key is provided to the government or the trusted third party that would allow the law enforcement agency to 'recover' the key if necessary to crack a message for police purposes.

The Communication adopts an appropriately negative position with respect to key escrow and key recovery systems. As the Commission points out,[24] such systems would be ineffective for law enforcement purposes, in so far as they would be easily circumvented. At the same time, key escrow and key recovery systems would significantly diminish the attractiveness of encryption to users. Obviously, any involvement by a third party in confidential communication increases its vulnerability, and thus diminishes trust in the confidentiality of electronic communication. In this connection, serious privacy concerns arise as well. Moreover, key escrow and key recovery systems would impose significant costs on the use of encryption, especially were such systems to be implemented on a global scale. In short, the adverse consequences flowing from the imposition of key recovery or escrow systems would, without providing any real law enforcement benefit, hinder the development of electronic commerce.

Privacy

While acknowledging that national security and law enforcement considerations can sometimes trump privacy rights, the Communication notes the importance of encryption to maintaining privacy. In particular by employing encryption methods, 'data controllers' can fulfil their obligations under the EC Data Protection Directive to protect personal data.

Most pointedly, the Communication hints that the Commission might use the EC Data Protection Directive and the Commission's power to enforce EC rules on free movement of goods and services to attack certain legislation hindering the use of encryption. As the Communication notes, the free flow of personal data throughout the Internal Market depends on the ability of encryption methods to 'travel' with the personal information they are securing. Thus, differing Member State rules regulating encryption could lead to obstacles in the flow of information, and thereby to the restrictions on the flow of goods and services among Member States. As the Communication puts it, "any regulation hindering the use of encryption products and services throughout the Internal Market thus hinders the secure and free flow of personal information and the provision of related goods and services".[25]

Commission's policy orientations

In laying out its policy orientations on encryption, the Commission, while acknowledging the competence of Member States with respect to national security and law enforcement, indicates that it may not hesitate to take action against encryption regulations that infringe EC law, including EC law on free movement of goods and services and data protection. In this connection, the Communication notes that Member States are obligated to notify the Commission of new national rules that might create Internal Market obstacles, and indicates that such notifications might provide the basis for Commission action.[26]

This policy orientation is certainly to be welcomed. Undoubtedly the Commission is correct that there will be no internal market for electronic commerce without an internal market for cryptography. Harmonization of Member State rules on cryptography to avoid regulatory inconsistencies is vital, and the Commission has an essential role in achieving this task.

In addition, the Communication's international orientation is important. As the Communication notes, the global nature of electronic commerce will require the European Community to seek an internationally compatible framework for digital signatures and encryption, including the establishment of international technical standards (necessary for interoperability) and mutual recognition of certificates on an international basis. We can hope that the Commission will promote its enlightened cryptography policy with its major trading partners, as well as in international organizations like the WTO and OECD.

As far as its future programme is concerned, the Commission intends to organize an international hearing on the questions addressed in the Communication during the first quarter of 1998 and to make a proposal for further action (perhaps including a directive on digital signatures) during the second quarter of 1998. Finally, and appropriately ambitiously, the Communication sets a target of the year 2000 for establishment of a common European framework for cryptography.

CONCLUSION

A refreshing wind is blowing from Brussels. For the first time since the debate began over cryptography, an official government communication has clearly acknowledged the need for the legal recognition of digital signatures on a global scale

and for the unhindered public availability of strong encryption. Promptly implementing the policy objectives laid out in the Communication would establish some of the main conditions to the deployment of electronic commerce and the broader development of the Information Society in Europe.

Rosa Julià-Barceló is researcher at the Centre de Recherches Informatique et Droit, Namur, Belgium. **Thomas Vinje** is managing partner of the Morrison & Foerster LLP Brussels office and a Report Correspondent.

Morrison & Foerster LLP
Avenue Moliere, 262
1180 Brussels, Belgium
Tel: +32 2 347 0400
Fax: +32 2 347 1824

Footnotes

[1]COM (97) 503 (hereinafter 'Communication'). This communication was foreseen in April 1997 by the Commission's communication entitled "A European Initiative in Electronic Commerce". (COM (97) 157 final, 16.4.97). DGXIII issued a Green Paper on the same subject on April 24, 1994 entitled "Green Paper on the Security of Information Systems", but no further action was taken at this time.

[2]See US Congress, Office of Technology Assessment Issue Update on Information Security and Privacy in Network Environments, Washington, DC, 1995, at 49.

[3]The ability to discover the private key from the public key is increasing as technology (and computing power) progresses. Therefore, the length of key necessary to obtain a reliable digital signature should be under constant review, as must the continued security of the relevant algorithm. Furthermore, technology must also ensure the security of the network. The management of the keys must occur in a secure environment.

[4]In the past, most publications have used the expression 'trusted third party' to cover both certification authorities and key escrow and recovery agents. However, the Communication, in accordance with the OECD Guidelines for Cryptography Policy (27 March 1997), uses the words, 'certification authorities' for those entities carrying our integrity services and uses the term 'trusted third party' exclusively for those bodies carrying out services relating to lawful access to encryption keys (key escrow and key recovery).

[5]Usually the certificate applicant generates his own private and public keys, and provides them as part of his application to the certificate authority, but it is also possible to set up a system where the certification authority generates the key pair.

[6]For example, in Belgium the company Isabel provides certification services within the banking sector and Belsign provides such services more broadly.

[7]See Section VI (Structure of the Proposals), Paragraph 43 of the Public Consultation Paper on Detailed Proposals for Legislation "Licensing of Trusted Third Parties for the Provision of Encryption Services" (UK Department of Trade & Industry, March 1997). Although the German law on digital signatures sets up a licensing system for certification authorities (see δ 4 of the Digital Signature Act), this system does not appear to be mandatory.

[8]See (A/CN,9/437), A/CN,9/WG.IV/WP.71, and A/CN.9/WG.IV/WP.73.).

[9]In the legislative discussion prior to the approval of Digital Signature Act, it was decided, because of the novelty of the issue, to refrain from including a special provision on liability but to analyse in the future whether special liability rules would be appropriate.

[10]See Section VI (Structure of the Proposals), Paragraph 43 of the Public Consultation Paper on Detailed Proposals for Legislation "Licensing of Trusted Third Parties for the Provision of Encryption Services" (UK Department of Trade & Industry, March 1997).

[11]Wright, B., Eggs in baskets: distributing the risks of electronic signatures, *The John Marshall Journal of Computer & Information Law*, Vol. XV, No. 2: 189-201 (1997).

[12]See Lamberiere, I., La valeur probatoire des documents informatiques dans les pays de la C.E.E., *Revue Internationale de Droit Comparé*, No. 3 (1992).

[13]For example, Article 1341 of both the Belgian Civil Code and the French Civil Code requires written evidence when the value of the contract (for example, a sales contract) is beyond a certain limit.

[14]E.g. Germany. For further comments on this particular issue, see Blechschmidt, R., The German Basic Electronic Data Interchange Model Agreement Versus the European Model EDI Agreement: Some Reflections on German Law, *The EDI Law Review*, No. 3, 1996, at 107-124.

[15]Communication, Section IV.1.2(ii).

[16]For UNCITRAL, see 1995 Recommendation (A/40/17), UNCITRAL Model Law for Electronic Commerce of 14 June 1996 (A/51/17). For TEDIS, see TEDIS- Situation Juridique des Etats Membres au regard du transfers électronique de données, Bruxelles, Commision des Communautés. For Trade Facilitation Working Party of UN/ECE see Recommendations UN/EC No.12; UN/EC No.13; UN/EC No.14.

[17]A similar *functional* approach is embodied in Article 7 of the UNCITRAL Model Law for Electronic Commerce.

[18]Communication, Section III.1 (iii).

[19]Wassenaar arrangement on export controls for conventional arms and dual-use goods and technologies (Dec. 19, 1995).
http://www2.nttca.com:8010/informofa/press/c_s/wassenaar.html;http://ideath.parrhesia.com/wassenaar/wassenaar.html.

[20]Council Regulation (EC) 3381/94, 19.12.94. Council Decision 94/942/CFSP, 19.12.94, OJ L 367/8 (31.12.94), establishes the lists of dual-use goods covered by the Regulation.

[21]Communication, Section IV.2(ii).

[22]Id.

[23]Communication, Section III.2.1.

[24]Communication, Section III.2.3.

[25]Communication, Section III.2.4. See also Communication, Section III.3(v).

[26]In this regard, it is worth noting that the French Government has notified the Commission of its pending encryption proposals.