CCBE POSITION ON ELECTRONIC IDENTIFICATION, AUTHENTICATION AND SIGNATURES

Conseil des barreaux européens – Council of Bars and Law Societies of Europe
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail ccbe@ccbe.eu – www.ccbe.eu

CCBE Position on electronic identification, authentication and signatures

The Council of Bars and Law Societies of Europe (CCBE) represents around 1 million European lawyers through its member bars and law societies from 31 full member countries, and 11 further associate and observer member countries. The CCBE responds regularly on behalf of its members on policy issues which affect European citizens and lawyers. In this submission, the CCBE responds to the public consultation that has been launched by the European Commission on electronic identification, authentication and signatures.

Since the questionnaire is largely directed towards the gathering of information and views at a member state or regional level, and owing to the diversity regarding the take-up and use of digital signatures amongst CCBE's member bars and law societies, it is not practicable for the CCBE to seek to answer the questionnaire. Accordingly, instead of responding to the specific set of 29 questions, the CCBE wishes to draw the Commission's attention to a number of more general issues and points of concern from the legal profession's point of view.

As a preliminary observation, the CCBE notes that there is some confusion caused by the terminology used in the questionnaire, which, throughout, refers to "e-signatures". The Electronic Signatures Directive (1999/93/EC) distinguishes "electronic signatures", "advanced electronic signatures" and "qualified electronic signatures", the latter two being what is more popularly known as "digital signatures". It is apparent from an examination of the questionnaire that the subject matter of the consultation is almost exclusively digital signatures rather than simple electronic signatures, and the present response proceeds upon that basis.

The CCBE welcomes the European Commission's proposal to review the existing Electronic Signature Directive and to prepare a planned initiative on the mutual recognition of electronic identification and authentication. Although not being in a position to comment upon any of the claimed advantages to business and commerce from such a review, the CCBE is concerned to ensure that any such review of the Directive will assist and facilitate the development of effective eJustice systems and hence also the improvement of access to justice in Europe. It stresses, however, that any solutions proposed both respect principles of subsidiarity and are proportionate, with the focus being on interoperability rather than harmonisation as such. Digital signatures and other forms of electronic identification and authentication are often used to a greater or lesser extent in a number of jurisdictions to enable lawyers to perform a wide range of operations, such as filing documents with the courts and public administrations or conducting cross-border proceedings and transactions. Other applications may also be developed through these technologies, for example, in the fields of legal aid or transactions related to fees and VAT. It should be noted that some member states, such as the United Kingdom do not make extensive use of digital signatures for these purposes, preferring to use Password and PIN solutions.

In the interests of facilitating access by EU citizens to justice, the CCBE is presently working on a number of projects including the Find-a-lawyer project and, in conjunction with the Commission, the development of the E-justice portal. Public access to the former will not require the use of any form of electronic signature, and, in relation to the latter, discussions are proceeding as to the level or levels of authentication which may be required for access to the portal or different parts of the portal with particular discussion surrounding the relative merits, for at least some purposes, of Digital signatures and Password and PIN access. The key point with regard to electronic identification and authentication relates to the security of the exchanges. The level of security should be adapted to the information at stake. Whenever this information is sensitive – for example because it falls within the scope of a deontological obligation of a lawyer such as confidentiality – a very high level of security should be required, though, as has been noted, there may be some diversity of approach in different member states as to how that might most appropriately be achieved.

Nonetheless, interoperability and, in certain circumstances, technical convergence between national e-Justice systems may be required in order to ensure the equivalent level of security of cross-border applications, in accordance with the relevant EU legislation.

This is the reason why the so-called e-CODEX project (e-Justice Communication via Online Data Exchange) is highly relevant. This project – in which the CCBE participates alongside 15 Ministries of Justice of 15 EU Member States – aims to develop building blocks that can be used in or between Member States to support cross-border procedures in the justice field, and seeks to (a) enable easy and secure access to legal discourse in other EU member states for citizens, businesses and legal practitioners, (b) create greater cross-border efficiency of legal processes through common standards and better interoperability, and (c) improve the effectiveness of cross-border judicial processes through standards and solutions that ease and facilitate cross-border case-handling activities

The CCBE has already undertaken important steps for the legal profession in relation to electronic Signatures and electronic Identity cards and has, through its IT Law Committee, issued the following guidelines and recommendations:

- Framework for establishing a European electronic ID-cards system for lawyers
- Technical standards for interoperability of electronic ID-cards for lawyers
- CCBE Recommendations on Electronic ID cards for the legal profession
- Guidelines for e-signature projects and for using electronic signatures by legal professionals

These recommendations and guidelines are not mandatory, and it is the policy of the CCBE that, consistently with the principle of proportionality, the decision on which, if any, form of identity verification is to be employed is a matter for the constituent bars.

Interoperability and technical convergence rather than harmonisation

From the background explained in the previous section of this response, it will be seen that the approach of the CCBE is to seek to achieve full interoperability. This approach is, in fact, consistent with the current EU framework regarding the conditions applying to electronic signatures, which, instead of seeking to harmonise national solutions for electronic signatures (including digital signatures), is based on common principles and a body of minimum (technical) standards which allow for cross-border interoperability. The means of compliance, the system of the national structure, certification policy and its finances are up to the Member States to decide according to their national situations. The CCBE believes that adherence to this principle should be maintained in any revised legal framework on electronic and digital signatures, eID and authentication. From a technical point of view there is no need for harmonisation. The need for EU co-operation in this field relates essentially to the demand for cross-border interoperability and should focus on common principles and minimum standards in order to facilitate intra-Community transactions. With this in mind, it is important that, for those applications where digital signatures are used there is an assurance of the full mutual recognition of those digital signatures.

Electronic consent

As to question 15 of the Commission's questionnaire, the CCBE would like to raise some concerns regarding the issue of "electronic consent". In essence, "electronic consent" in the sense in which it is used in the questionnaire, relates to a simple electronic signature (as opposed to a digital signature) such as is appended by, for example, clicking the "I accept" button. According to the CCBE, the real issue is not so much about what kind of technology is used for "electronic consent" but rather about how to ensure that the person who is accepting the content has really read or understood that content. The CCBE is concerned that consumers are very often mislead by unclear information and complicated content, and that there is, or ought to be, a real question, seen from a consumer protection perspective of whether the ticking of the "I accept" box is or ought to be sufficient to establish a transaction, regardless of questions of identity or the technology that is being used.

Future challenges

Looking at the current EU legal framework, which has already been in existence for more than ten years, there are clearly a number of challenges facing the EU today due to new factors and technological innovation. The CCBE would like to discuss just a few of these challenges, especially those that are of particular concern to the legal profession.

One of them is the issue of **hybrid signatures**. Digital signatures are more and more legally accepted, but electronic documents which have been signed digitally are actually only trustworthy as long as they are kept in their original electronic environment. As soon as these documents are taken out of their original context, by e.g. printing them out, the question arises as to what happens with the legal status of that document. Nowadays technology exists that can ensure end-to-end security, i.e. guarantee that the printed document is a valid extract of the original electronic document. However, from a legal point of view and in a cross-border context, the validity of hybrid signatures remains unclear.

Another challenge that gives rise to concerns is the issue of **long-term validation in relation to e-archiving of documents**. Whether one is using user ID passwords or PKI, after a few years documents which have been created through the use of digital signatures will have lost their technical security because e.g. the certificate has been revoked or the password is not valid any more. Some jurisdictions, such as Austria, have adopted mixed technical and legislative solutions in order to address this issue, but from a legal point of view and in a cross-border context, the long-term validity of these documents remains unclear.

A related question refers to the **life expectancy of electronic systems** used for e-Justice applications. These systems should guarantee, if necessary by means of regular updates, that it is always possible to access the content of the applications concerned and that the security of the latter is preserved. In this respect it should be noted that problems may arise with certain systems (at least those dependent on proprietary software) over time through failure of the suppliers of the product, and there may be real issues where continued updating cannot be maintained.

For the sake of legal certainty, the CCBE considers that an opportunity might be taken to introduce some clarity in relation to at least some of these issues when reviewing the existing Electronic Signature Directive.