EDITORIAL

'Il faut se méfier des ingénieurs: ça commence par la machine à coudre, ça finit par la bombe atomique'.[1]

The United Nations Centre for Trade Facilitation and Electronic Business has been considering adding to its Recommendations, in particular 'Recommendation 37 – Signed Digital Evidence Interoperability'.[2] According to the United Nations Economic Commission for Europe Report 2011 (ECE/INF/2011/1, New York and Geneva, 2011), at page 80, the Recommendation appears to have been issued:

> 'Building upon the success of its Recommendation on Single Windows for import and export clearance, in 2010, UN/CEFACT issued three new, supporting recommendations: Recommendation 35 – Establishing a legal framework for international trade Single Window; Recommendation 34 – Data Simplification and Standardization for International Trade; and Recommendation 37 – Signed Digital Evidence Interoperability.'

However, the web site of the United Nations Economic Commission for Europe included a news item dated 18 July 2011, which indicated that the Recommendation was far from being issued, and it was decided at the 17th UN/CEFACT Plenary on 7-8 July 2011 to extend the review period for Recommendation 37 to 12 September 2011.

Although the content of this Recommendation has altered from its initial iterations, nevertheless the text has the potential to affect laws across the globe. There are two significant issues in relation to this Recommendation. The first is the legal status of Recommendations in general: it is not clear what legal effect, if any, Recommendations have. The second, and more serious, is that it does not appear that any lawyer has been involved with the drafting, if indeed, it is even necessary.

The summary reads as follows:

> 'The Recommendation defines a set of functional rules that signed digital evidence should follow, in terms of the organization and the relationships between the signed content, signatories' certificates and signatures.'

This is a 'recommendation', yet uses the past tense of 'shall', indicating the mandatory nature of content of the document. It follows that it necessary to determine the legal effect, if any, of such a recommendation.

The Foreword (page 3) reads as follows:

> 'The Signed Digital Evidence Interoperability Recommendation aims at increasing the level of interoperability of electronically signed digital evidence in order to facilitate the development of paperless international trade.
>
> To achieve this goal, the Recommendation defines a set of functional rules that signed digital evidence should follow, in terms of the organization and the relationships between the signed content, signatories' certificates and signatures.
>
> The Recommendation does not deal with the legal aspects of electronic signatures, which are dealt with at the international level by other documents such as those published by UNCITRAL. Neither does it does deal with the semantics, usability or interpretation of the signed content. This Recommendation does not conflict with UNECE Recommendation 14 "Authentication of trade documents by means other than signature".
>
> To facilitate the implementation of these rules, annex B gives examples of technical implementations using some of the most recent digital evidence standards. This annex may be updated in the future to take into account other proposed technical implementations.
>
> Due to the urgent need for improved interoperability in digital evidence verification, the Recommendation and its annexes are delivered simultaneously to facilitate the rapid deployment of the Recommendation.'

The authors have made a number of statements that require explanation:

1. There is no evidence to suggest that there is a problem relating to the use of digital documents in international trade.

2. The use of the past tense of 'shall' indicates the mandatory nature of the document functional rules that signed digital evidence should follow. The Recommendation appears to require all documents in digital format to be 'signed' using digital signatures, yet there is no discussion of how digital documents used in international trade are presently dealt with in practice, nor any attempt to indicate how such documents are accepted into evidence in various legal systems in the event of litigation between the parties.[3]

3. There is an assertion that there is an 'urgent need for improved interoperability in digital evidence verification', yet there is no discussion of what evidence there is, if any, to indicate that there is such a need.[4]

1 *'It is necessary to be wary of the engineers: it starts with the sewing machine, it finishes with the atomic bomb', Marcel Pagnol, Critique des Critiques, (Nagel, 1949), page 38.*

2 *The most up-to-date version appears to be 'United Nations Economic and Social Research Council, Recommendation no. 37: Signed Digital Evidence Interoperability Recommendation' (Architecture, Engineering and Construction Working Group – TBG6, ECE/TRADE/C/CEFACT/2010/14 dated 27 September 2010).*

EDITORIAL

The Executive summary (p 4) reads as follows:

> 'A digital document, unlike a paper document, has little evidence value until it is reinforced by a mechanism, such as an electronic signature, which guarantees its integrity and authenticity.
>
> However, because of the multiplicity of electronic signature standards, verification of signed digital evidence by a recipient may be impossible. This has a direct impact on the ability of businesses and administrations to securely exchange digital documents between themselves and with their administrative and financial counterparts.
>
> To address this issue, a functional rather than a technical approach to signed digital evidence has been taken in this Recommendation, by focusing first on the "what" instead of on the "how".
>
> The verification of signed digital evidence must, at least, give the verifier a clear view of:
>
> The signatures' parameters (date, place, type of commitment).
>
> The integrity of the signed content.
>
> The integrity and validity of the signatories' certificates.
>
> The trustworthiness of the certification service providers.
>
> This Recommendation thus defines simple and generic requirements for creating and verifying signed digital evidence to improve its interoperability while keeping in mind that its adoption will elicit requests for changes over time.'

The authors assert, with no reference to any relevant laws or procedural rules (of either common law countries or civil law countries) that a 'digital document, unlike a paper document, has little evidence value until it is reinforced by a mechanism, such as an electronic signature, which guarantees its integrity and authenticity'.[5]

The weight to be attached to a digital document is a matter for the relevant substantive laws on evidence or procedural rules (or both) of individual nation states. A document that includes an electronic signature (the authors probably mean a digital signature) may have some probative value in relation to its integrity, but little weight will be attached to the authenticity of the document unless there is a presumption that an electronic signature (or a particular form of electronic signature) is attached to the data, or sufficient evidence (other than the electronic signature) has been adduced to the satisfaction of the finder of fact to convince them that the data can be considered to be authentic.[6]

The Recommendation provides, on page 5, a list of benefits. 1.1, which reads:

> 'This Recommendation provides business, administrative and financial organizations with a set of simple and standard requirements for exchanging secure documents, which can be matched by a variety of standard technologies and products, including open source projects.
>
> Its objectives are to:
>
> Improve efficiency and reliability of the verification of signed digital evidence received from another party.
>
> Increase interoperability of signed digital evidence, which, in turn, will increase trust and confidence.
>
> Provide a wide, yet coordinated, path to increase the rate of adoption of paperless technologies.'

The frequent references to 'certificates' merely indicate that the authors of the Recommendation intend that the only approach is to provide for a highly specific type of technology, namely Public Key Infrastructure (PKI), which is not a product, but a number of protocols. This will benefit the providers of PKI products. It will not deal with the legal issues relating to liability, significant as they are,[7] and the objective that asserts that the Recommendation will increase

3 *For more information on 45 legal systems across the globe, see Stephen Mason, general editor, Electronic Evidence, (2nd edn, LexisNexis Butterworths, 2010), covering: Australia, Canada, England & Wales, Hong Kong, India, Ireland, New Zealand, Scotland, Singapore, South Africa and the United States of America, and Stephen Mason, general editor, International Electronic Evidence, (British Institute of International and Comparative Law, 2008), covering: Argentina, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, Norway, Poland, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Thailand and Turkey; for a more detailed treatment of the United States of America, see George L. Paul, Foundations of Digital Evidence (American Bar Association, 2008).*

4 *Assertions that are not based on facts have been used to partially justify the eJustice project in the EU where a notice from the Council dated 5 June 2008 (only available in French) (Conseil de l' Union Européenne Note de Transmission; Origine: Pour le Secrétaire général de la Commission européenne, Monsieur Jordi Ayet Puigarnau, Directeur; Date de réception: le 2 juin 2008; Destinataire: Monsieur Javier Solana, Secrétaire général/Haut Représentant; Objet: Document de travail des services de la Commission – Annexe au projet de Communication de la Commission présentant une stratégie européenne en matière d' e-Justice – Analyse d' impact Les délégations trouveront ci-joint le document de la Commission (le 5 juin 2008) SEC(2008) 1947; 10285/08 ADD 1 LIMITE JURI FO 45 JAI 305 JUSTCIV 119 COPE 118 CRIMORG 87) included the following text at 2.1.2:*

> *' Si le pourcentage de citoyens européens (2%) ayant été impliqués dans une procédure civile dans un État membre autre que le leur, reste faible, ce chiffre rapporté à la population totale de l' Union devient particulièrement significatif. Ce sont ainsi 10 millions de personnes qui ont été concernées par une procédure civile transfrontalière,'*

An approximate translation into English renders the text as follows:

> *' If the percentage of Europeans (2%) involved in civil proceedings in a Member State other than their own remains low, the figure reported in the total population of the Union becomes particularly significant. This means there are 10 million people who were involved in cross-border civil proceedings'*

This text is routinely cited in EU documents, stating as a fact that there are 10 million people involved in cross-border civil proceedings. The precise number is not known, but in the UK, the Office of Fair Trading, in answering questions relating to the ' Call for Evidence and Views on the European Commission's Green Paper on policy options for progress towards a European Contract Law for consumers and businesses' by the Ministry of Justice, indicated that in 2009 there were 41 cross border cases in the UK out of 850,000 cases.

5 *As an aside, it must be explained that a contract is capable of being entered into by word of mouth, and such a contract is also enforceable. Billions of people across the world enter contracts in this way every day. For a criticism of PKI from a technical point of view, and what it does not do, see an early paper by Chris Sundt, ' PKI — Panacea or Silver Bullet?' , Information Security Technical Report (2000) 5:4, 53-65.*

'interoperability of signed digital evidence, which, in turn, will increase trust and confidence' provides an inaccurate and misleading suggestion that the user can expect to place 'trust and confidence' in a technical product that is far from perfect.

On page 5, paragraph 2, the authors put the Recommendation into context, commenting, at 2.1 in respect of 'scope' (footnotes omitted):

> '1. Since the early 1990s, numerous technical standards for signed digital evidence have been designed, proposed and adopted.
>
> 2. However, as a result, this multiplicity of standards with many possible options and lack of guidance on how to apply digital signatures to documents has led to a lack of interoperability of signed digital evidence from a syntactic, semantic and processing perspective.'

It is an open market. A vendor decides how to apply a standard (which is why standards are not quite what they seem), for which see an article by Paweł Krawczyk in the context of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,[8] and how the politicians used legislation to require the use of digital signatures and how different vendors implemented different standards in different ways: 'When the EU qualified electronic signature becomes an information services preventer', *Digital Evidence and Electronic Signature Law Review*, 7 (2010), 7 – 18.[9] Little has changed since Chris Sundt wrote on this topic in 2000:[10]

> 'These problems arise partly through ambiguities in the associated standards and protocols, leading to incompatible implementations, and partly through proprietary development of additional functionality by suppliers to make their offerings more attractive and usable. There are also inherent problems in the way that some of the standards are defined. For example, the X.509 V3 certificate format allows user-defined extensions to carry user-specific information. These extensions can be marked as critical, in which case verification of a certificate will only succeed if the recipient system can understand the significance of that extension.'

On page 7, paragraph 2.3.13, the authors have addressed the nature of the audience that the Recommendation is directed at:

> 'This document is intended primarily for organizations and individuals who have the following concerns:
>
> Exchanging signed digital evidence in an open environment.
>
> Choosing a format for signed digital evidence, suitable for a particular dematerialization project.
>
> Monitoring information technology with respect to the fields of digital signatures and probative archiving.
>
> Ensuring the interoperability, reversibility and validity of signed digital evidence.'

These Recommendations are laudable. However, it is necessary for the authors to include a reference to the difficulties in relation to the archiving of digital signatures, for which see: Stefanie Fischer-Dieskau and Daniel Wilke, 'Electronically signed documents: legal requirements and measures for their long-term conservation' *Digital Evidence and Electronic Signature Law Review*, 3 (2006), 40 – 44.

Generally, the Recommendation is not about evidence. It does not follow that by complying with it, that digital evidence be admissible in legal proceedings. The language includes the use of the words 'probative value'. It does not follow that a digital document signed with a digital signature has any probative value.

The Recommendation only considers one problem, which is, what can be understood from a digital certificate. There is a great deal of detail about what can be signed, the relationship between the signature and the content, the role and placement of 'co-signers' or 'counter-signatures', but no discussion of the nature of trust in relation to the supporting technologies and organization, nor whether any such support should be credible.

The central issue in relation to the electronic signature has not been addressed: indeed, it is assumed that it does not need to be addressed – that is, how the recipient can be assured that (a) the purported signing party was responsible for affixing the signature to the data, and (b) the purported signing party had the relevant authority to cause the digital signature to be affixed to the data. The perennially difficult question of the liability of the certifier is also not dealt with, except to the extent that potential liability may compel adherence to high standards.

Throughout the Recommendation, the authors have referred to the 'signatory'. There are two problems with their failure of logic. First, there is no 'signatory'. It is not possible to say that Alice 'signed' a document. It is only possible to say that one form of digital data (the data comprising a digital signature) is associated with another form of digital data (the data that makes up the document). That is all. Second, it is necessary to prove that a particular person (that is the person whose name is associated with the data) caused the digital data that comprises a digital signature to be affixed to the digital data comprising the document.

Thus the authors should indicate throughout the Recommendation that they refer to the 'purported signatory', not the 'signatory'. The use of the word 'signatory' presupposes that the person who is asserted to have 'signed' the document *has* done so.

Digital signatures are generally marketed as a form of electronic signature that enables the recipient to prove that a document or communication actually came from the person whose digital signature was used to 'sign' the data. This is not correct. The private key of a digital signature (also known as an 'advanced electronic signature' in the EU) is protected by a password. If a person uses a

6 *The same comments apply to the contents of paragraph 2.1.4 on page 5 of the Recommendation. For the proposed tests to demonstrate authenticity, see Electronic Evidence, Chapter 4.*

7 *Lorna Brazell, Electronic Signatures and Identities Law and Regulation, (2nd end, Sweet & Maxwell, 2008); Stephen Mason, Electronic Signatures in Law, (2nd edn, Tottel, 2007) [the third edition, published by Cambridge University Press, will be available in January 2012], M. H. M Schellenkens, Electronic Signatures Authentication Technology from a Legal Perspective, (TMC Asser Press, 2004).*

8 *OJ L 13, 19.01.2000, p. 12.*

9 *For a list (over 11 pages) of standards relating to digital signatures, see Electronic Signatures in Law, Appendix 3.*

10 *Chris Sundt, ' PKI — Panacea or Silver Bullet?', Information Security Technical Report (2000) 5:4, 53-65.*

EDITORIAL

digital signature, the most important point to be aware of is this: the private key of a digital signature is only as good as the password that protects it. This means that when the password is inserted into a computer to provide access to the private key of a digital signature, it proves either of the following:

> The person who keyed in the password (or username and password) knew the password (or username and password); or
>
> The person with access to the computer (whether they were sitting in front of the computer or whether they obtained control of the computer remotely) did not need to know the password because the computer was instructed to remember the password (or perhaps they correctly guessed it, or they were capable of overriding it in some way).[11]

This leads back to the notorious and notoriously failed concept of 'non-repudiation' that continues, erroneously, to be asserted by technicians.[12]

Furthermore, R16 bullet point 2 (page 12), provides as follows:

> 'Proof of approval, indicating that the signatory has approved the signed content'.

The authors do not indicate whether the purported signatory is legally bound by the signed document. In addition, it is to be noted that signatures serve a number of functions, only one of which is to approve the content of a document. It is a sweeping provision that asserts the purported signature *approves* the content.[13] The function of a signature can only be determined by understanding the full context of the signature, including evidence that is not part of the digital process. The function that a signature serves is not a question of evidence, but a question of law that cannot be resolved by technical means.

As the foregoing illustrates, the actual recommendation (below), is neither possible to achieve technologically, nor does it remotely address the complex legal issues that arise from the assumptions that the technology can adequately address any of the issues it purports to address:

> '1. Recommendation No. 37: Signed Digital Evidence Interoperability Recommendation
>
> This Recommendation encourages any organization that wishes to exchange signed digital evidence with others to maximize the interoperability of such evidence by following a set of proposed principles:
> Signed digital evidence:
>
> - MUST contain one and only one identifiable content
> - MUST be signed by one or more signatures
> - MUST contain all identities involved in an unambiguous way.

Each signature contained in the evidence:

> - MAY contain a date of signature and other properties
> - MUST sign the entire content
> - MAY be signed by one or many counter-signatures.'

At best, the Recommendation may be useful to standardize the form of assertions made by digital signatures, so that different systems of verification can recognize assertions made by different systems of creation of signatures. But from this point to assert that complying with the Recommendation makes a digital document of legal value or more probative than it was before, even if combined with existing standards on digital signatures, is unjustified.

The central question about this document has yet to be resolved: why such a project was initiated. There is no evidence to demonstrate that it is necessary. Marcel Pagnol was only partly correct at the time he was writing, because without the politicians, the engineers would not have developed nuclear fission, although it might only have been a matter of time. In one respect he was far more prescient: engineers are making sure that machines take over life, and this is very dangerous for humans as a species.

As a matter of record, the names of those involved in this Recommendation are set out below (this information is not included in the document dated 27 September 2010, but is include in the following document: Recommendation No. 37 Digital Evidence Certification Recommendation, (ECE/TRADE/TBG/CEFACT/2010/xx, DEC-R V1.1 – Proposal – revision 2.0.2, 19 February 2010), which is marked 'Working document: do not copy or distribute without authorization'):

Editors: François Devoret ((UN/Cefact Security Project Editor) and Julien Pasquier, both of whom work for Lex Persona, an organization that sells digital signatures and PKI products; Andrea Caccia, who is a member of AITI (Associazione Italiana dei Tesorieri d'Impresa) that includes financial payment systems and Commissione Tecnica Dematerializzazione Straight Through Processing (Member of ETSI/ESI) and Michel Entat, who founded Conseil en Management des Systèmes d'Information that deals with paperless tendering.

Contributors: Sujeet Bhatt (UN/Cefact Security Project Leader) and Ajit Menon, NexTenders (India) Pvt Ltd, which apparently deals exclusively with public eProcurement and eTendering using digital signatures and PKI, using a patented Security Architecture; Paul Burrows, who is Head of Information Systems of the RICS Building Cost Information Service that sells an eTendering product; Andrew Hudson of Kern CM Limited, an organization that provides an e-tendering service; Bernard Longhi of BLC-Consultants (he seems to be the only consultant) and Kevin Smith of Cloud Data Technologies Limited ((UN/Cefact TBG6 Chair).

Reviewers: Gordon Cragge of Sitpro, which ceased to exist on 31 August 2010 and Chris Hassler of DOD-DCMA (Defense Contract Management Agency).

11 *For cases where digital signatures have been used by criminals to transfer funds from company bank accounts, see Olga I. Kudryavtseva, ' The use of electronic digital signatures in banking relationships in the Russian Federation' , Digital Evidence and Electronic Signature Law Review, 5 (2008), 51 – 57, and Olga I. Kudryavtseva, Case note: Resolution of the Federal Arbitration Court of Moscow Region of 5 November 2003 N КГ-А 40/8531-03-П, Digital Evidence and Electronic Signature Law Review, 5 (2008), 149 – 151.*

12 *For a detailed discussion of why ' non-repudiation' is irrelevant, see Electronic Signatures in Law, 14.20 – 14.21.*

13 *For a detailed discussion of the functions a signature is capable of serving, see Electronic Signatures in Law, 1.20 – 1.26.*

