Electronic signatures

England and Wales

In the case of *Mehta v J Pereira Fernandes S A* [2006] EWHC 813 (Ch), His Honour Judge Pelling QC, sitting as a Judge of the High Court, overturned an earlier decision of District Judge Harrison of the Manchester County Court, in which he determined that an e-mail address was not capable of being a form of electronic signature. Compare this decision with the case of *1327/2001 – Payment Order*, as reported Georgia Skouma in e-Signature Law Journal, Volume 1, Number 2, 2004, 95 – 98, in which a Greek judge held that an e-mail address was capable of being a form of electronic signature. See also the US case of *Roger Edwards LLC v Fiddes & Son Limited* 245 F.Supp.2d (D.Me. 2003) and the Singapore case of *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd* [2005] SGHC 58, as reported by Bryan Tan, in e-Signature Law Journal, Volume 2, Number 2, 2005, 126 - 127.

Editors note: This decision illustrates the need for judges to (a) obtain expert opinion with respect to technical issues and (b) if electronic signatures are going to be consistent across the world, for decisions of judges from other jurisdictions to be considered when such cases are brought before domestic adjudicators.

The judgement is available in electronic format at
http://www.bailii.org/ew/cases/EWHC/Ch/2006/813.html

Denmark

Danish medical records online

All Danish citizens are now able to view their medical records on-line. Using their digital signature, the Danes can now obtain access to a registration of their own diagnoses, operations, examinations and other hospital treatments dating back to 1977. They can also obtain details of treatments outside the hospital, and psychiatric treatments dating back to 1995 as well as information about waiting lists and other personalised information. The new health information system uses the OCES signature, which is issued for free to all Danish citizens by the Danish telecommunication company TDC A/S on behalf of the Danish state. For more information, see Jan Hvarre, 'Electronic signatures in Denmark: free for all citizens' e-Signature Law Journal Volume 1 Number 1, 2004, 12 - 16.

Additional reporting by Jan Hvarre, country correspondent for Denmark.

Further information:
http://www.sundhed.dk/wps/portal/_s.155/1836

United States of America

Proposed Rule to permit investors to obtain proxy materials over the internet

On 29 November 2005, the Securities and Exchange Commission (SEC) voted to propose for public comment rules that will allow the internet to be used to enable companies and others to deliver proxy materials. The SEC explained the position in their press release:

'When a person solicits a proxy from the shareholders of a company that is subject to the Commission's proxy rules, Rule 14a-3 currently requires that a proxy statement, which must include specified disclosure, be delivered with or prior to that solicitation. Further, when a company solicits proxies, it also must deliver an annual report to shareholders, which must include additional specified disclosure. Under current rules and Commission interpretations, the proxy statement and annual report must be delivered in paper form or, if the shareholder consents, they may be delivered electronically (for example, by e-mail). The electronic delivery option requires affirmative shareholder consent and currently is used only on a limited basis.'

Comments on the proposed rules should be received by the Commission within 60 days of their publication in the Federal Register.

The SEC News release is available at
http://www.sec.gov/news/press/2005-166.htm

Digital signatures

Brazil

A Management Committee for the Judicial Certification Authority (Comitê Gestor da Autoridade Certificadora da Justiça (AC-JUS) was established in October 2005 by the President of the Superior Court of Justice in Brazil. The Committee, which has established provisions governing the use of digital signature in documents used in the superior courts, membership of the Committee include the Supreme Federal Court, the Superior Court of Elections and the Superior Labour Court.

The technology used by AC-JUS allows documents and other information exchanged by electronic means to be encrypted; it also creates standards with which documents will have to comply in order to be certified electronically for use in the courts. The application of the new technology will apply only to judges and other officials within the judiciary to begin with. In practice, it will serve to authenticate documents issued by judges or other judicial officials in Brazilian judicial

proceedings. Documents sent or communicated electronically by these means will carry a presumption of authenticity.

In the future, the AC-JUS will be able to issue regulations providing for the filing of electronic petitions and papers through the internet, providing these documents are electronically certified by AC-JUS. The Superior Court also contemplates the possibility, in the near future, of authenticating decisions issued on-line by judges and courts. The AC-JUS system entails the simultaneous use of at least three keys, which are maintained in the custody of the constituent entities of the Committee.

Information kindly provided by Cristina de Hollanda, member of the editorial board and country correspondent for Brazil.

Verification

Digital images of fingerprints as a form of verification

A system run by Pay By Touch is currently being tested in the UK. A person can be verified by the use of a digital image of their fingerprint. Pilot projects are under way in Co-op supermarkets in Oxfordshire, Wiltshire and Gloucestershire in the UK. Apparently the technology is already operating in more than 1,000 stores across America. The scheme requires customers to have their fingerprints scanned. They then register their debit, credit and loyalty cards on-line. The user places a finger on a scanner at the checkout to act as a form of verification, and they then use a personal identity number (the electronic signature) to indicate assent to the transaction.

Editor's note: A point that does not seem to have been covered in these reports, is that depending on the nature of the information they share with the third party, the customer can lose all rights under the contract with their provider, because if they share information with a third party that they are expressly prohibited from sharing, their liability for loss will increase.

Nina Goswami, 'Customers to pay for shopping with a fingerprint at the Co-op' News. Telegraph, 23 October 2005, available in electronic format at ***http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/10/23/ncoop23.xml***

Michele Chandler, 'Point of Sale: Retailers Try their Hand at Finger-Scanning Payment System' Mercury News, 20 June 2005, available in electronic format at **http://www.biometricgroup.com/in_the_news/06_20_05.html**

Biometric vein checking

Scanners checking the pattern of veins in finders will be the subject of trials in Europe. Registration will entail the person submitting a number of fingers to be scanned with an infra-red light to capture the pattern of the veins. The image is recorded in digital format and entered into a database. The user then submits a finger to the scanner to verify their identity, before using their PIN or password as their electronic signature to indicate assent. To prevent attacks by criminals, by which a person is forced to withdraw money from a cash machine, one finger will be registered as a 'duress' finger. Where the 'duress' finger, is used, the aim is for the system to recognise the person may be suffering from coercion, and the system can send out an appropriate alert.

Further information at **http://www.hitachi.com.sg/cat_index_214.shtml**

Electronic voting

California

California has proposed a list of ten requirements considered to be critical for any vendor to demonstrate before they apply for certification.

A new, permanent Office of Voting System Technology Assessment has been created in the Secretary of State's Office. Voting systems will not be considered unless the vendors or products have:

1. Been federally certified by the EAC-approved independent testing authorities.
2. Provided full documentation and training materials of all related system materials, including promotional materials.
3. Provided comprehensive use procedures applicable to California elections.
4. Established a county user group for annual system review and to ensure voter accessibility.
5. Deposited source code in an approved escrow facility and a copy of the source code and binary executables with his office.
6. Agreed to provide the Secretary of State a working version of the system components, upon request, for testing and analysis.
7. Been certified to be used together as a comprehensive system if the components have been independently certified.
8. Agreed to be combined only for purposes of aggregating vote totals or laying out their ballot types.

9. Provided printing specifications for any ballots to be used with the components.
10. Agreed to volume testing to simulate Election Day use.

A list of voting system requirements has also been established (for details, see the press release).

For the press release dated 5 October 2005, see **http://www.ss.ca.gov/elections/elections_vs.htm**

Electronic conveyancing

United Kingdom

The Land Registry in the UK has decided to test a limited prototype of electronic conveyancing. The first version is intended to be released in the third quarter of 2006. It is anticipated that a more in-depth project will take place in the third quarter of 2007.

For more information, see **http://www.landreg.gov.uk/e-conveyancing/news/?article_id=8194**

Registration cards

Korea

The present resident registration cards will be replaced in 2008 with new cards that include personal information on microchips. The Ministry of Government Administration and Home Affairs, together with a consortium led by the Korea Minting and Security Printing Corporation are developing the new cards.

The information contained on the chip will include resident registration numbers, a digital image of the person's fingerprints, their residential address, health insurance information and security passwords, amongst other information. The face of the card will include the person's name, photograph, gender, date of birth and registration site. The holder's registration number, which is currently printed on the card, will be removed. This number will be included in the chip.

It is hoped that the new cards will reduce the increasing number of criminal acts related to the forgery of personal identification cards. The government also intends to encourage people to use their cards to log into government web sites and perhaps to use them for electronic voting.

Article by Kim Tong-hyung, Staff Reporter, 'Chip-Embedded ID Cards Planned for 2008' 10 February 2006 available in electronic format at h**ttp://times.hankooki.com/lpage/200602/kt2006021017315610230.htm**

Article 'Smart ID Cards to Be Ready by 2008' The Chosun Ilbo, available in electronic format at **http://english.chosun.com/w21data/html/news/200602/200602090021.html**

United Kingdom

The Identity Cards Act 2006 has been passed by Parliament, setting up a National Identity Register. This scheme will go ahead even though Parliament has not been appraised of the cost of setting up the register, and nobody knows how it will be implemented.

The Act is available in electronic format at **http://www.opsi.gov.uk/acts/acts2006/20060015.htm**

Civil procedure

Brazil

Filing of papers by e-mail

The Superior Court with jurisdiction with respect to Labour Law has issued secondary legislation allowing for the filing of papers by e-mail. According to Normative Instruction N. 28, the criteria for acceptance of papers requires that:

1. petitions must be in pdf format,
2. petitions shall not exceed 2 megabytes in size, and
3. the attorney must have a certified electronic signature registered with one of the entities of ICP-Brasil.

Normative Instruction N. 28 is available in electronic format (in Portuguese) at **http://www.trt4.gov.br/edoc/in28tst.htm**
Information sent in by Cristina de Hollanda, member of the editorial board and country correspondent for Brazil.

Modifications to the Brazilian Civil Procedure Code

Following the creation of AC-JUS, Law 11.280 was enacted in February 2006, modifying ten articles of the Brazilian Code of Civil Procedure (CPC). The changes introduced by the new statute include the addition of a paragraph to Article 154 of the CPC, allowing the Brazilian superior courts to regulate the use of documents submitted electronically in procedural actions in order to guarantee the authenticity, integrity and legal validity of documents whose digital certificates and electronic signature have been conferred by the Brazilian Infrastructure of Public Keys (ICP–BR). [More information on the Brazilian Infrastructure of Public Keys (ICP–BR) can be found in

the article by Cristina de Hollanda 'Electronic signatures and digital certification: the liability or registry authorities under Brazilian legislation' *e-Signature Law Journal*, Volume 1, Number 1, and Stephen Mason *Electronic Signatures in Law* (LexisNexis Butterworths, 2003).]

Article 154 of the CPC enunciates a general principle of procedural law that, unless otherwise specifically mandated, the mere form of judicial acts does not determine their effectiveness or validity. The paragraph introduced by Article 154 authorizes the courts to permit the performance of certain procedural acts by electronic means, as long as the minimum requirements of authenticity, integrity, legal validity and compatibility established by the ICP-BR have been met.

The ICP-BR digital certification system was created by the Provisional Measure 2.220-2 of August 2001. [Available in electronic format at http://www.trt4.gov.br/edoc/legislacao-edoc.htm] E-mails have subsequently become more widely accepted as valid documents in courts and the prejudice against the use of digital documents has, in part, diminished. For example, the Superior Labor Court has issued Normative Instruction No. 28, which regulates the so-called "e-doc system" and is based on Provisional Measure 2.220-2. Normative Instruction No. 28 allows the filing of petitions, briefs and other legal documents through the internet since June 2005. ICP-BR has a direct effect on the development of procedures for substituting digital documents for paper in legal transactions and the flow of information, both in the public and private sectors. Nevertheless, the ICB-BR system has been criticized because it is purely a creature of the Executive Branch.

As Provisional remedies are enacted directly by the President of the Republic, the creation of the ICP-BR by means of a Provisional remedy meant that the legislature did not participate in the process. In addition, the management of ICP-BR reports directly to the President of the Republic. Its regulating agency (the Managing Committee) and the Directorate of the ITI, which holds its key-root, are nominated by the President of the Republic. ICP-BR has no representation other than from the Executive branch. Therefore, although not expressed in Provisional Measure 2.200-2, some commentators argue that the Administration of President Fernando Henrique Cardoso intended to impose the ICP-BR system on the other branches of government, and to require them to digitally certify their documents according to the criteria set by the Executive branch. However, such a requirement would violate the constitutional principles of separation of powers. Thus, the justification to modify Article 154 of the Civil Procedural Code, was to grant jurisdiction to the judiciary in regulating the use of e-documents within the judicial branch of government.

Information kindly provided by Cristina de Hollanda, member of the editorial board and country correspondent for Brazil

United States of America

The following Civil Rules Amendments, dated August 2004 - December 2006 Amendments have been posted on the US Courts Federal Rulemaking web site:

Civil Rule 5 (Service and Filing of Pleadings and Other Papers) (authorizes courts to adopt local rules requiring electronic filing)

Civil Rule 16 (Pretrial Conferences; Scheduling; Management) (establishes process for the parties and court to address early issues pertaining to the disclosure and discovery of electronic information)

Civil Rule 26 (General Provisions Governing Discovery; Duty of Disclosure) (requires parties to discuss during the discovery-planning conference issues relating to the disclosure and discovery of electronically stored information)

Civil Rule 33 (Interrogatories to Parties) (expressly provides that an answer to an interrogatory involving review of business records should involve a search of electronically stored information)

Civil Rule 34 (Production of Documents and Things and Entry Upon Land for Inspection and Other Purposes) (distinguishes between electronically stored information and "documents")

Civil Rule 37 (Failure to Make Disclosure or Cooperate in Discovery; Sanctions) (creates a "safe harbor" that protects a party from sanctions for failing to provide electronically stored information lost because of the routine operation of the party's computer system)

Civil Rule 45 (Subpoena) (technical amendments that conform to other proposed amendments regarding discovery of electronically stored information).

See **http://www.uscourts.gov/rules/newrules6.html**

Electronic signatures

European Union

A recent Report from the Commission to the European Parliament and the Council on the operation of Directive 1999/93/EC on a Community framework for electronic signatures 15.3.2006 COM(2006) 120 final, points out that, although electronic signatures are now legally recognised in all Member States, their take-up is minimal. It is alleged that the take-up of electronic signatures is too low and this is hindering the potential growth of trade in goods and services via the internet. In particular, the market for "qualified" signatures has been much slower to take off than expected.

Editor's note: The report refers, in the main, to digital signatures, not electronic signatures. There is a problem because the EU Directive insists on calling all forms of electronic signature the same name – electronic signature – when the term 'electronic signature' is a generative term encompassing all forms of electronic signature. The EU Directive does not use the word 'digital signature', but this is what is meant in this report. This report is factually incorrect. The use of digital signatures has not prevented the use of the internet as a means of trade in goods and services, as many retailers selling goods and services over the internet are very well aware. The EU seems intent on forcing the use of one particular type of signature: the digital signature, and it is clearly not happy that ordinary people and commercial organizations have declined to use such expensive and unnecessary methods of electronic signature. The comments in paragraph 2.3.4 are of interest:

> *2.3.4 Legal recognition*
> *Article 5.2 establishes the general principle of the legal recognition of all kinds of electronic signatures established by the Directive.*
> *It requires Member States to ensure that the qualified electronic signature (Article 5.1) is recognised as meeting the legal requirements of hand-written signatures and that it is admissible as evidence in legal proceedings in the same way as hand-written signatures are in relation to traditional documents.*
> *Concerning the legal effect of e-signatures, there is yet no representative case law that allows for any assessment of the recognition of electronic signatures in practice.*

First, all forms of electronic signature are recognized, but the inference is then made that only a qualified electronic signature 'is admissible as evidence in legal proceedings in the same way as hand-written signatures are in relation to traditional documents'. This comment makes the first assertion somewhat otiose, as it implies that no other form of electronic signature is admissible in evidence. The simple truth is, either a document is signed or not. The degree of signature is of no relevance. What is relevant is the evidence to prove a document was signed, or an 'I accept' icon was clicked.

Finally, the last paragraph is factually inaccurate. There have been a number of cases in Europe about electronic signatures, many of which have been published in translation in this Journal. There are a number that have not been translated, and if any reader wishes to get in touch to offer to help, that will be much appreciated. The list of known cases are as follows:

The list of cases below are noted by the United Nations Commission on International Trade Law, Working Group IV (Electronic Commerce) Forty-second session in Vienna, 17-21 November 2003

- **Amtsgericht Bonn, Case No. 3 C 193/01, 25 October 2001, JurPC—Internet Zeitschrift für Rechtsinformatik, JurPC WebDok 332/2002 available at www.jurpc.de/rechtspr/20020332.htm.**
- **Landgericht Bonn, Case No. 2 O 450/00, 7 August 2001, JurPC—Internet Zeitschrift für Rechtsinformatik, JurPC WebDok 136/2002 available at www.jurpc.de/rechtspr/20020136.htm.**
- **Oberlandesgericht Karlsruhe, Case No. 14 U 202/96, 14 November 1997, JurPC— Internet Zeitschrift für Rechtsinformatik , JurPC WebDok 09/1998 available at www.jurpc.de/rechtspr/19980009.htm.**
- **Bundesgerichtshof, Case No. XI ZR 367/97, 29 September 1998, JurPC—Internet Zeitschrift für Rechtsinformatik, JurPC WebDok 291/2002 available at www.jurpc.de/rechtspr/19990005.htm.**

The following cases mentioned in the review of the European Electronic Signature Directive "The Legal and Market Aspects of Electronic Signatures", prepared by Professor Jos Dumortier and his colleagues for the EU.

- **Finland: A case relating to the admissibility and legal enforceability of documents transmitted by electronic means (facsimile mainly) and whether specific types of documents can be delivered by electronic means, mentioned on page 81.**
- **Germany: A case relating to the evidential value of**

an e-mail that was not signed (AG Bonn, Decision of 25 October 2001), mentioned on page 80.

- Lithuania: A case from a court in Lithuania relating to the use of a PIN code on a payment card. Unfortunately, only mentioned on page 231.
- Netherlands: A case from a Dutch judge relating to an e-mail that was not signed, who ruled that the e-mail message could not be granted any legal value because of the evident security risks of the e-mail communication, mentioned on page 81.
- Slovenia: There have been a few cases in Slovenia relating to e-mails between parties that are admissible if signed with a qualified signature, but there is no other detail other than a case is mentioned on page 241.
- Spain: A case relating to a Court of First Instance of Madrid that ruled on an electronic contract between private parties was null and void on the grounds that it did not bear an electronic signature, mentioned in on page 81.
- Switzerland: Seite 181 (BGE_127_III_181) 31. Auszug aus dem Urteil der Schuldbetreibungs- und Konkurskammer vom 15. November 2000 i.S. R. (Beschwerde).
  Seite 252 (BGE_121_II_252) 43. Extrait de l'arrêt de la IIe Cour de droit public du 13 juillet 1995 dans la cause M. B., son épouse N. B. et leurs enfants A. et T. contre Département fédéral de justice et police (recours de droit administratif).

United Arab Emirates

The UAE have recently passed Federal Law Number 1 of 2006 regarding Electronic Transactions and Commerce. The law provides for electronic signatures and the formation and validity of contracts concluded on-line. The law also expressly stipulates that contracts are not invalid or unenforceable solely by reason that Electronic Communication was used in [their] formation. The law provides a detailed definition of secure electronic signatures and outlines the circumstances in which it is deemed reasonable to rely on such signatures; the establishment of a supervising authority for certification service providers, and the requirements that have to be met.

Certification

China

The Symposium on the Development of Electronic Certification Service Industry was held on 29 April 2006. More than 140 Certification Authorities (CAs) are now established in China, one year after the Electronic Signatures Law came into effect. However, only 17 have received a licence from the Ministry of Information Industry (MII), although they have issued 2,600,000 certificates up to date. The MII proposes to censor un-licensed CAs until October 2006.

Reported by Minyan Wang, country correspondent for China
A news item, in Chinese, is available at:
http://www.sxit.gov.cn/admin/newsshow.asp?id=100260 0&chid=100001

Electronic Notarization

China

Notarization Law of the People's Republic of China
The National People's Congress promulgated the Notarization Law of the People's Republic of China governing notary qualifications and notarization procedures on 28 August 2005. It went into effect on 1 March 2006. The new law includes statutory provisions governing the following areas:

Notarial Office

The Notarization Law clearly defines the term "notarial office" as a "a non-profit certification institution that is lawfully established and independently exercises the notarial functions and bear corresponding civil liabilities." One or more notarial offices may be established in one city. The following requirements must be satisfied: (i) having its own name; (ii) having a fixed place; (iii) being staffed with 2 or more notaries; and (iv) having necessary funds.

Notaries

The major criteria for qualifying as a notary include having PRC citizenship and successfully passing the National Judicial Examination.

Notarization Procedures

The Notarization Law stipulates a set of detailed procedures for notarization. Any notarization request can be made to a notarial office in the place where the applicant is domiciled or habitually resides, or where the relevant act is committed, or where the relevant fact

occurs. Notarization of documents related to real property shall be undertaken by a notarial office where the real property is located.

Effect of Notarization
Once a specific act, fact or document has been notarized, such will be considered as accurate unless proven otherwise by evidence. Anyone who contests the contents of the notarial certificate may file a civil suit in the People's courts.

The main points noted above are courtesy of Morrison & Foerster on-line at **http://www.mofo.com/news/updates/bulletins/bulletin02150.html**

United States of America

The eTrust Subcommittee of the Electronic Filing Committee, Science and Technology Law Division of the American Bar Association Chaired by John H. Messing has issued a paper on the subject of eNotarization, available on-line at

http://www.abanet.org/dch/committee.cfm?com=ST231005

The National e-Notarization Commission (2005-2006) Chaired by Secretary of State Elaine Marshall has issued a paper setting out Proposed Standards for e-Notarization, dated 16 May 2006, available on-line at

http://www.nass.org/releases/National%20Commission%20eNotarization%20Draft%20Standards.pdf

Electronic voting

Australia

The Joint Standing Committee on Electoral Matters produced a report 'The 2004 Federal Election' (September 2005, Canberra). Recommendation 41 is set out in full below, in which it suggests the use of electronic voting to assist blind and visually impaired people to vote in a secret manner:

> 'The Committee recommends that a trial of an electronic voting system be implemented at an appropriate location in each electorate to assist blind and visually impaired people, who currently cannot cast a secret and independently verifiable vote.
>
> - In terms of the type of electronic voting system, and the most appropriate locations, the AEC should liaise with relevant groups, and then report back to the Committee with its proposal.
> - Following the election, the AEC should report back to the Committee on all aspects of the trial.'

The Report is available on-line at **http://www.aph.gov.au/house/committee/em/elect04/prelims.htm**

France

On 5 June 2006, Andrew W. Appel attended a training session for assesseurs (poll watchers) of the world-wide internet election for the Assemblée des Français de l'Etranger. This Assemblée elected 12 members of the French Senate. In the opinion of Mr Appel, his observations are such that it is impossible for the assesseurs to certify with any confidence that the election was conducted accurately and without fraud.

Report by Andrew W. Appel: 'Ceci n'est pas une urne: On the Internet vote for the Assemblée des Français de l'Etranger' available on-line at **http://www.cs.princeton.edu/~appel/urne.html**

United States of America

A report suggests the worst security flaw seen in Diebold AccuVote-TS touch screen voting machines has been revealed. Apparently an examination of one of the most popular touch screen voting machines used in public elections in the United States of America, has demonstrated that it a single switch can make the machine can behave in a completely different manner compared to the tested and certified version.

Ariel J. Feldman, J. Alex Halderman and Edward W. Felten 'Security Analysis of the Diebold AccuVote-TS Voting Machine' (Centre for Information Technology Policy, Princeton University, September 2006)

The following text is from the web site:

> 'To our knowledge ours is the first public study encompassing the hardware and software of a widely used DRE. The famous paper by Kohno, Stubblefield, Rubin, and Wallach studied a leaked version of the source code for parts of the Diebold AccuVote-TS software and found many design errors and vulnerabilities, which are generally confirmed by our study. Our study extends theirs by including the machine's hardware and operational details, by finding and describing several new and serious vulnerabilities, and by building working demonstrations of several security attacks.'

The main findings of the study are:

- Any person with physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install malicious software easily.
- Malicious software running on a single voting machine can change votes with a low risk of detection, and modify the records, audit logs, and counters on the voting machine in such a way that even a forensic examination of these records will find nothing amiss
- The machines are susceptible to voting-machine viruses.
- It is recommended that election procedures are altered to ensure security.

A copy of the paper is available on-line at **http://itpolicy.princeton.edu/voting/**

For further items of relevance, see the papers provided by Andrew W. Appel in the case of Gusciora et al. v McGreevey, available on-line at **http://www.cs.princeton.edu/~appel/nj-voting-case/**

See also a report by the United States Government Accountability Office Report to Congressional Requesters (September 2005, GAO-05-956) 'Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed' Report available on-line at **http://www.gao.gov/new.items/d05956.pdf**

Electronic payments

China

On 26 October 2005, the People's Bank of China promulgated the 'Guidelines for Electronic Payment' on 26 October 2005.

News items:
Business Forum China 'Third Party Platform - Online Payment Practice in PRC' on-line at **http://www.bfchina.cn/index.php?option=com_content&task=view&id=45&Itemid=28**

Miller Nash 'Summary of new laws and regulations' 27 January 2006, on-line at **http://www.minterellison.com/public/connect/Internet/Home/Legal+Insights/Newsletters/Previous+Newsletters/A+-+D+Summary+of+new+laws+and+regulations**

Contactless card technology

The Royal Bank of Scotland carried out the first trial of the PayPass contactless cards from MasterCard in Scotland during the summer of 2006 as an alternative to low-value cash payments.

News report by Andrew Bolger, 'Contactless payment to change how we shop' Financial Times, Monday August 21, 2006, p 18.

Procedural rules

United States of America

Amendments to the Federal Rules of Civil Procedure dealing with electronic discovery and related matters have been published. The new rules and amendments have been passed to Congress and will take effect on 1 December 2006, unless Congress enacts legislation to reject, modify, or defer the amendments.

General site:
http://www.uscourts.gov/rules/#proposed080904

Available on-line at
http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf

Registration cards

Trans-National registration database

The Ninth Meeting of the international Porvoo Group took place in Ljublijana, Slovenia, between 11-12 May 2006 to review progress made towards an interoperable European electronic registration database. The aim is to promote a trans-national, interoperable electronic identity, based on a Public Key Infrastructure and plastic cards. The relevant resolutions that were published are as follows:

Resolution 1. European Citizen Card standard
The Porvoo Group welcomed the status report on the European Citizen Card standard where the first two parts are under ballot. The Porvoo Group endorsed the need for the additional parts on middleware and use cases and invited the Porvoo members to actively participate in the relevant groups.

Resolution 2. Common requirements
It was duly noted that the Common requirements as earlier endorsed by the Porvoo Group have been influential in the eID standardisation domain and did not ask for further action at this time. However if future developments –like the eID roadmap- might ask for it the issue will be reassessed by the Porvoo Group.

Resolution 3. eID Demonstrator
The Porvoo Group highly regards the work done by the Interoperability Demonstrator project and Bud

Bruegger. The Porvoo members noted that the IOP expert mailing list will now be hosted by the Italian government and is open to Porvoo participants. It was also agreed that more joint meetings focused on Interoperability testing in cooperation with the GCF, CEN TC 224 Working group 15 and other interest groups shall be arranged.

Resolution 4. CA demonstrator proposal
The Group acknowledged a proposal by Mr. Rissanen to exploit the possibilities to set up a two layer Consortium open to any CA fulfilling legal and other conditions set by the Consortium to discuss harmonization of global PKI services. The Porvoo Group will monitor this development and discuss the issue again in the Porvoo 10 Meeting.

Resolution 5. Liaison with eID related groups within EU Commission
The Porvoo Group will closely monitor the actions taken by the Member States and the EU Commission related to the eIDM as defined in the i2010 eGovernment Action plan. All Porvoo members are encouraged to be involved in this activity. The Porvoo Group will start a regular information exchange with the eEurope eGovernment Ad-hoc group on eID/eDOC roadmaps and eID interoperability for PEGS group within the IDABC programme which are to be active in the realization of the eID roadmap.

The Porvoo Group web site:
http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/20710B02C6C5B894C2256D1A0048E290

Full minutes of the meeting:
http://ec.europa.eu/idabc/en/document/5673/355

Electronic passports

Austria

The Austrian government will make a new electronic passport available to Austrian citizens as from 31 August 2006. The passports are issued in accordance with Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (L385/1 29.12.2004).

Apparently at the press launch, it was claimed an increased level of security will make them impossible to forge. A microchip is embedded in an inside cover page, containing most of the data set out in writing in the passport, including a facial scan of the bearer. It is also equipped with copy protection mechanisms, a digital signature and encrypted transmission codes which, apparently, make it impossible for unauthorised parties to read the information contained in the passport.

The price of the new passports will remain the same at €69 for adults and €26 for children.

Institute for e-Government web site:
http://www.uni-potsdam.de/db/elogo/ifgcc/index.php? option=com_content&task=view&id=20600&Itemid=128&lang=en_GB