Legal aspects of electronic signatures

G.C. Parry, M. James-Moore, A.P. Graves and O. Altinok

University of Bath
School of Management
Working Paper Series
2008.02

University of Bath School of Management
Working Paper Series

School of Management
Claverton Down
Bath
BA2 7AY
United Kingdom
Tel: +44 1225 826742
Fax: +44 1225 826473
http://www.bath.ac.uk/management/research/papers.htm

2008		
2008.01	Ana Lozano-Vivas & Fotios Pasiouras	The impact of non-traditional activities on the estimation of bank efficiency: international evidence
2008.02	G.C. Parry, M. James-Moore, A.P. Graves and O. Altinok	Legal aspects of electronic signatures

LEGAL ASPECTS OF ELECTRONIC SIGNATURES

G. C. PARRY*§, M. JAMES-MOORE†, A.P. GRAVES§, AND O. ALTINOK†

§ University of Bath School of Management
† Warwick Manufacturing Group, University of Warwick

*Corresponding author. Email: g.c.parry@bath.ac.uk

Abstract

The need for electronic signatures in management processes is becoming more important as value chain and supplier flows become fully electronic. Many operations and process managers have introduced electronic tools for sign-off within process flows. However, few realize the legal implications or validity of international processes that use electronic signatures. Fully electronic information flows facilitate global commerce, but when working in the global market place, international information transfers become subject to different legal frameworks. This article identifies the various UK, EU, and US legislative instruments concerned and articulates and compares the key elements of the regulatory regimes that are established. It also highlights some of the potential difficulties facing those working within an international arena in achieving legally sound electronic process flows.

Keywords: signature - digital signature - public key infrastructures (PKI's);

1. Introduction

The need for electronic signatures in management processes is becoming more important as process flows become fully electronic. When working in the global market place, international information transfers become subject to different legal frameworks. For electronic signature infrastructures to work effectively they require not only technological solutions but also an authoritative infrastructure. The absence of a common legal base regarding digital signature technology makes it very difficult for most businesses to implement a digital signature system. Business transactions can not be completed electronically unless digital signatures can be legally validated and enforced, which would require their acceptance as being legally binding during arbitration. There is conflicting opinion and uncertainty as to the legal basis of digital signatures. There are many loopholes that people can take advantage of, and little case law to act as a guide. This is currently seen as a barrier by many to the introduction of electronic value streams.

A brief overview of legislative issues may be useful in order to understand the overall situation of digital signatures in legal platforms. It is a complex issue which we have endeavoured to explain as clearly as we can, examining UN legislation and focussing on the EU and US markets.

There are two ways of testing the validity and effectiveness of a signature. The law might determine whether the signature has the required *form*, and offer a list of acceptable forms of signature, or *function* in order to be treated as legally valid. The second approach can be called the technology neutral approach (Reed, 2000).

Generally the technology neutral approaches allow the use of electronic signature and give the same legal status to electronically signed documents as hand written ones, without making any discrimination about the form of the electronic signature. This approach does not specify any technique in particular. Making the signing act technology neutral prevents legislative

problems with future technologies (Spyrelli, 2002). Therefore it is better suited to deal with potential future technologies than legislation that enforces a specific technology (Nagpal, 2002) However, it is also disadvantageous since it may give legal validity to substandard methods of authentication (Broderick, Gibson, & Tarasewich, 2001).

The legislation that will be discussed such as UNCITRAL, UETA, the E-Sign, EU Directive, and the Electronic Communications Act are all technology neutral.

2. UNCITRAL

The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce in June 1996 (Kuechler & Grupe, 2003). The Model Law was developed to establish internationally accepted rules for electronic commerce and to help structure a secure legal environment for e-commerce activities. Article 7 of the law addresses electronic signatures (Broderick, Gibson, & Tarasewich, 2001). It deals with the functions and the binding power of e-signatures and identifies full legal validity. It is very similar to other legislation, in that, it seeks to remove some barriers for digital signature usage, and promotes the use of common terminology when dealing with digital signature technology (Kuechler & Grupe, 2003).

It has a technology neutral approach, given that it focuses on the functional equivalency. It examines the traditional paper- based document requirements, such as ensuring that documents are reliable, traceable, and unalterable, and determines how those requirements can be satisfied in an electronic context. It does not suggest any specific technology (Broderick, Gibson, & Tarasewich, 2001).

After five years, the Model Law on Electronic Signatures was approved in July 2001 at the UNCITRAL meeting. It was designed to improve and refine the earlier UN Model Law on Electronic Commerce. UNCITRAL prepared this law to help international harmonisation of laws '*supporting certification processes, including emerging digital authentication and*

certification technology; the applicability of the certification process; the allocation of risk and liability of users, providers and third parties in the context of the use of certification techniques; the specific issues of certification through the use of registries; and incorporation by reference' (Ford & Baum, 2000).

Article 1 provides that the UN model Law on E-Signatures does not pre-empt consumer protection laws. The law also addresses public key infrastructures (PKI's) and issues relevant to certification service providers. It suggests that signatories pay attention to avoid unauthorised use of signatures, and take care in ensuring accuracy and completeness of information (Broderick, Gibson, & Tarasewich, 2001).

3. US UETA and E-Sign Act

The first law that was adopted by more than 22 states was the Uniform Electronic Transactions Act (UETA), which was developed by the National Conference of Commissioners of Uniform State Laws in 1999 (Kuechler & Grupe, 2003). This act states that e-signatures are legally accepted in court proceedings, and that they meet signature requirements (Spyrelli, 2002). It focuses on the requirements for creating valid electronic signatures and maintaining documents in electronic form (Mincoff, 1999).

After that, the Electronic Signatures in Global and National Commerce Act (E-Sign) was electronically signed into law by President Clinton on 30th June 2000, and effective as of 1st October 2000. E- Sign is a federal statute which pre-empts state law (Bell, Gomez, & Hodge, 2001).

E-Sign defines an electronic signature in *§106: Definitions* as:

> 'an electronic sound, symbol or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record'

The act is completely technology neutral for political reasons, so that pressing a touch-tone keypad, clicking I agree on a web page, typing the name at the bottom of e-mail can be considered as an electronic signature if it appears to be intended as a signature. The intent is more important than the technology. The fact that no standards are set for the technology to be used can be considered as a weakness of this act. The act also does not require that electronic signatures fulfil the same functional goals as hand-written ones (uniqueness, linkage to the user, data integrity) (Canter, 2001).

E-Sign provides non- discrimination and clarifies the legal status of electronic contracts, signatures and electronic records by implying:

- a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
- a contract relating to such a transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its information (Baum, 2001, Bell, Gomez, & Hodge, 2001) (E- Sign §101 (a) General Rule of Validity).

However the legal effect and validity of electronic signature are not defined in E-Sign. E-Sign neither obstructs nor advances enforceability. Parties using electronic contracts are left on their own to prove the non- repudiation of the other party (Broderick, Gibson, & Tarasewich, 2001). It does not address the liability issue (Bell, Gomez, & Hodge, 2001).The E- Sign Act also states that:

> "the requirement for retention of contracts and records is met by retaining an electronic record of the information".

It requires that the information remain available for access to both parties for the period of time required by law and 'in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise' (Kuechler & Grupe, 2003).

The Act exempts certain types of contracts, but both business to business and business to consumer transactions are covered (Broderick, Gibson, & Tarasewich, 2001). (§103: Specific Exceptions). However, even if it does not preclude contractual parties in the business-to-business sector from using electronic signatures, parties are left to agree on the validity of electronic signatures (Bell, Gomez, & Hodge, 2001). It focuses on consumer protection (§101: Consumer Disclosures). It also addresses '*retention of contracts and records and accuracy and ability to retain contract and records*', which is not mentioned in the UN Model Law. Both laws recognise foreign electronic signatures and certificates. If a country which bases its law on the UN Model Law transacts with a US firm, conflicts are likely to arise concerning issues such as what constitutes a reliable signature or whether adequate disclosures were provided to customers.

States are permitted to modify the Electronic Signature Act (§102: Exemption to Pre-emption), but only if they adopt the US Uniform Transactions Act (UETA), which is more comprehensive. UETA explains what constitutes a transferable record, and sets specific operating rules for creating contracts and modifications. It also identifies more protection for consumers and different safety procedures for storage and authentication of original documents. In many states UETA applies rather than E-Sign, and some states have their own digital signature laws. Whilst the E-sign and UETA acts appear legal and binding, in practice, no state has challenged the federal law so there is no significant case law that challenges and supports or undermines these acts (Garritano, 2006).

4. EU Directive for Electronic Signatures

On December 1999, Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures was enacted (Bell, Gomez, & Hodge, 2001). Article 1 defines the scope of the Directive as:

> 'The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification- services in order to ensure the proper functioning of the internal market.'

The Directive is a European Union level legal instrument which directs member states to pass national laws to implement electronic signature technology as stated in the Directive's rules. It gives flexibility to nations in order to accommodate different cultures giving the possibility of deciding whether to implement or not certain aspects. However this flexibility also creates differing national electronic signature frameworks, failing to satisfy its main goal of structuring a harmonised and coherent legal framework across the European Union.

The EU Directive incorporates the technology neutral approach of the UN Model Law on Electronic Commerce (Ford & Baum, 2000). Moreover it defines two different kinds of electronic signatures: *a simple electronic signature,* and *an advanced electronic signature.* The *simple electronic signature* is defined in Article 2.1. as:

> 'data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication"

where the *advanced electronic signature* is defined in Article 2.2 as:

> "An electronic signature, which meets the following requirements,
>
> a) it is uniquely linked to the signatory

b) it is capable of identifying the signatory

c) it is created using means that the signatory can maintain under his sole control ; and

it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable'

According to Directive Article 5 concerning legal effects of electronic signatures, currently only the advanced electronic signatures which are "*based on a qualified certificate and created by secure signature creation device*" such as digital signatures are fully legally equivalent to handwritten signatures, and for other forms of e-signatures, it states that:

'the legal effectiveness is not denied solely on the grounds that it is:

- In electronic form

- Not based upon a qualified certificate, or

- Not based upon a qualified certificate issued by an accredited certification-service- provider, or

- Not created by a secure signature creation device'

However, this statement gives freedom to the Member States to refuse to recognise electronic signatures for any other reason (Reed, 2005, Spyrelli, 2002).

Even with advanced signatures legal recognition is not always assured because of loopholes. Advanced signatures are only considered equivalent to hand written signatures. Therefore if a statute requires more than a handwritten signature, such as a signature in the presence of a public notary, an advanced signature will not be legally recognised. This really

restricts the applicability of the Directive given that in most of the European nations many transactions require more than a handwritten signature (Bell, Gomez, & Hodge, 2001).

This Directive addresses how electronic signatures are created and explains what type of organisational structure is needed in general terms. It gives legal recognition to documents electronically signed, like E-Sign, but it also prioritises the growth of a complex network of PKI's providing electronic certificates for the recognition and development of electronic signatures (Murray, 2003). It sets out the requirements for a qualified certificate, a qualified certificate provider, and secure signature creation devices in Appendices I, II, and III consecutively.

The Directive requires that the EU member states ensure that certification authorities (C.A.s) are liable for the damage caused to their customers who rely on a qualified certificate issued by them. It also provides that the C.A.s can limit their liabilities by limiting the use of their certificates (Bell, Gomez, & Hodge, 2001). Once more the rules are only applied to advanced electronic signatures with qualified certificates; the Directive does not address the liability of anyone else. Simple electronic signature providers are therefore held accountable in accordance with national liability rules. This may cause an uneven situation for electronic signature providers in Europe, since the national liability rules vary.

Article 3.2 of the Directive addresses the need for a voluntary accreditation scheme. Article 4 ensures that there is free circulation of electronic signatures in the European Union and there are no restrictions on the services on the certification services originating in any Member States if they comply with the Directive. In addition Article 7 provides that the foreign C.A.s are only recognised if there is a link with the EU, such as an arrangement between the EU and the relevant third country (Angel, 1999, Downing & McKean, 2001).

The Directive does not give precise and practical solution to both government and businesses; therefore businesses are confused and still await more liberal and less restricted regulations on e-signatures (Spyrelli, 2002).

5. Electronic Communications Act

English law has initially assessed the validity of signatures according to their form. From history it can be seen that case law recognised new forms of signature as valid such as initials, marks, seals, adoption of a printed name, and the use of rubber stamps (Mincoff, 1999). Now it assesses the validity in terms of the function performed by the signature method, which means it follows a technology neutral approach (Reed, 2000). The Electronic Communication Act is the consequence of this technology neutral approach.

After the EU Directive, the United Kingdom government issued a consultation paper on the implementation of the EU Electronic Signatures Directive in 19 June 2001. The Department of Trade and Industry's (DTI) initiatives, in preparing the consultation paper, helped the House of Commons pass the Electronic Communications Act. This Act transposed the EU Directive into national law in May 2000 (Downing & McKean, 2001, Saxby, 2001).

The Electronic Communications Act has three stated aims: to clarify the status of electronic signatures; to remove legal barriers to electronic communication and transaction, and to build confidence in public key cryptography. In order to achieve these aims, the Act implements legal recognition of electronic signatures, provides a framework for removal of legal obstacles to electronic documents replacing paper documents, and proposes a statutory voluntary approvals scheme for suppliers of cryptographic services (Murray, 2003).

The Act permits electronic signatures to be legally admissible in legal proceedings and to provide the authenticity and integrity of the communication or the data in accordance with the provision of section 7 (1) of the Act which states:

‘In any legal proceedings

(a) an electronic signature incorporated into or logically associated with particular electronic communication or particular electronic data, and

(b) the certification by any person of such signature,

shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication data.’

However it also requires that electronic signatures (a) *must be incorporated into or logically associated with a particular electronic communication or data,* and *(b) there must be a certification process* to provide authenticity and integrity of the communication and to have a legal effect. Therefore if someone receives an electronic communication, which is *(a) signed with an electronic signature,* and *(b) the certificate relating the electronic signature verified by a trusted party,* the communication is admissible according the provision of the Act. It defines the electronic signatures in section 7(2) of the Act as:

‘ (2) … an electronic signature is so much of anything in electronic form as-

(a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and

(b) purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication data, the integrity of the communication or data, or both’

This definition appears to be insufficient to implement the Directive’s ‘certified advanced electronic signature’ requirement in Article 5(1)(a) (Reed, 2000).

The Act touches upon the issue of the legal acceptability of electronic documents as replacements for paper documents in sections 8 and 9. It provides for the acceptability of the electronic documents on a case-by-case opt-in mechanism, and gives power to the relevant Secretary of State to provide secondary legislation (Murray, 2003).

The Act provides relevant legislative provisions relating to Certification Authorities (C.A.s). Part I of the Electronic Communications Act 2000 talks about cryptography service providers, and approvals. The voluntary accreditation schemes issue is touched upon in the consultation paper as well where it suggests that:

> 'member states may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification service provision' .

The UK government took a step further from that Act, and intended to introduce '*a statutory voluntary approvals scheme'* (19th June 2001, Mason, 2002, Saxby, 2001). As an alternative to the government implementing the approvals scheme, the tScheme has been established by the Alliance for Electronic Business to facilitate the approvals and standards for cryptographic services. The tScheme "is a non-statutory voluntary approvals regime" for trust service providers, or in other terms C.A.s. Even though the government (DTI) is working in partnership with the tScheme, it is private sector led. Therefore the government does not plan to introduce a voluntary accreditation scheme since the tScheme appears to fulfil the broad objectives for schemes in accordance with the Directive (Murray, 2003).

The consultation paper also addresses the supervision of certification service providers, and states that the DTI will maintain the supervisory role, but a review will take place after two years. However, the Act does not address the issue of liability of C.A.s. The DTI touches upon that issue in the consultation paper, and states that the liability of the C.A.s to its customers will be subjected to existing law, and it also mentions that if any type of encryption technology is exported from some other countries, then it has to be confirmed that

it is permitted by both sides: from which it is being exported and in which it will be used (Downing & McKean, 2001).

After The Electronic Communications Act in 2000, the UK government enacted the Electronic Signatures Regulations 2002 on the 8th March 2002. The main difference between these regulations and existing provisions in UK law regarding electronic signatures is that they implement the concept of advanced electronic signatures. The definition of advanced signatures and the Appendices I and II are adopted word by word in the Regulations.

The 2002 Regulations, in addition to the general provisions of the Electronic Communications Act 2000 regarding electronic signatures, have implemented the framework for digital signatures and a developed PKI into UK law (Murray, 2003).

6. EU-US Partnership on Governmental Level (TABD)

The TABD organisation tries to bring US and EU legislations on e-signatures closer in order to standardise the legal requirements of validity of e-signatures on a transatlantic level. Identrus plays an important role in this effort (Spyrelli, 2002).

Identrus is a joint European and American private sector initiative founded by some financial institutions including ABN-AMRO, Citibank, Industrial Bank of Japan, Bank of America, Commerzbank, Natwest Group, Barclays, Deutsche Bank, Sanwa Bank, Chase, Dresdner Bank, Scotiabank Group, CIBC, HSBC, Wells Fargo, and Hypo Vereinsbank (Ford & Baum, 2000). Identrust's main goal is:

> 'to ensure authentication of identity of the transacting parties, authorisation, confidentiality of communications, integrity of transmitted messages, and non repudiation of signatures over open networks and guarantee an interoperable system of e-transacting based on uniform standards and beyond any legal divergence'.

Every financial institution that joins Identrus becomes an accredited C.A. that has the same goal as Identrus. At the core of the Identrus solution is an international scale PKI through which businesses are certified via their financial institutions. The EU officially approved Identrus a few months after its establishment, and now there are approximately 50 banks worldwide that have joined Identrus.

There is also the VeriSign Trust Network, which is the largest certification authority network. It involves VeriSign, and expands the network continuously including major service providers such as British Telecommunications, KPN Telecom, Telia, and CIBC.

These initiatives on governmental and business level have started before the acceptance of the Directive on e-signatures and the E-Sign Act. But still the American and European legislators did not cooperate to find a common way to deal with this new technological issue, and build a compatible legal environment between the USA and EU. More surprisingly they followed completely different approaches toward the authentication methods.

As a transatlantic consensus has been successfully achieved in the 'Safe Harbour Agreement' on the protection of personal data of individuals, there is at least hope that it can be done for e-signatures.

7. Summary of Findings

Issues Covered	UNCITRAL	EU DIRECTIVE	E- SIGN	ELECTRONIC COMMUNICATIONS ACT	ELECTRONIC SIGNATURE REGULATIONS
Full legal validity	✓	✓ only to advanced signatures	Parties have to agree on the validity	They are admissible to provide authentication and integrity	Accepts it as a method of authentication
Technology neutral Approach	✓	✓	✓	✓	✓
Non - discriminatio n	✓	For simple signatures	✓	×	×
Consumer protection	×	×	✓	×	×
Supports PKI	×	✓	×	✓	✓
Is liability addressed?	×	✓only for advanced signatures	×	×	✓
Foreign e-signature Recognition	✓	✓ if there is arrangement in between	✓	✓	✓
Advanced signature recognition	×	✓	×	×	✓
Need for voluntary scheme to accredit signatures	×	✓	×	✓	✓

Table I summarises the key points of each legal framework, and compares them with each other.

8. Conclusions

There is, as yet, no globally adopted legislation, and very little case law. This leads to uncertainty regarding the legal status of e-signatures and e-signed e-documents.

At present the use of digital signatures is based on agreement between the communicating parties. In the United Kingdom there have been no test cases to determine the legal standing of a digital signature (Ganley, 1998).

For the time being, in the case of forgery of an e-authorisation or of alteration of a document, the legitimate person is liable to prove that he was victimised. Both Directive and E-Sign do not limit the liability in these cases, but it is very difficult to prove the invalidity of a signature which is issued by an accredited C.A..

Before starting to implement an electronic signature in a business it has to be recognised that the technology and the legislation are not adequate. Before implementing a solution, these questions have to be answered by solution provider:

1. Is the solution technically secure?
2. Is it enforceable? Is it easy to enforce? Am I covered legally?
3. Are my financial risks managed to a satisfactory level?

Currently, without an international legal framework, electronic signature processes may have to be reviewed on a case by case basis and independent legal advice may need to be sought to ensure compliance with differing international laws.

Acknowledgements

The authors would like to acknowledge leading UK Aerospace companies and many smaller ones contributing towards the UK Lean Aerospace Initiative research programme. Also the support of the Society of British Aerospace Companies (SBAC), and the Engineering and Physical Sciences Research Council (EPSRC).

References

Consultation Paper on EC Directive 1999/93/EC of the European Parliament and Council on a Community Framework for Electronic Signatures.In Industry, Department of Trade and, editor. 19th June 2001.

Angel, J. Why Use Digital Signatures for Electronic Commerce? *Journal of Information, Law and Technology* 1999 (2).

Baum, M.S. Digital Signatures and E- SIGN: Implications for PKIs, *The Verisign Internet Trust Symposium*. 2001. http://www.verisign.com/repository/esign10-00-msb.ppt.

Bell, J., R. Gomez, & P. Hodge. Electronic Signatures Regulation. *Computer Law & Security Report*, 2001.17(6): 399-402

Broderick, M., V.R. Gibson, & P Tarasewich. Electronic Signatures: they're Legal, now what? *Internet Research: Electronic Networking Applications and Policy*, 2001. 11(5): 423-34.

Canter, S. Electronic Signatures, *PC Magazine.* 2001: www.pcmag.com/solutions.

Downing, R. & R. McKean. Digital Signatures: Addressing the Legal Issues. *Business Credit,* 2001. pp. 44-47.

Ford, W. & M.S. Baum. *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Ed.)*. 2000. New Jersey: Prentice- Hall, Inc.

Ganley, M.J. Digital Signatures. *Information Security Technical Report*, 1998. 2(4): 12-22.

Garritano, A. E-Signatures Get OK from an Auditor. *National Mortgage News*, 2006. 30(37): 29-29.

Kuechler, W. & F.H. Grupe. Digital Signatures: A Business View. *Information Systems Management.* 2003. (Winter): 19-28.

Mason, S. The Evidential Issues Relating to Electronic Signatures. *Computer Law & Security Report*, 2002.18(3): 175-80.

Mincoff, M. An Overview of Electronic and Digital Signature Legislation and Regulation in the United States: Silanis Technology. 1999.

Murray, J. Public Key Infrastructure Digital Signatures and Systematic Risk. *Journal of Information, Law and Technology.* 2003. (1).

Nagpal, N. Electronic Signatures and the Law: Asian School of Cyber Laws. 2002.

Reed, C. What is a Signature? *Journal of Information, Law and Technology.* 2000. (3).

Reed, M. Discussant's response to "Outsourcing and foreign direct investment: Boon or bane?". *Review Of Agricultural Economics*, 2005. 27(3): 402-04.

Saxby, S. Cautious Progress on Digital Signatures. *Computer Law & Security Report*, 2001. 17(3): 146.

Spyrelli, C. Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach towards Electronic Authentication. *Journal of Information, Law and Technology,* 2002. (2).

University of Bath School of Management
Working Paper Series

School of Management
Claverton Down
Bath
BA2 7AY
United Kingdom
Tel: +44 1225 826742
Fax: +44 1225 826473
http://www.bath.ac.uk/management/research/papers.htm

2007		
2007.01	Fotios Pasiouras	International evidence on the impact of regulations and supervision on banks' technical efficiency: an application of two-stage data envelopment analysis
2007.02	Richard Fairchild	Audit Tenure, Report Qualification, and Fraud
2007.03	Robert Heath & Paul Feldwick	50 Years using the wrong model of TV advertising
2007.04	Stephan C. Henneberg, Daniel Rohrmus & Carla Ramos	Sense-making and Cognition in Business Networks: Conceptualisation and Propositional Development
2007.05	Fotios Pasiouras, Sailesh Tanna & Constantin Zopounidis	Regulations, supervision and banks' cost and profit efficiency around the world: a stochastic frontier approach
2007.06	Johan Lindeque, Mark Lund & Steven McGuire	Non-Market Strategies, Corporate Political Activity and Organizational Social Capital: The US Anti-Dumping and Countervailing Duty Process
2007.07	Robert Heath	Emotional Persuasion in Advertising: A Hierarchy-of-Processing Model
2007.08	Joyce Yi-Hui Lee & Niki Panteli	A Framework for understanding Conflicts in Global Virtual Alliances
2007.09	Robert Heath	How do we predict advertising attention and engagement?
2007.10	Patchareeporn Pluempavarn & Niki Panteli	The Creation of Social Identity Through Weblogging

2007.11	Richard Fairchild	Managerial Overconfidence, Agency Problems, Financing Decisions and Firm Performance.
2007.12	Fotios Pasiouras, Emmanouil Sifodaskalakis & Constantin Zopounidis	Estimating and analysing the cost efficiency of Greek cooperative banks: an application of two-stage data envelopment analysis
2007.13	Fotios Pasiouras and Emmanouil Sifodaskalakis	Total Factor Productivity Change of Greek Cooperative Banks
2007.14	Paul Goodwin, Robert Fildes, Wing Yee Lee, Konstantinos Nikolopoulos & Michael Lawrence	Understanding the use of forecasting systems: an interpretive study in a supply-chain company
2007.15	Helen Walker and Stephen Brammer	Sustainable procurement in the United Kingdom public sector
2007.16	Stephen Brammer and Helen Walker	Sustainable procurement practice in the public sector: An international comparative study
2007.17	Richard Fairchild	How do Multi-player Beauty Contest Games affect the Level of Reasoning in Subsequent Two Player games?
2007.18	Klaus Meyer, Saul Estrin, Sumon Bhaumik & Mike W. Peng	Institutions, Resources, and Entry Strategies in Emerging Economies