

# The IPTS REPORT

EDITED BY THE INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS)  
AND PART OF THE COOPERATION WITH THE EUROPEAN SOCIETY OF EVALUATION (EUROPE)



## SPECIAL ISSUE: e-PAYMENT SYSTEMS CHALLENGES FOR EUROPE

**2 Editorial. e-Payment Systems Challenges for Europe**  
*Ioannis Maghiros*

**18 Secure On-Line Retail Payments: The Potential of Public Key Infrastructures and Digital Signatures**  
*Clara Centeno*

**Mobile Payments: A Challenge for Banks and Regulators**  
*Malte Krueger*

**26 The Innovation Dynamics of Internet Payment Systems Development**  
*Knud Böhle*

**The Political Dimension of Payment System Innovations: The Case of Mobile Payments**  
*Joachim Henkel and Felix Zimmermann*

**34 Consumer Protection and Redress in e-Payments: Issues, Policies and Technologies**  
*Pravir Chawdhry and Marc Wilkens*

**BRIEF NOTE:**  
**Observations from the ePSO inventory**  
*Gérard Carat*

EUROPEAN COMMISSION  
Joint Research Centre

CEE: XV/18

THE IPTS REPORT

63

APRIL 2002

EDITED BY THE INSTITUTE FOR PROSPECTIVE  
TECHNOLOGICAL STUDIES (IPTS)  
And issued in Cooperation with  
the European S&T Observatory Network

PUBLISHED BY THE EUROPEAN COMMISSION  
Joint Research Centre  
ISSN: 1025-9384  
Catalogue Number LF-AA-02-063-EN-C  
DEPOT LEGAL: SE-1937-95

**DIRECTOR**

Jean-Marie Cadiou

**EXECUTIVE EDITOR**

Dimitris Kyriakou

**EDITORIAL BOARD**

B. Clements, G. Fahrenkrog, J. Gavigan,  
M. González, H. Hernández, D. Kyriakou, I. Maghiros  
(Production Manager), P. Sorup, A. Sorla, C. Tahir.

**PRODUCTION**

CINDOC-CSIC/BGS

**PRINT**

Graedel

**TRANSLATION**

CINDOC-CSIC/BGS

**COPYRIGHT**

The views expressed in this publication do not  
necessarily reflect those of the European Commission

© ECSC-EEC-EAEC Brussels-Luxembourg, 2002  
Reproduction is authorised, except for commercial  
purposes, provided the source is acknowledged.  
The EC may not be held responsible for the use  
made of the information.

**THE IPTS REPORT**

is published in the first week of every month, except  
for the months of January and August. It is edited  
in English and is currently available at a price of  
50 euro per year, in four languages: English,  
French, German and Spanish.

**SUBSCRIPTIONS**

For a subscription to The IPTS Report,  
or to amend an existing subscription, please

write with full details to:  
The IPTS Report Secretariat  
IPTS, JRC Sevilla  
Edificio Expo-WTC  
C/ Inca Garcilaso, s/n  
E-41092 Sevilla, Spain  
Tel: +34-95-448 82 97  
Fax: +34-95-448 82 95  
E-mail: [ipts\\_sec@jrc.es](mailto:ipts_sec@jrc.es)  
Web address: [www.jrc.es/iptsreport/subscribe.html](http://www.jrc.es/iptsreport/subscribe.html)

C O N T E N T S

European Commission Delegation  
Library  
2300 M Street, NW  
Washington, DC 20037

MAY 30 2002

**Special Issue: e-Payment Systems Challenges for Europe****2 Editorial. e-Payment Systems Challenges for Europe****5 Mobile Payments: A Challenge for Banks and Regulators**

Banks and telecommunications operators (telcos) are the most obvious candidates for offering mobile payments systems, and the entry of telcos in the market may increase competition and foster the development of cross-border payment solutions.

**12 The Political Dimension of Payment System Innovations: The Case of Mobile Payments**

The potential for mobile commerce is creating a need for mobile payments. To be successful standards will need to emerge, whether through regulation, voluntary agreements, or market forces. The quality of the services that are offered may depend on the form the standardization process takes.

**18 Secure On-Line Retail Payments: The Potential of Public Key Infrastructures and Digital Signatures**

Although the cost and effort required to implement public-key-based security has meant it has generally not been widely adopted, closer cooperation between the public and private sectors may create an opportunity for these technologies in the longer term.

**26 The Innovation Dynamics of Internet Payment Systems Development**

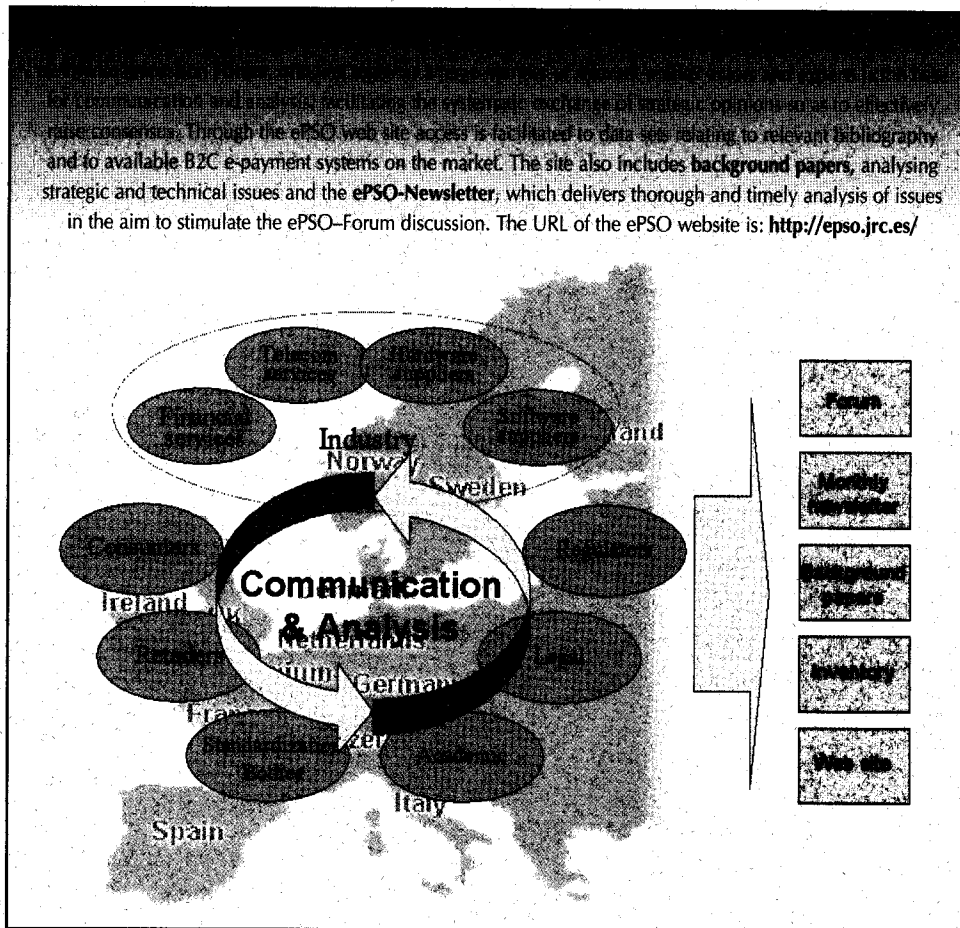
Competition between new start-ups and traditional financial institutions is gradually leading to payment systems better matched to users' needs. Innovation can be fostered in the field of payment methods suitable for digital goods and services and in the field of cross-border-commerce payments.

**34 Consumer Protection and Redress in e-Payments: Issues, Policies and Technologies**

Country-of-origin rules determining jurisdiction for intra-EU trade may force consumers to seek redress in a foreign country. Thus a variety of alternatives are emerging to help them do so, but Europe-wide measures may be needed to avoid consumer confusion and build e-confidence.

**41 Brief Note: Observations from the ePSO Inventory**

**Figure 1. e-Payment Systems Observatory Operation**



Payment Systems Observatory (ePSO) with the primary objective of **enhancing the information exchange in the field of e-payment systems**.

More than 3 years after its inception and after almost two years of operation, the ePSO (e-payment systems Observatory) project has become a visible instrument, as is witnessed by the growing number of ePSO web site hits, the quantity and quality of the comments that we get on the ePSO-Forum discussion list and by the 230 participants from 25 countries attending its final conference. During its operation ePSO has raised and discussed a multitude of issues, ranging from technological innovation, to business models, to legislative efforts to promote e-payments and subsequently e-commerce.

The issues discussed have included creating a 'trusted' environment, PKI implementation, paying for and building infrastructure, the impact of regulation, m-payments challenges, and creation of a European e-payments area. Banks, non-banks and "near-banks" have contributed to defining and pilot testing product and services that make e-payments more efficient. The Observatory project and its activities have contributed by ensuring that information exchange on the strategic options available has taken place among all interested players. By engaging the so-called network of correspondents, a network of academics and practitioners that exchange added value ideas, the Observatory has been able to produce a 'vision of the future' that in principle, through the Steering Group, could influence envisaged

# Mobile Payments: A Challenge for Banks and Regulators

Malte Krueger, *PaySys Consultancy GmbH*

Information and  
Communication  
Technology

**Issue:** Compared to other payment systems, mobile payments have the particular advantage that they can be used at the real point-of-sale, as well as in electronic commerce (e-commerce) and in mobile commerce (m-commerce). The current market penetration of mobile phones in conjunction with the expected growth of m-commerce, make it highly likely that m-payments will grow considerably over the next few years. While there are many actors that might be providing mobile payment services, banks and telecommunications operators (telcos) are the most obvious candidates for offering mobile payment services. Telco entry into the payment market would increase competition and might foster more efficient cross-border payment solutions.

**Relevance:** The effective functioning of m-payments will require cooperation and interoperability. This raises a number of competition policy issues, in particular with respect to pricing. In addition, non-bank activities in the m-payment sector raise a number of regulatory questions. At some stage the authorities may well have to consider the benefits of telcos becoming banks or Electronic Money Institutes.

## Introduction

Mobile payments or 'm-payments' (defined as payments that are carried out via the mobile phone) are expected to become an important part of the retail payments system. In principle, the mobile phone can be used at the real POS (point of sale), in e-commerce and in m-commerce. High levels of market penetration and a number of its technical features make the mobile phone an attractive device for making payments. Just like e-purses, most mobile phones have an embedded chip that can be used to store value or provide secure authorization and identification. In addition, the fact that the mobile

phone provides communication services means it does not have to rely on a card reader, PC (personal computer) and modem combination or a POS terminal. Therefore, it is not surprising that some experts believe that the mobile phone will replace smart cards as a means of payment.

One group of natural candidates for offering mobile payment services are mobile telephone operators. They have the customer base, they already do billing and they have the technical expertise. At the same time, they are looking for business models that will allow them to create revenue streams sufficient to justify their investments in expensive 3G (third generation)

channel, SMS or USSD (Unstructured Supplementary Services Data). Once the connection is established the customer can authorize the payment, usually using a PIN (personal identification number). Afterwards the customer and the merchant receive payment confirmation. Merchants usually receive the funds via payments into their bank account.

### The role of telecommunications companies

For mobile operators, mobile payments may be a key-sector and not just one of many possible

value-added services they can target. The existence of a convenient and cheap means of paying for 'mobile goods' is a pre-condition for the take-off of m-commerce. The lack of a convenient means of payment would hit mobile telcos in two ways: it would depress the volume of traffic on their networks and it would reduce revenues from the sale of value-added services. Thus, they are highly dependent on convenient mobile payment instruments.

Mobile telcos are natural candidates for providing payment services since they are already involved in billing for voice and data transport services anyway. Telcos already have experience

**Table 1. Some mobile payment systems as of December 2001<sup>2</sup>**

SUPPLIER	TYPE OF TRANSACTION
<b>Banko.max</b> (Austria)	Virtual POS
Bibit (Holland, international)	M-commerce (WAP-enabled)
Cellonet (Sweden, Netherlands)	Parking
<b>Cingular DirectBill</b> (USA)	Virtual POS
<b>EMT</b> (Estonia)	Parking
<b>GiSMo</b> (Sweden, UK, Germany)	Virtual POS
Metax (Denmark)	Real POS (filling stations)
Mint (Sweden)	Real POS
<b>NTT DoCoMo</b> (Japan)	M-commerce (subscription)
<b>Omnitel Onphone</b> (Italy)	Virtual POS
<b>Orange Mobile Payment</b> (Denmark)	Purchase of mobile air time
<b>Oskar</b> (Czech Republic)	Payment for prepaid and invoice
<b>Paiement CB sur mobile</b> (France)	Mail order and virtual POS
Paybox (Germany, international)	Real and virtual POS
PayDirect (USA)	Virtual POS, P2P
Payitmobile (Germany)	Virtual POS
Payline (France)	Virtual POS
PayPal (USA)	Virtual POS, P2P
Phonepaid (UK)	Virtual POS, P2P
<b>Sonera Mobile Pay</b> (Finland, Sweden)	Real POS (including vending machines)
StreetCash (Germany)	Real and virtual POS
<b>Telenor Mobil</b> (Norway)	Tickets
<b>Telia Payit</b> (Sweden)	Virtual POS
VisaMóvil (Spain)	Real and virtual POS
<b>Swisscom Sicab</b> (Switzerland)	Virtual POS
<b>Waaap Pag</b> (Brazil)	Real POS, top-up prepaid

Ventures in which mobile operators are participating are shown in **bold**<sup>3</sup>

Information and  
Communication  
Technology

*Although m-commerce is still a new phenomenon there are already a large number of m-payment systems in existence, most of which centre on a payment intermediary*

*Mobile telcos are natural candidates for providing payment services since they already have the experience and infrastructure to charge customers for a variety of services they or others provide*

The phone could be a dual-slot terminal<sup>4</sup> it could involve a separate payment chip embedded in the mobile phone, a multi-application chip with an embedded payment function, or it could use a separate card that communicates with the phone via a wireless network protocol such as Bluetooth.

Consumers would benefit from more convenient access possibilities. Given the established relationship of trust, consumers would most probably welcome the fact that banks continue to be the main payment service providers. However, a bank-dominated set-up would leave the competitive situation in the payment system more or less as it is. Since recent investigations into the payment system found evidence of non-competitive practices<sup>5</sup>, this would be a drawback. In addition, it has to be remembered that banks have been slow, so far, to come up with efficient solutions for cross-border retail payments and it is not clear that a further engagement in m-payments would change this.

The bank-dominated model is just one possibility. It is also conceivable that a different scenario will come about. Just like credit-card companies, telcos or other non-banks may offer payment services and use the Internet, the mobile phone or the PDA as an access device. As with credit cards, ultimate payment would be via bank transfer. However, banks would no longer be involved in the consumer-to-merchant or consumer-to-consumer side of the payment. Customer contact would move to a large extent to the intermediary. In principle, such intermediaries could offer a wide array of payments: pre-paid accounts, pre-paid cards, billing ("post-paid accounts") as well as traditional payments such as credit card payments or bank transfers (the German m-payment scheme PayBox would be an example of the latter).

The second scenario is much more likely to raise competition in the retail payment system. Even if new players may eventually have to become

banks, new entries would be beneficial. Furthermore, new intermediaries may be less reluctant to offer services across borders. For instance, telcos that operate internationally may also find it easier to offer international payment systems.

While some of these opportunities are open to non-banks, others might require them to acquire an EMI<sup>6</sup> (Electronic Money Institute) licence or even a banking licence. Alternatively, these non-banks could cooperate with a bank. For telcos, cooperation would have the advantage that they would not have to be concerned about payment regulation. Furthermore, they would lock-in a trusted brand and the risk-management know-how of banks. Banks have two incentives to cooperate with telcos. Firstly, it is in the interests of the banking sector as a whole to cooperate in order to prevent telcos from entering the market on their own. Individually, banks may see cooperation as beneficial because it helps them to gain customers and keep costs down. Furthermore, most mobile operators subsidize the price of mobile handsets. If banks want consumers to use a handset that is suitable for their m-payment schemes (for instance a dual slot phone) they would either also have to subsidize handsets themselves or cooperate with telcos.

### Regulatory issues

In the longer term, competition problems may arise as a result of network effects. There is little scope in the market for payment services for a large number of incompatible m-payment solutions. The usefulness of a payment system increases with the number of users. Therefore, users have a high preference for ubiquity. Ubiquity has two dimensions: first, a user wants the ability to send (receive) money to (from) any other user; second, a user wants to be able to use the payment function wherever he is (i.e. even outside of the reach of his service provider). Industries with large network effects provide a particular challenge for policy-makers.

*Banks have so far been slow to come up with efficient solutions for cross-border retail payments and it is not clear that a further engagement in m-payments would change this*

*Another scenario is that of telcos or other non-banks offering payment services using the Internet or mobile phone as an access device, while banks handle the actual payments, as they do for credit cards*

## Keywords

mobile payments, networks, telecommunications, banking

## Acknowledgements

This article is based on my work during a temporary assignment at the IPTS in Seville. I would like to thank Bernard Clements and my colleagues Knud Böhle, Gérard Carat, Clara Centeno and Ioannis Maghiros who worked with me on the ePSO project (Electronic Payment Systems Observatory) for their support.

## Notes/References

- 1. This section draws on the estimates of: Barnett, Nick, Stephen Hodges and Michael Wilshire, 'M-Commerce: An Operator's Manual', The McKinsey Quarterly, No. 3, 2000, 163-173.  
<http://www.mckinseyquarterly.com/electron/mcop00.asp>; BITKOM, 'Wege in die Informationsgesellschaft. Status quo und Perspektiven Deutschlands im internationalen Vergleich', Edition 2001.  
<ftp://www.bvb.de/bitkom/markt/060201/WegelInfo2001.pdf>; UMTS Forum, 'Enabling UMTS/Third Generation Services and Applications', Report No. 11, October 2000.  
<http://www.umts-forum.org/reports.html> and UMTS Forum, 'The UMTS Third Generation Market – Structuring the Service Revenue Opportunities', Report No. 9, September 2000.  
<http://www.umts-forum.org/reports.html>
- 2. A more detailed description of these schemes can be found in the ePSO inventory (<http://www.jrc.es/cfapp/invent/list.cfm>). Other projects that have been announced or are at the pilot stage: EMPS (Sweden, Finland), iCash (Sweden), Genion M-payment (Germany), Movipay (Spain) and mobilpay (Germany).
- 3. Mobile operators are also involved in a number of schemes that have not yet been deployed; for instance Telefónica, Airtel and Amena in Movilpago and Pagomovil (the two schemes have been merged to form 'Mobipay') and Telecom Italia Mobile in Easybuy.
- 4. An example of this would be the French "Paiement CB sur mobile" system.
- 5. See, for instance: Reserve Bank of Australia and Australian Competition and Consumer Commission, 'Debit and Credit Card Schemes in Australia. A Study of Interchange Fees and Access', October 2000  
[http://www.rba.gov.au/publ/pu\\_interchange.pdf](http://www.rba.gov.au/publ/pu_interchange.pdf) and Cruickshank, Don, 'Competition in UK Banking. Report to the Chancellor of the Exchequer', March 2000.  
[http://www.bankreview.org.uk/final\\_report.html](http://www.bankreview.org.uk/final_report.html)
- 6. The concept of the Electronic Money Institute was introduced in *Directive 2000/46/EC of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions* (known as the E-Money Directive). Available on-line at: [http://europa.eu.int/eur-lex/en/lif/dat/2000/en\\_300L0046.html](http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0046.html)

## Contacts

Dr. Malte Krueger, PaySys Consultancy GmbH

Tel.: +49 69 95 11 77 12, fax: +49 69 52 10 90, e-mail: [mkrueger@paysys.de](mailto:mkrueger@paysys.de)

Ioannis Maghiros, IPTS

Tel.: +34 95 448 82 81, fax: +34 95 448 82 08, e-mail: [ioannis.maghiros@jrc.es](mailto:ioannis.maghiros@jrc.es)

**About the author**  
**Malte Krueger** works as a consultant for PaySys GmbH (Frankfurt). He holds a Ph.D. in economics from the Universität Köln (Germany) and has worked as a research fellow for the Bank of Spain, the University of Western Ontario, the University of Durham and the IPTS. Dr. Krueger has published widely in academic and industry journals on foreign exchange markets, monetary policy and innovations in the payment system.

### Historical experience: the evolution of electronic direct debit schemes

The experience of past innovation in payment systems shows that standard setting frequently occurs outside of purely competitive market frameworks. Two other general mechanisms of standard setting can also be identified: voluntary cooperative agreements and coercive regulation<sup>1</sup>. In practice, combinations of these three paradigms can be observed, which can best be illustrated by the example of the evolution of electronic direct debit schemes. Box 1 describes Germany's experience of standardizing card-based electronic direct debit schemes, as an example of different standardization methods with policy relevance.

The example of standard setting in the German card-based payment services sector demonstrates the advantages and drawbacks of standard-setting mechanisms relying upon voluntary agreements and/or coercive regulation. Coercive regulatory power can be a quick way of achieving standardization, as it can be wielded by both public execu-

tive bodies and quasi cartels. It can significantly shorten the period of pre-standards competition in which several incompatible proprietary solutions compete in the market. However, there is a risk of coercive regulation setting standards which do not fully match the needs of customers in the market, but rather maximize the profit of the actor wielding the strongest influence over the standard setting body. This is less likely to occur in a competition-based standard setting process when competitive suppliers have stronger incentives to develop solutions which match their customers' preferences. Cooperative standard setting relies on voluntary agreements between independent actors. Compared to coercive regulation, it is therefore less prone to being captured by the interests of a single actor. However, a sufficiently large number of actors has to be included in the cooperative agreement to achieve the critical mass required for the innovation to spread. Yet if, in the extreme case, all companies from one industry agree upon a cooperative solution, they enjoy a quasi cartel position vis-à-vis future entrants as well as firms

*For interoperability to be achieved there needs to be standardization at the organizational level as well as technical interoperability*

*Coercive regulatory power can be a quick way of achieving standardization, but there is a risk of setting standards which do not fully match customers' needs*

#### Standardization in card-based electronic direct debit schemes

The German card-based payment systems has relied heavily on both voluntary agreements and coercive regulation. The initiative has generally been taken by the main German banking associations in cooperation with the ZKA (Central Credit Committee), which is a non-profit association of German banks. Since the nationwide introduction of the first card-based payment systems in 1990, the ZKA has emerged as the main standard setting body for card-based payment systems. Basically, the ZKA functions as a platform for agreements between the main banking associations and acts as a central clearing body for the card-based payment service industry. When the first authorization request-based system called *ec-cash* in 1990, it was criticized for being too expensive. The ZKA set relatively high charges for authorization requests, which were included with the help of independent payment network providers in introducing a non-standardized, considerably cheaper, no-authorization request-based system called "ELV systems" spread much more widely than the *ec-cash* system. The ZKA reacted by introducing a second system called POZ, which was a no-authorization request-based system. This relied on a simple check against a list of authorized merchants and did not incorporate a payment guarantee. So far, all three systems have been successful in the market. It is noteworthy that all three systems are fully interoperable with each other as customers can use their normal debit cards in all three systems. The main conflict between the systems only occurs from the perspective of card-based payment service providers, which is a complex matter between actors in different industry positions





## Keywords

compatibility, consortia, regulation, mobile commerce, mobile payment, standardization, voluntary agreement

## Notes

1. "Coercive regulation" can be defined as a process of top-down regulation whereby mandatory standards are set. Note that coercive regulation can be based either on the legal powers of political institutions or on de facto control over an industry as a result of market power. In the latter case, it may well favour the interests of one industry.

2. More detailed information about these and other forums can be found in the ePSO Newsletter 8&3 by Centeno (2001, <http://epso.jrc.es/newsletter/vol08/3.html>).

## Acknowledgements

The authors would like to thank several interviewees, in particular: Ulrich Dietz, Vodafone Pilotentwicklung; Jens Hinrichs, Go Solutions; Donald Müller-Judex, Payitmobile AG; Bernd Suckfüll, VIAG Interkom GmbH; Ralph Westenburger, Paybox.net AG; Ralph Woern, brainwork Consulting; Hans-Hermann Wolf, Siemens AG; Manfred-Kaspar Wolff, Telego! GmbH. Special thanks go to the "Arbeitskreis E-Payment", member of the "Förderkreis Internet-Wirtschaft München e.V."

## Contacts

Dr. Joachim Henkel, Institute for Innovation Research and Technology Management, University of Munich  
Tel.: +49 89 218 029 86, fax: +49 89 218 062 84, e-mail: [henkel@bwl.uni-muenchen.de](mailto:henkel@bwl.uni-muenchen.de)

Felix Zimmermann

Tel.: +49 80 318 29 85, e-mail: [felix@felixzimmermann.com](mailto:felix@felixzimmermann.com)

Ioannis Maghiros, IPTS

Tel.: +34 95 448 82 81, fax: +34 95 448 82 08, e-mail: [ioannis.maghiros@jrc.es](mailto:ioannis.maghiros@jrc.es)

17  
Information and  
Communication  
Technology

## About the authors

**Joachim Henkel** is an assistant professor at the University of Munich, Institute for Innovation Research and Technology Management. He holds a degree in physics and a Ph.D. in Economics. His research focuses on virtual communities, user-generated innovations, and e-payments. He is currently a visiting scholar at MIT's Sloan School of Management, Boston.

**Felix Zimmermann** studied economics and business administration at the Universities of Stuttgart-Hohenheim and Munich and holds an MSc in development studies from the London School of Economics. His research interests comprise innovation research and development economics. He is currently working at the German Chamber of Trade and Industry in Tokyo, Japan.

overall shopping process and constitutes a key element in building consumer trust (Cheskin, 1999). There are other important contributing elements such as a contractual framework, the merchant's use of trust marks, codes of conduct, data privacy statements, clear information on terms and conditions and pricing, the availability of effective dispute resolution procedures, customer service and the graphical design of the web site (OECD, 1999).

When analysing the security of the payment instrument, it is important to take into account the variety of instruments that consumers use when paying for e-commerce transactions (Böhle and Krueger, 2001). Some of these, the so called *on-line* payment instruments, are new or are used under new conditions (technical, procedural or legal) when used for e-commerce, such as debit and credit cards and credit transfers. Credit cards are the most frequently used on-line payment instrument with, on average, a 93% share (Gartner Group, March 2001). Others, the *off-line* payment instruments, such as cash on delivery, payment after invoice, money transfer and direct debits are already used in the physical market place, particularly in the distance selling market, and their use for e-commerce does not entail additional risks for the consumer. Table 1 summarizes the findings of a survey on how Europeans paid last year for on-line purchases.

This article focuses on the role that Public Key Cryptography, Public Key Infrastructure and digital

signatures can play as enablers for the deployment of secure *on-line* e-payments over the Internet<sup>1</sup>. Box 1 introduces the basic concepts of Public Key Cryptography, digital signatures, digital certificates and Public Key Infrastructure.

Despite the importance of the use of credit cards as a payment instrument, the statistics from the two US consumer complaint registrations available<sup>2</sup> indicate that less than 15-28% of transactions resulting in consumer complaints where paid by credit card, the majority of purchases being paid for by money transfers or cheques. Furthermore, only a fraction of the complaints related to payment fraud. These figures put into perspective the relative importance of e-payment fraud risk compared to other types of risks (e.g. auction fraud or non-delivery of merchandise), which should also be considered in an overall e-commerce risk analysis.

#### The nature and size of the fraud risk problem

In relation to the vulnerability of Internet communication networks, statistical fraud data highlight the following major e-payment risks that consumers and merchants face when using on-line payment instruments:

- Risk of merchant malpractice or fraud: bogus merchants carrying out data capture, disappearing and charging unauthorized transactions; merchants charging transaction amounts higher

**Table 1. How Europeans paid for on-line purchases in the past year**

Country	On-line (%)	Some on-line (%)	None on-line (%)
France	60	20	20
Germany	12	20	68
Italy	25	25	50
Spain	49	8	43
Sweden	17	10	73
UK	80	10	10

Source: Datamonitor, Oct 2001 (From the study "European ePayments 2002: opportunities and threats for FSIs", based on two surveys of 7500 and 6500 consumers).

*The security of the payment instrument plays a key role in the security of the overall shopping process and constitutes a key element in building consumer trust*

*Although credit cards are generally the most frequently used payment instrument, transactions paid for in this way account for only a small fraction of consumer complaints*

- than agreed or making unauthorized recurrent charges;
- Risk of identity and payment data theft for further fraudulent use on the Internet or in the physical world. Identity data can be stolen with unauthorized on-line access to merchant or bank servers, to consumer PCs or to transactional data;
  - Risk of misrepresentation, i.e., fraudulent use of consumer identity and payment data for purchasing, using data stolen in the physical world or on-line through the Internet;
  - Risk of a consumer fraudulently repudiating a transaction.

The statistical data available on e-commerce e-payment fraud, or on e-commerce fraud in general, is contradictory, incomplete and imprecise. This is due, among other things, to the nature of the data, the lack of up-to-date systems to identify Internet transactions, and also to the lack of a central point where consumers and merchants can report fraud suffered as a result of commercial transactions, independently of the payment instrument used.

Another difficulty for accurately assessing the Internet e-payment fraud risk and its trend is its intimate relation with other fraud areas such as: credit card payment fraud in the physical marketplace, fraudulent remote selling practices, cyber crime, Identity theft and financial fraud.

Collecting data from numerous sources makes it possible to outline, however, some significant fraud data:

- E-commerce-related card fraud in Europe is estimated at 6-9% of total card fraud, 0.25-0.35% of total e-commerce sales (Europay International, VISA EU, 2000). This is between 3 and 30 times higher than in the physical world (Visa, Celent Communications, 2000; Gartner Group, 2001).

- The Internet appears to be, indeed, a riskier environment for commerce than both the physical and distance selling market for a variety of reasons:
  - Merchants are smaller, with limited skills and budgets to invest in fraud prevention;
  - The environment is a more favourable vehicle for hackers to communicate and act, where access barriers are low and resources (hacking programs, credit cards numbers) can be exchanged and used anonymously;
  - Legal action is more difficult, because transaction values are generally low, the electronic evidence tools and skills available are very limited, and where transactions have taken place across borders complex jurisdictional issues may arise.
- E-commerce fraud is expected to grow, in line with growth trends in Internet access and e-commerce, as well as growth in card fraud in general (Europay International estimates a yearly increase of Card-Not-Present<sup>3</sup> fraud of 94% and counterfeit fraud 65% for the period of 2001-2004), cybercrime (Computer Security Institute, 2001) and identity theft (Celent Communications in 2001, estimates cases will triple between 2000 and 2005).

### The Security Requirements

In order to analyse the potential of PKC, PKI and digital signatures in securing on-line e-payments, it is first necessary to define the security requirements that derive from the analysis of e-payment fraud risks (see table 2).

In addition to the security requirements, additional aspects need to be considered for a secure e-payment solution in order to ensure consumer and market adoption, such as: user friendliness, acceptable cost, a degree of familiarity with the payment instrument (i.e. already used in the physical market place) (Berlecon Research,

*The lack of a centralized point where consumers and merchants can report fraud regardless of the method of payment used means that there is a lack of reliable data on e-commerce fraud*

*A number of factors, such as limited resources merchants can dedicate to security, the ease with which hackers can communicate with one another, and the jurisdictional complexities of small value and cross border transactions, can make the Internet a riskier environment than traditional channels*

In spite of the promising findings on the capabilities of the technology under analysis, research on which on-line payment solutions actually use PKC, PKI and digital signatures, shows low adoption. Indeed, while PKC is widely used on the Internet to provide data confidentiality and integrity (Secure Socket Layer -SSL), PKI is still in its infancy with regards to authentication and non-repudiation both in Business-to-Consumer e-commerce and in e-government.

Both private initiatives, such as trials of the SET payment protocol by banks, and public initiatives (FINEID project, Finland) have encountered common barriers for the implementation of PKI. These include insufficient consumer incentives for adoption to overcome the costs and effort required, a lack of incentives for banks to invest in greater security, the cost and complexity of the solutions, and a lack of technical interoperability between vendors. E-government initiatives, however, need to overcome particular legal, procedural and technical interoperability problems in order to achieve mutual recognition between central and local government departments and between countries.

Other cheaper and simpler technologies and mechanisms are being used to provide consumer authentication and to minimize the risk of repudiation. These solutions range from the use of passwords and user IDs, address validation, additional card data validation (number on the back signature panel), use of pseudo-random card numbers requested by the consumer from his/her bank for each payment transaction and use of virtual cards (for Internet-only use), to the use of mobile phones for identification, authentication and transaction signature and the use of Trusted Third Party intermediaries.

New approaches have been recently suggested by market actors such as Visa International (VISA *Authenticated Payment System* under the 3D-Mo-

*del* initiative, Sept 2001) and MasterCard (*Universal Cardholder Authentication Field - UCAF* together with *Secure Payment Application - SPATM*, May 2001), which aim at providing an acceptable level of security while solving the barriers encountered for SET deployment. However, the diversity of approaches and questionable business incentives call into question interoperability and market adoption by the different players.

### **Potential cooperation between the private and public sectors**

Following the analysis of the major challenges faced by private and public players in the implementation of PKI systems, closer cooperation between banks and governments as a possible way forward is being considered. Indeed, market analysis and development show that the two pioneer segments in authentication services are governments and financial institutions, and that both could take on a role as trusted third parties, under the PKI concept.

Collaboration between the private and public sectors in the definition and implementation of PKI and digital signatures could bring a number of potential benefits, such as:

- Synergies between retail e-payment services and e-government planned e-payment services both towards citizens and businesses, in both directions (e.g. tax payment and refund, payment of family allowance, e-procurement);
- Faster deployment of e-commerce infrastructure in the private sector by exploiting governments' role in infrastructure promotion;
- Development of economies of scale and acceleration of the development of the PKI services market, thanks to the opportunity for banks to exploit their capabilities (e.g., wide branch networks and knowledge of their customers, long service in the trust business, experience of mass smart card issuing, security

*Both public and private PKI initiatives have provided insufficient consumer incentives for adoption to overcome the barriers presented by the cost and effort involved. This has led to cheaper and simpler mechanisms predominating*

*Collaboration between the private and public sectors in the definition and implementation of PKI and digital signatures could bring a number of potential benefits such as synergies, economies of scale and a consistent and simpler user experience*

menting PKI and digital signatures could bring potential benefits in terms of cost-effectiveness and more rapid deployment and market adoption. Such a collaboration could solve a number of implementation barriers and provide a better case for market players to make use of PKI and digital signatures in order to secure on-line payments.

However, cooperation in this field would face a number of challenges, particularly as regards the sectors' disparate aims and concerns in terms of economic, interoperability, trust and data privacy issues, and given the differences in the nature and timing of the decision-making process in the public and private spheres.

### Keywords

e-commerce, e-government, on-line payments, security, public key infrastructure, digital signature

### Notes

1. This analysis is based on work done for the electronic Payment Systems Observatory (ePSO) project, particularly ePSO background paper No. 6 (Centeno, 2001).
2. The FBI Internet Fraud Complaint Center, 2000, and the Internet fraud Watch of the US National Consumer League, 2001.
3. A Card-Not-Present transaction refers to a payment transaction where the merchant is not able to see the card, such as in Mail Order, Telephone Order or Internet transactions.

### References

- Böhle, K. and Krueger M. *Payment Culture Matters – A comparative EU – US perspective on Internet Payments*. ePSO project – Background Paper No. 4, 2001.
- Centeno, C. *Securing Internet Payments: The Potential of Public Key Cryptography, Public Key Infrastructure and Digital Signatures*. ePSO project – Background Paper No. 6, 2001.
- Cheskin Research, Studio Archetype/Sapient, *eCommerce Trust Study*, January 1999.
- European Parliament and the Council of the European Union. *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*. Jan 19<sup>th</sup> 2000.
- The Government of Iceland's Committee on PKI. *Preliminary Study on Requirements and Comparable initiatives in other countries*. KPMG, 2001.
- OECD – Organisation for Economic Co-operation and Development. *Guidelines for Consumer Protection in the Context of Electronic Commerce*, Dec 1999.
- PKI Forum. *PKI Interoperability Framework*, 2001.
- Winn, J.K. *The emperor's new clothes: The shocking Truth about Digital Signatures and Internet Commerce*. Revised Draft – March 9, 2001.

### Contacts

Clara Centeno, Crescendo Consulting S.P.R.L., Brussels

Tel.: +32 278 43 979, fax: +34 636 21 47 01, e-mail: [ccenteno@compuserve.com](mailto:ccenteno@compuserve.com)

Ioannis Maghiros, IPTS

Tel.: +34 95 448 82 81, fax: +34 95 448 82 08, e-mail: [ioannis.maghiros@jrc.es](mailto:ioannis.maghiros@jrc.es)

### About the author

**Clara Centeno** has a degree in Telecommunication Engineering (UPC, Barcelona, Spain) and in Business Administration (CEPAC, Solvay, Brussels, Belgium), as well as over than ten years international experience in the electronic payments field, from both the business and technology perspective.

She has been an independent management consultant on electronic payments for Crescendo Consulting S.P.R.L. in Brussels since 1997, and has temporarily joined the IPTS to work on the electronic Payment Systems Observatory (ePSO) project.

for e-commerce, credit card information and bank account numbers were sent via the Internet without any security precautions. 1994 can be regarded as the year of birth of more secure payment methods: the introduction of SSL (Secure Socket Layer) by Netscape brought online security approximately up to the same level as when making credit card payments over the phone. At the same time start-ups such as DigiCash, CyberCash and First Virtual Holding entered the market place introducing novel payment methods designed specifically for use on open networks. These events, together with e-money developments outside the Internet, caused considerable irritation in the banking world. Taken to the extreme the potential of the new developments looked like a nightmare: E-money, technically insecure, issued by non-banks in offshore havens circulating through the borderless Internet from person to person like cash defied any control by payment authorities. Years later one is inclined to say that both new and old players and their proponents have – whether intentionally or not – tended to overstate the potential autonomy of new payment systems from the existing payment networks and banking infrastructure. The challenge posed to the banks by technology providers and new payment service providers (PSP) and the potential loss of control they represent, has been, and still is, undeniable.

In the light of the threat –whether real or imagined– from innovative payment methods, the banking sector tried to regain control through initiatives of its own. One important initiative was the credit card companies' development of a protocol called SET (Secure Electronic Transactions), which relies on Public Key Infrastructure (PKI) and requires the authentication of all the parties involved in card payments. It was meant to fight online-fraud, make SSL redundant, and to strengthen the position of credit card companies vis-à-vis their new competitors. Another response to the challenge was the outright adoption of the

new schemes by certain banks via licensing agreements or joint ventures. The DigiCash scheme, for example, was adopted by banks in the US, Finland, Norway, Austria, Germany, and Switzerland. Another option chosen by the banking sector was to promote the smartcard-based e-purses, designed originally for the use at attended and unattended Points of Sale, as well as for remote payments on the Internet. Neither of these approaches has turned out to be very successful.

The demise of first generation Internet payment systems began in 1998, when the FirstVirtual service was discontinued and DigiCash went bankrupt. The unfortunate micropayment ventures by technology providers such as IBM (IBM Micropay) and DEC/Compaq (Millicent) are further indicators of this decline. At the same time, efforts to push SET through were frustrated, and Internet enabled e-purses failed to attract merchants and online shoppers. Table 1 summarizes this short and tentative historical sketch.

More recently analysts have observed a second wave of new Internet payment methods such as 'prepaid dedicated accounts', sometimes requiring the purchase of a scratch-card, or 'virtual accounts', combining 'e-mail payments' and remote access to a virtual account enabling P2P (person-to-person) and B2C (business-to-consumer) payments. This latter trend first began in the US with PayPal and is closely linked to online-auctions. The new breed of Internet payment methods also covers 'private currencies' like beenz. The huge spectrum of mobile payment solutions for the real

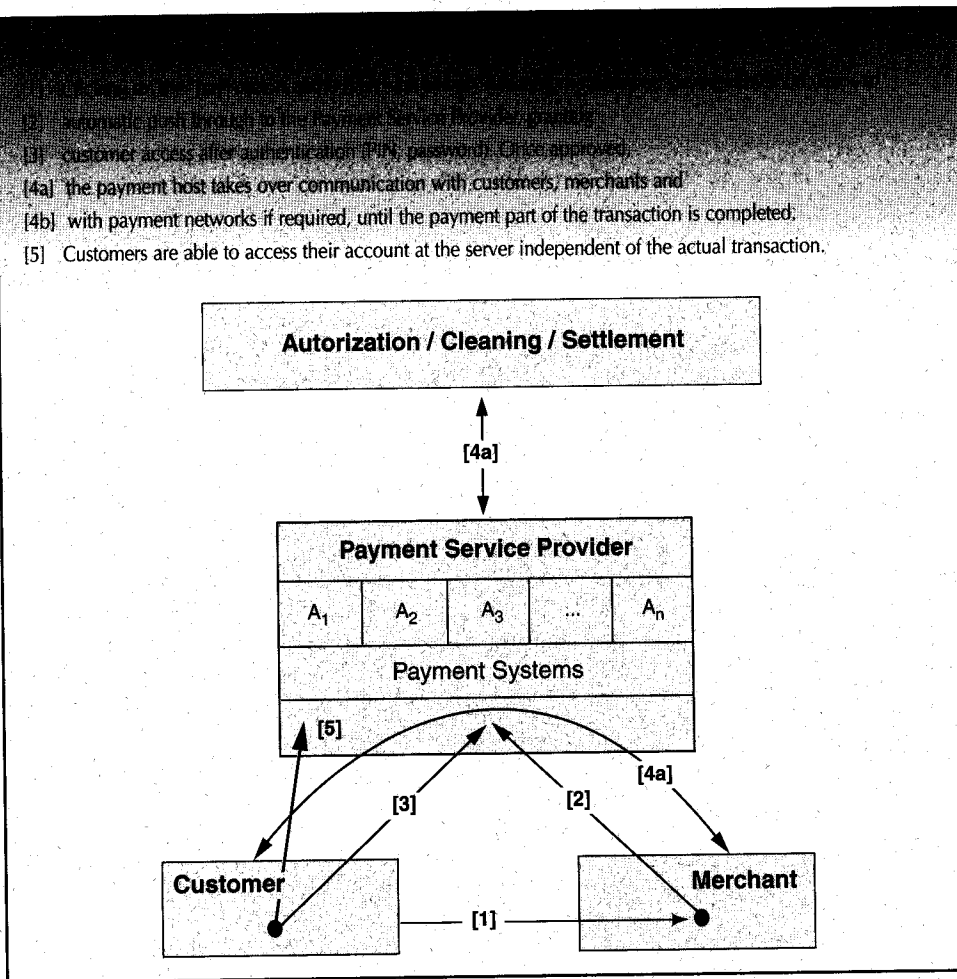
**Table 1. Tentative marks on the Internet payment systems timeline**

1992	Unsecured B2C payments on WWW
1994	Birth of more secure solutions by non-banks
1995	Bank and credit card company initiatives to catch up and to take the lead
1998	Demise of first generation internet payment methods
1999	Advent of Second generation Internet payments

*Banks were initially very concerned about the threat posed by borderless, cash-like e-money to the status quo in the banking industry. In the event, the impact of new payment systems has so far been slight*

*In response to the challenge of e-money banks either developed their own systems or adopted those offered by their new competitors*

**Figure 1. Internet payment scheme with a payment service provider as an intermediary**



Credit card companies have also drawn lessons from their earlier experience and proposed more 'lightweight', server based (non-PKI-based) authentication approaches. This paradigm shift (Böhle 2001 b and c) also covers other traditional payment solutions like direct debits (e.g. Belgium Banxsafe) and credit transfers (e.g. the 'electronic giro' in Finland), and also includes m-payments.

In addition to the steps towards a harmonized user experience there are further advantages to this new approach: mobility for the customers, device independence, operating system independence, and ease of maintenance for service providers.

This paradigm shift strengthens the role of Payment Service Providers, and the data show that this corresponds to a change in the behaviour of online merchants. Most of them now outsource the payment function. While in an earlier phase retailers wanted to take care of all functions in-house, today more and more functions (content hosting, payment hosting, and logistics services) are outsourced because of complexity and costs, and because the new intermediaries are gaining acceptance as 'trusted third parties'. Data from the UK show that of 10,000 retailers 9,950 have outsourced all or part of the payment function. It is mainly big companies that still do everything by themselves (ePSO workshop 2001).

*Drawing on the lessons of the first generation, second generation solutions tend to be less onerous for both users and merchants, with third party payment services providers acting as intermediaries*

*Whereas initially merchants tended to take care of payment functions in-house, recent data suggest that the majority are now outsourcing these tasks*



direct debits, credit transfers, virtual accounts, and mobile payment solutions are worth considering.

To start with e-purses, the CEPS standard (Common Electronic Purse Specifications) successfully demonstrated cross-border interoperability between national e-purses in the DUCATO project, which finished at the end of 2001. However, experts do not expect widespread rollout of CEPS compliant e-purses before 2005, and the work to further develop CEPS for the online environment has only just started. Bearing in mind also that the required smartcard reader infrastructure is not in place, it is clear that the e-purse remains a solution for the future with practically no relevance for cross-border payments today.

Looking at giro payments, i.e. direct debits and credit transfers, they are still very much bound to the national payment culture. Standards necessary for cross-border payments are under development, and the adoption of the IBAN (International Bank Account Number) and payment messaging standards like OFX (Open Financial Exchange) or ePI (Electronic Payment Initiator) developed by ECBS (European Committee for Banking Standards) are key elements (Leinonen 2001). While these standards are the basis, common user interfaces and integration with e-commerce systems are further steps forward. Integrated solutions of this kind exist at the national level but not at the international level. Cross-border European giro payments integrated into e-commerce also have to be envisaged, therefore, as a solution for the medium term.

In this situation virtual account systems run by non-banks like PayPal would seem to offer an alternative. Although technically a "non-bank", PayPal can be viewed as a type of huge online "quasi bank" where millions of customers and merchants have an account. As every transfer within the system is just an in-house transfer, there are no interoperability problems at this level. The

challenges for PayPal include multiple national regulations and the effort required to link to the numerous national banks and giro systems. This is perhaps reflected in the fact that although PayPal is currently available in eighteen European countries, disbursements into national bank accounts are only possible in five.

Turning to mobile payments, two important roles for them can be envisaged in the context of cross-border payments and e-commerce. Firstly, there is their potential as facilitators for cross-border giro payments<sup>2</sup>. The second role envisaged in this context for mobile payments would be to build on the potential of telcos for micro(billing) and micro-payments (prepaid schemes). Given that a fairly secure international wireless infrastructure is already in place, there could be an opportunity for these operators to play a major role as Payment Service Providers within the emerging international digital goods and services market.

### Conclusions

Observing the ongoing evolution of Internet payment systems has led to a number of lessons. Firstly, just as the acceptance of electronic payment systems in general is very much influenced by its most common alternative and competitor, i.e. 'cash', the acceptance of new integrated e-commerce payment systems is influenced by the existence of non-integrated payment alternatives which work well in many situations. Focussing on online payment systems, the important question is what lies beyond the credit card – especially when we look at cross-border B2C e-commerce payments. Any foresight on new and future solutions should take the availability of non-integrated payment methods and the dominance of credit card payments into account.

Secondly, the innovation dynamics of the first and second generation of internet payment systems

*Banking and payment systems have historically developed along national lines, leading to specific 'payment cultures' with a particular set of payment methods and different usage patterns in each country*

*A number of developments are taking place in the European cross-border payments field, but the need to work with the variety of existing institutions and regulatory frameworks in the Member States is an obstacle for start-ups*

**Keywords**

electronic payment systems, m-payments, Internet, E-commerce, European integration, globalization, foresight

**Notes**

1. The analysis presented here is based on work done for the ePSO project, particularly ePSO background paper No 3 (Böhle 2001b) and No 4 (Böhle and Krueger 2001). Online versions are available from the project's website at <http://epso.jrc.es>
2. Paybox is probably the best example of this at present. The company is currently operates in five European countries and provides cross-border payments between customers in those countries by channelling giro payments through Deutsche Bank, a major German bank. Paybox acts as a payment intermediary and the mobile phone is used as a standard interface.

**References**

- Böhle, Knud (a): *On Hype, Sacred Cows, Data Holes, and How to Cope with them*. ePSO-Newsletter No. 4 (January 2001). <http://epso.jrc.es/newsletter/vol04/6.html>
- Böhle, Knud (b): *The Potential of Server Based Internet Payment Systems – An attempt to assess the Future of Internet Payments*. EUR 19935 EN, Brussels 2001.
- Böhle, Knud (c): *Access is king: about the bright future of server-based e-payment systems*. ePSO-Newsletter No. 6 (March 2001). <http://epso.jrc.es/newletter/vol06/2.html>
- Böhle, Knud and Krueger, Malte: *Payment Culture Matters – A comparative EU-US perspective on Internet payments* EUR 19936 EN, Brussels 2001.
- Datamonitor *European ePayments 2002: opportunities and threats for FSIs. Report - DMFS1409*. London 01 Oct 2001.
- ePSO workshop: *Integration of Internet payment systems into e-commerce* Friday 9th of November 2001, IPTS Seville. Minutes at <http://epso.jrc.es/project/WTPminutes.pdf>
- Lafferty Publications: *Credit card use for Online Purchases by region*. available from ePayNews (retrieved June 2001) at <http://www.epaynews.com/statistics/purchases.html#29>
- Leinonen, Harry: *Developments in Retail Payment Systems. In: Bank for International Settlements. BIS Papers No 7. Electronic finance: a new perspective and challenges*. Basel 2001, pp. 61-68.

**Contacts**

Knud Böhle, ITAS, Forschungszentrum Karlsruhe

Tel.: +24 782 29 89, fax: +24 782 48 06, e-mail: [Knud.Boehle@itas.fzk.de](mailto:Knud.Boehle@itas.fzk.de)

Ioannis Maghiros, IPTS

Tel.: +34 95 448 82 81, fax: +34 95 448 82 08, e-mail: [ioannis.maghiros@jrc.es](mailto:ioannis.maghiros@jrc.es)

**About the author**

**Knud Böhle** holds a diploma in sociology and an M.A. in information science and has several years experience in the field of technology assessment of ICT. He joined the Institute for Technology Assessment and Systems Analysis of the Research Centre Karlsruhe and has led and worked on projects on internet payment systems and e-commerce since 1997. He is currently a Visiting Scientist at the IPTS (October 2000 to April 2002) where he has helped set up the European Commission's "electronic Payment Systems Observatory". His responsibilities at the IPTS include payment system developments and their policy relevance, editorial work and authoring for the electronic Newsletter ePSO-N, as well as moderation and analysis of the electronic discussion Forum ePSO-F.

jurisdiction, but issues such as the accessibility and cost of seeking redress in a foreign court of law for a small claim render the legal options impractical.

Novel mechanisms are therefore required to establish e-confidence. A number of complementary measures will be required to achieve this goal in a partnership between self-regulation and third-party mechanisms: codes of conduct, trust seals, alternative dispute resolution, and cooperation between the existing national out-of-court bodies for consumer disputes.

### Disputes in e-Payment

According to some estimates, 2-3% of e-Commerce transactions could result in disputes. E-disputes relate to problems such as non-delivery, unsatisfactory goods, etc., and quite often concern e-Payment either directly as a source of complaint or indirectly as a way of settling the complaint by means of a refund.

In B2C transactions, there are two main forms of e-payment: conventional plastic cards, and those developed for Internet shopping. For the purpose of e-disputes, the *form* of payment becomes relevant when either a dispute arises due to the payment method or the payment mechanism can act as an intermediary for settling a complaint.

Common problems relating to payments encountered in B2C transactions are: poor business process; poor security; intentional fraud. A recent survey highlighted common types of B2C disputes related to payments and charges (Consumers International, 2001):

- Charges without delivery
- Payment before delivery
- Currency conversion rates
- Cross-border transfer charges
- Payment security

- Legal compliance
- Fraudulent transaction

### Current Protection Mechanisms

In payment-related disputes, there are three main protection mechanisms:

- **Charge-back.** Banks issuing plastic cards operate a charge-back mechanism that enables the consumer to claim a refund for a disputed transaction. This mechanism can be applied in cases of over-charging, incorrect charging, charging without delivery, cancelled transactions and fraud. However the process is operated as a goodwill mechanism and can take weeks before a refund is made. By virtue of its status and role in the payment settlement process, the card-issuing bank implicitly acts as a trusted third party.
- **Conditional Settlement.** Also known as the escrow mechanism, it involves a trusted intermediary who acts as a guarantor for payment for goods or services ordered. Buyers can inspect merchandise before the seller is paid. Sellers ship the merchandise only if the escrow agent guarantees payment. Although the concept of conditional settlement is well understood by international businesses, it is a somewhat novel idea for lay consumers. Moreover, there is a need for minimum regulatory standards that escrow services must satisfy to have trust of the two parties as a trusted intermediary<sup>1</sup>.
- **Insurance.** Financial institutions and some trustmark owners offer insurance against fraud, wrongful business practices, and loss/damage of goods in transition as a part of their service. The consumer may have to pay a fee on an annual or per-transaction basis. The insurance model is well understood by consumers and can integrate the traditional protection mechanisms with the needs for trust in e-commerce.

*E-disputes relate to problems such as non-delivery, unsatisfactory goods, etc., and quite often concern e-Payment either directly as a source of complaint or indirectly as a way of settling the complaint by means of a refund*

*The three main protection mechanisms available for payment-related disputes are charge-back, where the consumer claims a refund for a disputed transaction, conditional settlement using an escrow mechanism and insurance*

European challenges include cultural, business, legal and technological dimensions.

### S&T issues in e-Payment Disputes

Apart from the technological challenges specific to online dispute resolution, there are several technological issues related to online transactions more broadly which must be addressed as complementary measures for enhanced trust and confidence. Those particularly relevant to resolving e-payments related disputes include authenticity, security, e-evidence and protection.

- *Authenticity of merchant and customer*  
Each party must be able to authenticate the identity of the other party.

- *Authenticity of transaction*

The merchant must be able to establish the genuineness of an order; the consumer must be able to have confidence in the delivery of the genuine goods ordered.

- *Security of transaction*

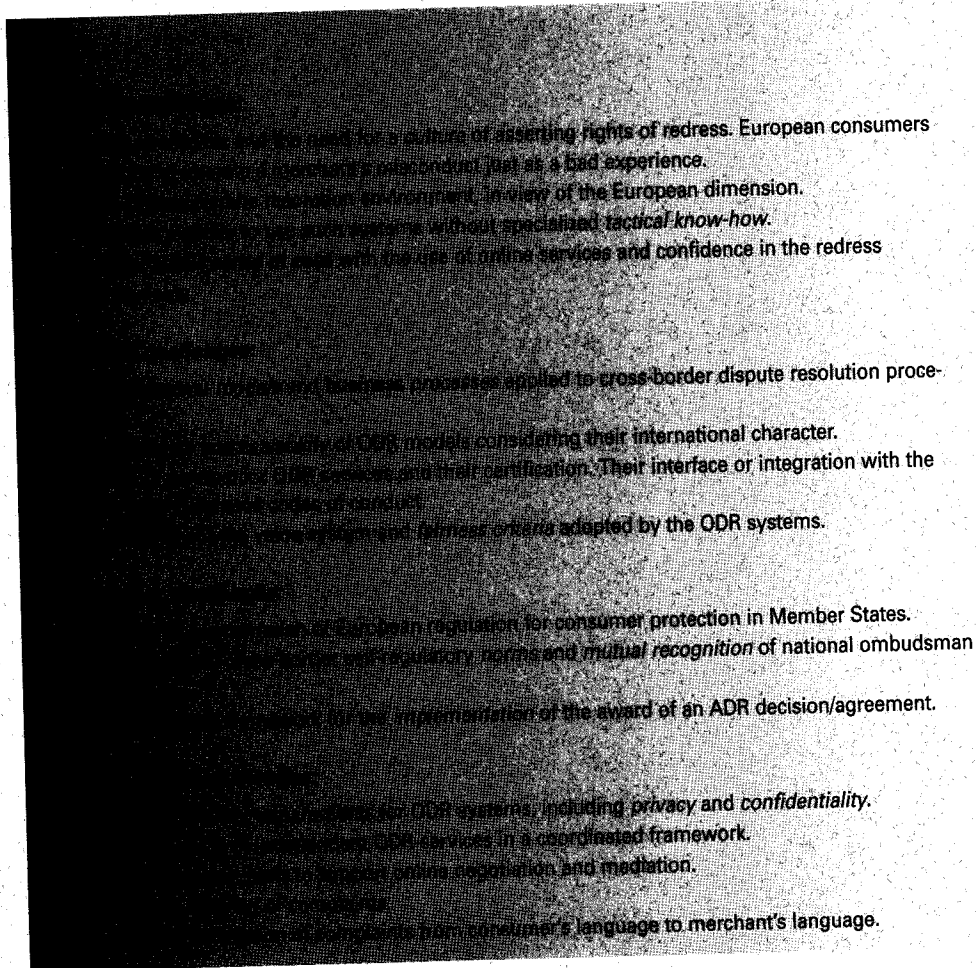
The transaction should take place in a secure environment: transfer of confidential information and goods delivery channels should be secure from external interference.

- *Electronic evidence of transaction*

A transaction log, including the offer of sale, order for goods, confirmation and payment authorization, must be created and deposited in an unalterable format at a trusted repository from where it can be retrieved, in event of a dispute.

37  
Information and  
Technology

*Apart from the challenge of finding a suitable business model for affordable and dependable ODR services, cultural, business, legal and technological issues need to be tackled*



codes of conduct consistent with the European consumer laws. Consumer- and industry associations are strengthening *self-regulation* by coming together to define a meta-code of conduct that would lead to higher quality trustmarks.

- **Generic Technology**

For cross-border dispute resolution networks such as EEJ-Net to function effectively and reliably, a number of technological issues need to be addressed: ensuring interoperability, platform-independence, multi-channel access and verifiable trust features.

Scientists at the EU Commission's Joint Research Centre (JRC) have defined *OdrXML*, a web-based to enable exchange of dispute documents between ADR bodies. A technology demonstrator shows communication and sharing of documents in a dispute resolution network<sup>3</sup>.

- **Future Policy Options**

Following the *e-confidence initiative* under *e-Europe*, various policy initiatives are being discussed to offer a cross-border ADR frame-

work. One possible solution promotes out-of-court dispute settlement systems in a cross-border European network, utilizing the existing ADR infrastructure. Such systems are seen as precursors and/or complements to judicial options, allowing cheaper, timely and easier access to justice in consumers affairs.

### Conclusions

Redress and protection mechanisms are essential for e-confidence. Efficient e-Payment mechanisms are not only key enablers for on-line transaction but can also play an effective role in dispute resolution. E-Payment mechanisms can be coordinated with dispute resolution to promote higher levels of e-confidence. Europe faces a mix of cultural, business, regulatory and technological challenges for a new cross-border redress infrastructure. European initiatives include regulation, self-regulation and cross-border redress networks. European e-commerce will benefit from greater consumer confidence through co-ordination between e-Payment, cross-border ADR services and other trust enhancing mechanisms.

*The European Extra-Judicial Network (EEJ-Net) aims to help EU/EEA consumers submit complaints to an appropriate ombudsman for any product sector*

*A trustmark is a recognizable logo granted to e-businesses that are compliant with a code of conduct.*

*However, the proliferation of trustmarks is causing confusion among consumers*

*For cross-border dispute resolution networks to function effectively and reliably, a number of technological issues need to be addressed*

# BRIEF NOTE

## Observations from the ePSO inventory

Gérard Carat, IPTS

41  
Information and  
Technology

We are currently witnessing the deployment of a host of internet-based payment solutions exploiting traditional payment systems in innovative ways. One of the deliverables of the ePSO project was the construction of an inventory of European consumer e-payment systems<sup>1</sup> in order to be able to look more closely at this new generation of internet payment solutions and identify potential trends. Having done so, we decided to further exploit the inventory by monitoring simple parameters to: 1) ascertain the validity of hypotheses set out in the ePSO background papers; 2) understand market trends in more detail; 3) and, possibly identify further policy relevant issues.

This note summarizes some of the observations derived from a selection of 100 e-payment solutions (see box 1) taken from the 180 ePSO inventory records compiled by November 2001<sup>2</sup>.

### Cooperation rather than competition

Telecom operators seem to favour partnership rather than competition with banks. And when they are in up-front competition against banks, telcos are in fact mainly acting in micropayments/micro-billing, a field where banks are not very active. This suggests a pattern of cooperation rather than competition between banks and non-banking institutions. This trend is also observable through the state of development of payment systems: The majority of the completed projects were initiated by non-banks, while schemes announced or at the pilot stage were mainly offered by mixed profile entities, indicating that the cooperative trend is likely to continue.

### Cross over between the Internet and the real-world

Payment systems designed for use on the Internet are also being used in real-world trans-

Payment systems monitored, as at Nov. 2001

	Bank	Non-bank	Mixed profile
Total:	100	70	30
	17	15	15
	59	19	100
	22	13	39
	41	20	

**Notes**

1. <http://epso.jrc.es/paysys.html> The ePSO database on e-payment systems monitors electronic payment systems, related projects and initiatives.
2. A full report on the analysis will be released in the first quarter of 2002 and published on the ePSO homepage.

**Contact**

Gérard Carat, IPTS

Tel.: + 34 95 448 83 53, fax: + 34 95 448 82 08, e-mail: [gerard.carat@jrc.es](mailto:gerard.carat@jrc.es)

43  
Information and  
Technology

**About the author**

**Gérard Carat** holds an MBA from ENST. Before joining the IPTS, where his current activities include the monitoring of the interface between S/T and EU policy and Marketing for the Institute, he worked at DGXIII on the team of the Advisor to the Director General on Economic and Strategy Aspects, Analysis and Forecasts, where he focused on market analysis of the telecoms and multimedia sector.

# A B O U T   T H E   I P T S

The Institute for Prospective Technological Studies (IPTS) is one of the seven institutes making up the Joint Research Centre (JRC) of the European Commission. It was established in Seville, Spain, in September 1994.

The mission of the Institute is to provide techno-economic analysis support to European decision-makers, by monitoring and analysing Science & Technology related developments, their cross-sectoral impact, their inter-relationship in the socio-economic context and future policy implications and to present this information in a timely and integrated way.

The IPTS is a unique public advisory body, independent from special national or commercial interests, closely associated with the EU policy-making process. In fact, most of the work undertaken by the IPTS is in response to direct requests from (or takes the form of long-term policy support on behalf of) the European Commission Directorate Generals, or European Parliament Committees. The IPTS also does work for Member States' governmental, academic or industrial organizations, though this represents a minor share of its total activities.

Although particular emphasis is placed on key Science and Technology fields, especially those that have a driving role and even the potential to reshape our society, important efforts are devoted to improving the understanding of the complex interactions between technology, economy and society. Indeed, the impact of technology on society and, conversely, the way technological development is driven by societal changes, are highly relevant themes within the European decision-making context.

The inter-disciplinary prospective approach adopted by the Institute is intended to provide European decision-makers with a deeper understanding of the emerging S/T issues, and it complements the activities undertaken by other Joint Research Centres institutes.

The IPTS collects information about technological developments and their application in Europe and the world, analyses this information and transmits it in an accessible form to European decision-makers. This is implemented in three sectors of activity:

- Technologies for Sustainable Development
- Life Sciences / Information and Communication Technologies
- Technology, Employment, Competitiveness and Society

In order to implement its mission, the Institute develops appropriate contacts, awareness and skills for anticipating and following the agenda of the policy decision-makers. In addition to its own resources, the IPTS makes use of external Advisory Groups and operates a Network of European Institutes working in similar areas. These networking activities enable the IPTS to draw on a large pool of available expertise, while allowing a continuous process of external peer-review of the in-house activities.