



ELECTRONIC PAYMENT SYSTEMS OBSERVATORY-

ePSO - NEWSLETTER ISSUES 9 - 15

SEPTEMBER 2001 - JUNE 2002



ABOUT IPTS

The Institute for Prospective Technological Studies (IPTS) is one of the seven Research Institutes of the European Commission (EC). These Institutes together make up the EC Directorate General known as the Joint Research Centre (JRC), which is the corporate research laboratory of the European Union with sites in Ispra (Italy), Geel (Belgium), Karlsruhe (Germany), Petten (the Netherlands) and Seville (Spain).

IPTS, established in Seville in September 1994, is a unique public advisory body, independent from special national or commercial interests and closely associated with the EU policy making process. In fact, most of the work undertaken by IPTS is in response to direct requests from the European Commission Directorate Generals, or the European Parliamentary Committees, or takes the form of long term policy support on their behalf. IPTS also does work for Member States' governmental, academic or industrial organisations, though this represents a minor share of its total activities.

Particular emphasis is placed on key Science and Technology fields, especially those that have a driving role and the potential to reshape our society, and effort is devoted to improving the understanding of the complex interactions between technology, economy and society. 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 fulfill 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, IPTS draws on a large pool of available expertise, while allowing a continuous process of external peer review of the in-house activities (<http://www.jrc.es>).

ABOUT ITAS

The Institute for Technology Assessment and Systems Analysis (ITAS) is one of 16 institutes within the Forschungszentrum Karlsruhe (Karlsruhe Research Centre). The Research Centre is a member of the Hermann von Helmholtz Association of German Research Centres. ITAS also runs the Office of Technology Assessment at the German Parliament (Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, TAB).

At the heart of ITAS' research work is the comprehensive analysis and evaluation of the development and application of technology and its inter-relationship with processes of societal change. Work is done on environment related, economic and political-institutional issues and results in the development and assessment of alternative options for action and design. This type of scientific treatment of complex issues is termed problem-oriented research and usually demands interdisciplinary co-operation. The ITAS web site provides – in both German and English – extensive information on the Institute, its staff, on-going and completed projects, publications and events. In addition, the TA-Datenbank-Nachrichten archive and selected contents of the TA-Database are made available in electronic form (<http://www.itas.fzk.de>).



ELECTRONIC PAYMENT SYSTEMS OBSERVATORY- ePSO - NEWSLETTER ISSUES 9 - 15

SEPTEMBER 2001 – JUNE 2002

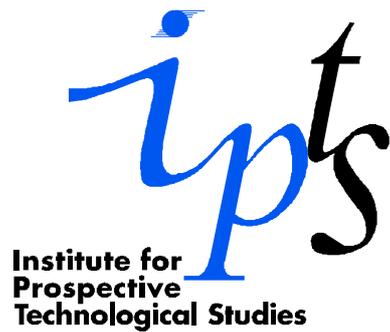


<http://epso.jrc.es/newsletter>

EUR 20522 EN

Michael Rader
ITAS
Co-ordinating Editor
Rader@itas.fzk.de

Ioannis Maghiros
IPTS
EPSO Project Leader
Ioannis.maghiros@jrc.es



European Commission

Joint Research Centre (DG JRC)

Institute for Prospective Technological
Studies

<http://www.jrc.es>

Legal notice

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of the following information.

Report EUR 20522 EN

© European Communities, 2002

Reproduction is authorised provided the source is acknowledged.

ABOUT ePSO

The Institute for Prospective Technological Studies (IPTS), part of the European Commission's DG-JRC, has set up an electronic Payment Systems Observatory (ePSO). The project is co-financed by DG Enterprise (ISIS Programme). The ePSO project's primary objective is to **enhance the information exchange in the field of e-payment systems** and thus contribute to the promotion of e-commerce in Europe. In order to achieve this, ePSO has set-up an electronic Forum of relevant actors and experts, which facilitates the systematic exchange of opinions with a view to enhancing the knowledge base, and working towards consensus.



<http://www.eps0.jrc.es>

How does the observatory operate?

A high level **Steering Group**, chaired by Mrs. Christa Randzio-Plath, MEP, President of the Economic and Monetary Affairs Committee of the European Parliament, provides guidance to the project.

A large number of experts and market players, participating on a voluntary basis, constitute the **ePSO-Forum**. This electronic discussion Forum, facilitated by the ePSO-team, addresses strategic and technological issues in the area of e-payment systems.

Background papers analysing strategic and technical issues are drafted by ePSO-team and reviewed and approved by the Steering Group before being presented to the Forum participants in order to raise awareness on controversial matters.

The **ePSO-Inventory** contains an updated data base of B2C e-payment systems for e-commerce and the comprehensive and up to date bibliographical database of Leo Van Hove.

A **conference** will set the stage for state-of-the-art e-payment systems presentations, reinforce and extend communication channels established by ePSO, and allow actors to exchange views on existing trends and future developments in electronic payment systems.

ePSO-Newsletter

ePSO-N, which is published monthly with the exception of August and January, is made available electronically free of charge on the web, and is edited by the Institute for Technology Assessment and Systems Analysis (ITAS) at Karlsruhe Research Centre, assisted by the ePSO team and an international network of experts. ePSO-N seeks to initiate informed discussion among stakeholders and other interested parties in the field of electronic payment systems and related e-commerce matters. Space for this discussion is provided by the ePSO Forum. Each issue of ePSO-N includes three to five articles on a special focus topic jointly selected by the editors and the network of correspondents. Beside papers discussing specific aspects of electronic payments, the newsletters contain interviews, country reports, news items, pointers to net resources, conference reports, facts and figures, plus a regular book review feature.

Foreword

The Electronic Payment Systems Observatory-Newsletter (ePSO-N) is one of the tools within the ePSO project used to structure the ePSO Forum discussions. ITAS of the Karlsruhe Research Centre has been awarded the task of elaborating and editing the newsletter. A collection of the first 8 issues of ePSO-N was published in 2001 and this volume contains the remaining 7 issues. It comprises a total of 56 articles on e-payment system related themes presented in a single volume, which will allow readers to browse through and may serve as a reference manual.

The Observatory Newsletter (ePSO-N) is the first ePSO deliverable to be produced; the first issue appeared in July 2000, and since then a total of 15 issues has been produced. It has been very well received by its public, despite the ever growing number of e-commerce related newsletters in circulation. It started with a subscriber base of over 200 people, before the Forum was operational, and is now regularly distributed to all ePSO-F subscribers (more than 500). It is also available on the ePSO web site for downloading; some 200 additional readers per month prefer to use this method of accessing the newsletter.

Designed to structure and stimulate the ePSO-F electronic discussion, ePSO-N presents high quality, timely and relevant articles supported by an international network of highly skilled correspondents [see section 15&9]. The ITAS staff responsible for editing ePSO-N, currently consisting of Michael Rader, Ulrich Riehm and Arnd Weber, manage the 23-strong correspondent team, who discuss, author, and review articles. Experts from outside this group have also submitted articles that have been edited and published in ePSO-N. Moreover, ePSO-F participants are invited to comment on issues presented in the articles and pose further related questions in the forum discussion, to which corresponding authors usually respond.

Short analytical articles addressing a rich variety of themes and providing insight into various e-payment topics are included in ePSO-N. In addition, each ePSO-N issue contains a special focus section consisting of three to five in-depth articles. Each issue's special topic is selected according to the need to follow wider developments in the e-payments field, covering persistent knowledge gaps as well as the broader requirements of the ePSO team in authoring background papers. The choice of topics tries to balance the diverse needs of the subscribers, some of whom are more interested in technological development and innovation in the field, while others are more concerned with policy implications. The six special topics addressed in this volume focus on:

- Security (two issues),
- Money services regulation in the US and Europe,
- Standards for payment systems integration,
- e-Payments in transport,
- Small value cross-border payments, and
- South East European transition economies.

In addition, country reports on payment systems in use help provide a better understanding of the different national payment cultures. Although ePSO-N concentrates on Europe (including Eastern European countries), developments in the US and Asia are also taken into account. Furthermore, EU funded e-payments projects are reviewed or their project leader is invited to present their findings through ePSO-N. Leo Van Hove, of the Free University of Brussels, presents a regular book review section entitled "Leo's corner". Last, but not least, an editorial introduces the issue, giving the personal opinion of the editor on the subject matter so as to further stimulate the debate.

We hope this collection of newsletters will raise awareness of the important issues in the field of e-payments and serve as a useful reference document.

The editors

ELECTRONIC PAYMENT SYSTEMS OBSERVATORY- NEWSLETTER ISSUES 9 - 15

Table of Contents 1 – organised by Issue

ISSUE 9 – September 2001

[9&1] *Editorial: Security and the Consumer* 9

Focus: Security (II)

[9&2] Risks in Using Personal Computers for Electronic Signatures and Electronic Banking 10

[9&3] Fraud in Electronic Payments: Achieving Security Standards 13

[9&4] DASIT: Privacy Protection in the Internet by User Control 15

[9&5] Creating Consumer Confidence: Current Efforts towards International Quality Criteria for E-Commerce 16

[9&6] Security & Trust: Taking Care of the Human Factor 19

Country Report

[9&7] Mobile Payments in the Baltic States 21

Leo Van Hove's Review Corner

[9&8] The Payment Blues of German Internet Merchants 24

ISSUE 10 –November 2001

[10&1] *Editorial: Authentication, Privacy and Regulation* 27

Focus: Security (III)

[10&2] Guaranteed Transactions, the Quest for the 'Holy Grail' 28

[10&3] Interview: Largest German Credit Card Issuer on Massive Reduction of Charge Backs 31

[10&4] Hi-tech Payment Technologies in Russia: The Case of Paycash 34

[10&5] JAP: A Cloak of Invisibility on the Internet 37

Miscellaneous

[10&6] Failure of Beenz and Flooz Indicates the End of Digital Web-Currencies? 39

News from the ePSO-Project

[10&7] ePSO Final Conference on Consumer Online Payments: Trends and Challenges for Europe 41

Leo Van Hove's Review Corner

[10&8] Meet the Heavyweight of Payment System Statistics: ECB's 'Blue Book' 42

ISSUE 11 –December 2001

[11&1] *Editorial: The Vulnerability of Technology – the Achilles' Heel of Globalisation* 44

Vulnerabilities of Payment Systems

[11&2] The Day After 45

[11&3] Worms, Disputes and Rolling Blackouts – Protecting the Citizen 47

Conference Report

[11&4] Innovations for an e-Society. Challenges for Technology Assessment :
A Note on the E-Commerce Track of the Conference 48

News from the ePSO-Project

[11&5] Integration of Internet Payment Systems – What's the Problem? 50

Focus: Money Services Regulation in the US and Europe

[11&6] The European Electronic Money Institutions Directive and the U.S.
Uniform Money Services Act – Similarities and Differences 53

[11&7] E-Money Regulation in the United States 55

Leo Van Hove's Review Corner

[11&8] E-money not ECLIPsed by Regulation 58

ISSUE 12 – February 2002

[12&1] *Editorial: Elegant Standards and Everyday B2C E-Commerce* 60

Focus: Standards for Payment System Integration

[12&2] The Internet Open Trading Protocol: What is it and why is it needed? 62

[12&3] Interview: Whether or not the Internet Open Trading Protocol (IOTP)
is successful depends on the definition of success 64

[12&4] The CEN/ISSS eWallet Project presents its work 67

Other Articles

[12&5] Paybest, an emerging micropayment solution for digital goods and services 69

[12&6] The CashCard: Lessons from Singapore 72

[12&7] How can PKI-services take off in Finland? From One ID-card to
Multiple Company and Customer Cards 74

Leo Van Hove's Review Corner

[12&8] “Survey of Electronic Money Developments”: BIS repetita placent 77

ISSUE 13 –April 2002

- [13&1] *Editorial: ePayments in Transport – High Speed Systems or Customer Monitoring?* 79

Focus: ePayments in Transport

- [13&2] Payment Solutions for Automotive Telematics 81
- [13&3] New Technology for Mobile Electronic Fee Collection 83
- [13&4] ERG Buys Proton 85

Third Party Billing

- [13&5] Billing Woes 87

Security

- [13&6] Success Factors for Credit Card Fraud? An Illustrative Example: the Yescard 89
- [13&7] Internet and Mobile Security in Singapore 91

Leo Van Hove's Review Corner

- [13&8] The ePSO Final Conference: Hopefully not the End 92

ISSUE 14 – May 2002

- [14&1] *Editorial: Cross with Old Banking Boys' Cross-border Retail Payment Networks* 95

Focus: Small Value Cross-Border Payments

- [14&2] Interview: The Road to Efficient Cross-border Retail Payment Systems in Europe: Long and Winding or Straight Through? 97
- [14&3] Cross-border Low-value Payments. What is Likely to Emerge from the EC Legislation? 102
- [14&4] The Cross-border Payments Malaise: M-payments to the Rescue? 106
- [14&5] Back to Tin Foil and Banknotes? The Trials and Tribulations of Petty Cross Border Trading 108

Consumer Online-Payment Survey

- [14&6] Expanding Niches. Some Results of an Online-survey about Online-shopping and Paying 109

News from ePSO

- [14&7] Internet Banking Workshop – A Spanish and European Perspective of the Future 112

Leo Van Hove's Review Corner

- [14&8] Recommendation 97/489/EC Revisited: A Case of Frustrated Expectations? 113

ISSUE 15 – June 2002

[15&1] *Editorial: Payment Transition from the Balkans to the Dnjepr* 116

Focus: South East European Transition Economies

[15&2] Interview: Mobile Banking on Low-cost Networks in Romania 118

[15&3] Evolution and Present Status of Bulgarian Card Market 122

[15&4] EU-funded Balcard Project: Targeting the Unbanked Internet Buyers 124

[15&5] Ukraine – from "Specific Units" towards Electronic Payments 125

Miscellaneous

[15&6] I-Payments Strategies 127

Report about the ePSO Project

[15&7] ePSO Final Report 128

Leo Van Hove's Review Corner

[15&8] Bye, Bye Banknotes? 135

Of Contacts, Correspondents and Disclaimers

[15&9] Masthead 138

TABLE OF CONTENTS 2 – organised by topic 139

INDEX OF NAMES 142

ePSO Newsletter – Issue 9, September 2001

Focus: Security (II)

[9&1]

Editorial: Security and the Consumer

Michael Rader (rader@itas.fzk.de), Arnd Weber (arnd.weber@itas.fzk.de), ITAS, Karlsruhe, Germany

*/consumer protection/digital signatures/secure operating systems/pseudonyms/
evaluation/trustmarks/usability*

Is it possible to make an order on a network securely while using the same end-user device for downloading all sorts of code? How can consumer rights, requirements and interests be taken into account when designing payment instruments and on-line shops? Approaches for solving such issues are discussed in this issue.

Predictions for the growth of electronic commerce from the end of the last millennium are now proving to be wide off the mark. We vividly recall an article predicting the imminent end of the high street as consumers changed more and more to buying from the comfort of their living rooms. Even at that time there were surveys which revealed that the most important barriers for consumer adoption of e-commerce were security, privacy of personal data and trust. In more concrete terms, the major concerns of consumers are or were theft or abuse of personal information such as credit card numbers, non-delivery of items and uncertainty concerning consumer rights, or unauthorised and undesired sale or transfer of personal data for marketing purposes.

Measures to counter these concerns are a common thread running through almost all of the articles included in this issue of "ePSO-N". The dilemma facing "supply side" actors is that all of these measures cost money and that consumers' willingness to pay for something that they would not need shopping on the high street is probably severely limited. The challenge is obviously to provide a range of solutions offering protection of varying degrees so that customers can choose according to personal preferences, such as confidentiality and comfort, and depending on who currently bears the risk in situations where things can go wrong.

In the first article, Hanno Langweg reports about ways to create malicious code, so-called Trojan horses, for attacking digital signature solutions on PCs. Of course, similar attacks can be made to abuse passwords in solutions without signatures. Can we be sure that insuring these risks will be the best? The author discusses the use of technical means to make such attacks more difficult, if not impossible. One way would be to use more hardware which can't be manipulated, such as tamper resistant chips and WORM-media, with the objective to make attacks more costly, so that they won't happen. Another way would be to use a secure operating system, which is designed to keep viruses or other malicious code away from sensitive applications, to make attacks through the network impossible. The operating systems specialists know design principles to protect a banking application from any other, even on a Windows machine. This would allow a secure application to run in a secure environment. Sounds fascinating?

How would you know an instrument is secure? Whose security needs does an instrument protect? One way would be to use components from a trustworthy manufacturer. Another way would be to use components the design of which is open and has been investigated by the interested security community. The latter investigation is, of course, neither necessarily structured nor easy to judge by laypersons. Formally evaluating components can be a more comprehensive way, and competent institutions could certify a component and put a logo or something similar onto it. Luigi Sciusco provides an overview of the issues involved in arriving at secure components, and emphasises the core role of documents defining the requirements. Will such "protection profiles" take into account the needs of banks, merchants and consumers? See Luigi's article for an overview of the issues.

German DZ Bank, formerly DG Bank, has a pilot running to test two things. One is to use pseudonyms to protect the privacy of Internet shoppers. DZ Bank believes that lack of trust in privacy is a major obstacle for increased use of on-line networks. The other thing being tested is to have the consumer digitally sign the consent for processing of personal data. See Matthias Enzmann's and Günter Schulze's article for details on the DASIT project.

Florian Egger and Dennis Abrazhevich provide suggestions in their article on how to design the user interface of security solutions. They emphasise that any instrument needs to be seen in the context of the whole purchasing process for creating trust.

This reminds us that Internet shoppers may fear poor or late delivery, and may distrust remote merchants. Dirk Klasen provides an overview of many initiatives aiming at creating reliable trustmarks, assuring users that a certain merchant offers certain means of protection. Doing this understandably on a global scale appears to be a challenge.

Other Articles

In our section "country reports" Ülle Adamson and Kaido Kaarli report about mobile payments in Estonia. They draw an amazing picture of a Baltic transition economy in which payment for car parking is increasingly done via mobile phones.

We conclude this issue with Leo van Hove's review of a survey of merchant views of payments in electronic commerce. The survey, conducted by Berlecon Research, Berlin, not only analyses the current situation of Internet merchants, but also examines whether new means of payments will reduce some of the problems faced by merchants, such as chargebacks.

A Thousand Readers

In June, more than 700 people accessed the newsletter from the Web-site, up from about 200 at the beginning of the year. In addition to this, we now have 550 subscribers. In total, this means that the ePSO-Newsletter is now read by more than 1,000 readers. We would like to thank you all for the trust that this reflects and take the opportunity of reminding you that a major function of the articles contained in this newsletter is to spark debate in the "ePSO Forum". The Forum is another important component of the ePSO project and serves the purpose of bringing together all actors involved in the development and application of electronic payment systems to state clearly their interest and views. For this purpose, we have recently added a link to the Forum at the foot of each article. It would please us greatly if this feature found your approval by making intensive use of it.

[info]

- See the Security Notice of the German Regulatory Authority for Telecommunications and Posts (www.regtp.de) for what appear to be repercussions of Hanno's work.

[9&2]

Risks in Using Personal Computers for Electronic Signatures and Electronic Banking

Hanno Langweg (langweg@informatik.uni-bonn.de), University of Bonn, Germany

/security/digital signatures/electronic banking/consumer protection

Signing a document or transaction electronically on a personal computer will have legal consequences in a growing number of countries. Untrustworthy programs pose a threat to the signing process. We surveyed software for the creation of electronic signatures – and were amazed that there was little protection against attacks on the software. We think that manufacturers should improve their products to better protect the end-user.

1. Introduction

Software for the creation of electronic signatures and for home banking applications performs a delicate task. Signing a document or transaction will have legal consequences in a growing number of countries, therefore the security of the software on the user's computer is an important issue. In the past, Trojan horses (i.e. untrustworthy programs) have proved to be a growing concern for end-users. Software for electronic signatures must be protected or provide protection against Trojan horses attacking the process.

In our scenario a Trojan horse is a program with a hidden functionality running on the user's computer. It may send messages to other programs running in the same session. In Microsoft

Windows, programs can communicate with each other sending Windows messages, e.g. "reveal the text displayed in a window" or "key 'A' has been pressed". These messages can be used by a Trojan horse to get information from another program (e.g. retrieving a PIN) or to remotely control another program by simulating user action (e.g. placing transactions in a home banking application).

During our research on the preservation of integrity against Trojan horse attacks we surveyed software for the creation of electronic signatures. However, the methods could also be applied to payment systems. We were amazed that there was little protection against attacks on the software.

2 Lack of protection

We tested five programs for the creation of electronic signatures for their susceptibility to Trojan horse attacks (Deutsche Post eTrust Mail, Utimaco Safeguard Sign&Crypt, Deutsche Telekom PKSCrypt, SSE TrustedMIME, Giesecke&Devrient GDtrust Mail). The selection is not representative; the programs were available for purchase in Germany and usually able to facilitate a smart card to store the secret keys and to compute the signature. In our research the tests conducted only played a minor role so we did not set up a comprehensive test scheme. We rather focused on what an attacker would be able to do with limited knowledge and resources. The simulated attacks used Microsoft Windows 98 and 2000 as a platform.

In our study we concentrated on three vulnerabilities a Trojan horse would be likely to exploit:

- Capturing the PIN (personal identification number) to access the smart card
- Modifying data before it is processed by the signing software
- Modifying data between the signing software and the smart card

2.1 Capturing the PIN

Most programs use a smart card for the storage of the signatory's private signing key and for the computation of the signature. The smart card is regarded tamper-resistant and a Trojan horse should never be able to obtain the secret information from the card.

To obtain the PIN in our tests we did not modify the operating system and we did not employ keyboard loggers to observe key strokes. The protection offered by most programs is to display asterisks instead of numbers. We sent a standard message in the Windows messaging model to the applications requesting the content of the PIN input field. Four out of five applications responded with the PIN.

2.2 Modifying data before it is processed by the signing software

The user works with an application software to create and modify the data that is going to be signed. At some point he decides to finish the work and sign the data. The document is then transferred from the application software to the signing software, sometimes displayed again for confirmation, and finally transmitted to the signature smart card that computes the signature. A Trojan horse can attack many interfaces, including the application software (e.g. as a macro), the transfer between application software and signing software, the signing software itself, the device driver between signing software and smart card.

None of the products surveyed cared about the origin of the data to be signed. Three of the five programs signed the data without verifying its correctness. The other two offered a viewer, and one of them was easily modifiable. Sending four messages in the Windows messaging model sufficed to corrupt the "*what-you-see-is-what-you-sign*" pledge. The security consisted of setting the read-only property of the richedit control. While preventing a user from typing in the viewer, the application allowed other programs to change the contents.

2.3 Modifying data between the signing software and the smart card

At least one of the programs allowed a Trojan horse to modify the communication between the signing software and the signature smart card. The last command, after authentication, was not protected by secure messaging. Hence, a malicious smart card reader device driver could alter the communication to get different data signed.

3 Approaches to provide higher protection

We propose some low-cost and easy-to-use measures to avert attacks of the kind presented. The idea is that the process of creating an electronic signature involves a chain of components. This chain is only as strong as its weakest link. While the smart card can be regarded as secure against software attacks, the other components mostly cannot. Increasing their strength against attacks increases the strength of the whole chain. Not providing the PIN to programs that ask for it should be obvious. Using a smart card reader with an integrated keyboard would be even better and prevent keyboard logger attacks. The communication between software and smart card should employ cryptography for every command, especially sending the data to be signed. While this advice is not new, we propose a novel method for obtaining untampered input to the signing process. A *write-once-read-multiple* medium should be used to store the data to be signed. Once the data is stored it cannot be modified. The aim is not "absolute" security. However, the effort needed by an attacker to circumvent the protection can be raised.

These measures have to be applied in a comprehensive architecture. Just fixing one problem may create another. For instance, using a dedicated keyboard to input the PIN directly, interrupts the connection between user and signature software. The software cannot prove it is actually being used by the user. The communication protocol has to be extended to include authentication of the signing software to the smart card.

Enhanced protection of the applications themselves can be supported by the operating system. There are two aspects that can be discussed here. One is strengthening the operating system against attacks, the other is reducing interference with possibly malicious programs.

- *Trusted Computing Platform Alliance (TCPA)* is an industry work group, supported by major companies, focused on enhancing trust and security on computer platforms. The goal is to build secure software applications on top of a verified computing base without the need for additional expensive hardware. Starting from a hardware module that is resistant against software attacks, the integrity of components involved in the boot process of a computer is verified. The results of these measurements can be reliably retrieved by software that needs certain components to be trustworthy. Unfortunately there is only a specification. The group still has to deliver compliant components.
- *Perseus* is a security kernel. Its trusted computing base provides basic security services to protect critical applications against malicious code. The design is clear enough to be formally verified. To provide backward compatibility Perseus acts as a host which executes a common operating system as a task. The system is intended to be applicable to low-cost personal security devices (e.g. PDAs) but can also be applied to other computers with e.g. Linux or Windows. However, a security application has to be modified to work under Perseus and to be shielded from malicious code. Device drivers have to be developed to be compatible.

4 Conclusions

With our analysis we focus on some attacks that every attacker with no inside knowledge of the signing software can perform. In the current implementations the surveyed products offer almost no protection against attacks by Trojan horses. Even using Windows NT/2000 does not offer help, since manufacturers offer the same software for Windows 98 and 2000.

We think that there is opportunity to improve the security of signature software applications by careful design of the whole signing process. This will be easier with home banking applications since their communication with other programs is traditionally limited. Robust applications may be supported by an enhanced operating system.

As long as the mechanisms available are not used, waiting for operating system enhancements simply appears as an excuse

[info]

- Bontchev, V. (1996). 'Possible macro virus attacks and how to prevent them'. *Computers & Security* 15(1996):595-626.
- CEN/ISSS Workshop on Electronic Signatures (2001). N 141. CEN/ISSS WS/E-Sign; PT on Area G1; Draft CWA: "Security Requirements for Signature Creation Systems". <http://www.ni.din.de/sixcms/detail.php3?id=389>

- CERT Coordination Center (1999). CERT Advisory CA-99-02-Trojan-Horses. <http://www.cert.org/advisories/CA-1999-02.html>
- European Parliament and European Council (1999). 'Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures'. *Official Journal of the European Communities* No. L 13(2000):2. http://europa.eu.int/eur-lex/en/lif/dat/1999/en_399L0093.html
- Pfitzmann, B., Riordan, J., Stübke, C., Waidner, M. and A. Weber (2001). *The PERSEUS System Architecture*. IBM Research Report RZ 3335 (#93381) 04/09/01, IBM Research Division, Zurich. <http://www-krypt.cs.uni-sb.de/~perseus>
- Spalka, A., Cremers, A.B. and H. Langweg (2001). 'Protecting the Creation of Digital Signatures with Trusted Computing Platform Technology Against Attacks by Trojan Horse Programs'. Proceedings of IFIP/SEC'01. <http://www-student.informatik.uni-bonn.de/~langweg/research/sec01t.pdf>
- Spalka, A., Cremers, A. B. and H. Langweg (2001). 'The Fairy Tale of »What You See Is What You Sign«. Trojan Horse Attacks on Software for Digital Signatures'. Proceedings of IFIP Working Conference on Security and Control of IT in Society-II. <http://www-student.informatik.uni-bonn.de/~langweg/research/scits01.pdf>
- Trusted Computing Platform Alliance (2001). *TCPA Trusted Subsystem Specification Version 1.1*. <http://www.trustedpc.org>
- Deutsche Post Signtrust, <http://www.signtrust.de>
- Deutsche Telekom T-Telesec, <http://www.telesec.de>
- SSE, <http://www.sse.ie>
- Utimaco Safeware, <http://www.utimaco.com>
- Giesecke & Devrient, <http://www.secartis.com>

[9&3]

Fraud in Electronic Payments: Achieving Security Standards

Luigi Sciusco, (sciusco@tiscalinet.it), Rome, Italy

/security/evaluation/digital signatures

Security evaluation criteria were born in the military environment but their application to IT commercial products is rapidly gaining momentum. A "security certificate" could be of particular interest for IT products that need high levels of trust, like Internet payment platforms. The article describes the main goals of the evaluation and certification process and its limits.

Today the majority of consumer Internet payments are made with credit cards: the problems due to fraud and validation failures are widespread but there is no evidence to suggest that such fraud is due to interception of credit card data. Rather, it is a consequence of the remote, non-face-to-face nature of Internet transactions, combined with security lapses at the customer and merchant ends. It is well accepted that cryptographic techniques, based on electronic signatures and electronic certificates, are the best way of providing the level of trust required for electronic business exchanges. The minimum requirements for the key generation devices and signature generation and verification instruments are often stated in terms of satisfying *standardised evaluation requirements*. According to the Italian digital signature legislation, for example, key generation has to be evaluated against ITSEC E3 while signature functions have to be evaluated against ITSEC E3 (generation) or E2 (verification). With this approach the importance of IT security is clearly stated in the legal and regulatory framework but IT security evaluation is left to specialised and accredited organisations, usually on a commercial basis. The final goal is to enhance confidence of citizens in the new electronic payment instruments.

Most IT consumers lack the resources necessary to judge whether their confidence in the security of their IT products or systems is appropriate, and they may not wish to rely solely on the assertions of the developers: they may therefore ask for a security evaluation. The most widely used evaluation criteria in Europe are ITSEC and Common Criteria. Common Criteria may be considered to have advantages over the ITSEC criteria as they represent the latest thinking on how criteria should be established and they have been standardised on a global basis (ISO 15408).

Evaluation criteria are the "standards" against which security evaluation is carried out. They support the development of standardised sets of IT security requirements by user communities. Manufacturers can use similar sets of requirements to describe the security capabilities of their products. Security evaluations are formalised testing and analytic processes to determine whether IT products have been correctly developed to specification and whether they are effective in countering the security problems as claimed. The evaluation criteria are used in two general ways:

- As a standardised way to describe security requirements. A community of users can decide that a standardised set of security capabilities should be used in software or hardware on their systems. They will begin to write a “user document” (a Protection Profile, in the Common Criteria terminology) to express those common requirements, according to the chosen evaluation methodology. They will first identify the type of product envisioned and the general IT features needed. They will then consider the environment in which it will operate, in particular identifying the security problems and challenges that must be addressed. This activity is, in essence, a risk analysis and leads to a statement of general needs or security objectives to be met both by the product and by its environment. The methodology will help them to transform the security objectives into a set of IT security functional requirements. Based on the desired level of confidence in the security of products to be built, an evaluation level is assigned. (Note that the higher the evaluation level, the greater the burden on the product developer, and consequently the more time and money needed to bring the product to complete availability). It is *desirable* that the “user document” be submitted to an independent *evaluation facility*, usually a commercial company, for evaluation to ensure that it is correct, complete, and internally consistent. The “user document” may then be entered into a central registry for use by the community to communicate the product security needs to manufacturers. The preceding scenario involving a user community is only one possible approach. It is also possible for one or several manufacturers to develop a “user document” that incorporates the features of their products, as a means of communication with potential users.
- As a sound technical basis for evaluating the security features of these products and systems. In a typical product evaluation scenario, a manufacturer identifies a “user document” incorporating the product desires of a group of users and potential customers. The manufacturer builds the product, following the “user document”-specified requirements, according to the methodology. Once the product is built, the manufacturer prepares a “developer document” (Security Target, in the Common Criteria and ITSEC methodology), which makes a claim of compliance with a particular “user document”. The manufacturer then submits the “developer document”, the product, and accompanying documentation to an accredited, independent *evaluation facility* for evaluation. If the product passes evaluation, it may be submitted to a *certification body* for validation of the evaluation results. The certification body is an independent organisation that issues a publicly available document which summarises the results of an evaluation and confirms the overall results. While definitely preferable, it is not necessary for a product to claim compliance with a “user document”. In the absence of “user document” claims, the “developer document” is prepared in a process similar to that described for the “user document”. The evaluation of the “developer document” and then the corresponding product can proceed as before, but no “user document” compliance claims will be examined, as typical in ITSEC.

It is worthwhile emphasising that with the security evaluation we do not know if the security objectives really fit the environment of the system or if the identification of the threats and the choice of the security functions are correct: in other words, a security evaluation is not a risk analysis and it does not express any opinion about the risk analysis process. Moreover, it does not take into consideration “non-technical” security functions (e.g. physical access and environmental protection, organisational and procedural security functions involving the staff); finally, it does not evaluate the strength of the algorithms and of the cryptographic protocols.

No evaluation is able to say that a system is absolutely “secure”: the evaluation process establishes only a level of confidence that the security functions of such products and systems and the assurance measures applied to them must meet. Therefore we could have a complex system with many sophisticated security functions with a low-level evaluation (e.g. ITSEC E1) or the same system with few security functions with a high-level evaluation (e.g. ITSEC E5): the reason is that the evaluation assumes that the risk analysis is correct. That is why user communities and Authorities can play an active role in writing consistent “user documents” otherwise software developers can use the security evaluation as a marketing tool.

[info]

- A short survey on IT security standards: <http://www.iso.ch/iso/en/commcentre/pdf/ITsecurity0006.pdf>
- National Security Authorities: www.bsi.de www.tno.nl www.cesg.gov.uk
www.radium.ncsc.mil/tpep/library/ccitse www.scssi.gouv.fr

[9&4]

DASIT: Privacy Protection in the Internet by User Control

Matthias Enzmann (matthias.enzmann@sit.fraunhofer.de) and Günter Schulze (schulze@sit.fraunhofer.gmd.de), Darmstadt, Germany

/data protection/pseudonyms/digital signatures

Internet services like news-reading and online shopping are making their way into our daily life. However, convenience to use these services practically anywhere and anytime might come at a high price: the consumers' loss of privacy. Taking the service providers' position, this fear, even if not always justified, hinders many people from using these services, and thus, wastes great consumer potential. DASIT offers a practical framework that allows consumers to better control and protect their personal data.

The research project DASIT, conducted by the German DZ Bank (formerly DG Bank; project leader), Fraunhofer Institute for Secure Telecooperation (FhI-SIT, formerly GMD-SIT) and law experts from the University of Kassel, took on the problem of privacy friendly shopping and payment over the Internet. DASIT stands for „Privacy Protection in the Internet“ (Datenschutz in Telediensten), and it is supported by the German Ministry of Economics (BMWi). The motivation for BMWi to support such a project was to find out if shopping and payment over the Internet is economically and technically feasible in a way that is compatible with Germany's data protection laws. The final prototype developed within DASIT is the first, and to date only, implementation that completely satisfies all requirements of German privacy law.

One of DASIT's main features is the customer's ability to use pseudonyms to hide her true identity from the Internet shop, while not giving up the possibility to get orders delivered at her home address, despite the fact that the address is never revealed to the shop. In addition, by using a pseudonymous payment system, revealing the customer's identity is also not necessary for billing purposes. This is privacy friendly in the sense that the merchant may re-identify the user via her pseudonym but cannot directly link this pseudonym to the customer's real identity, and thus, the merchant cannot do "bad things" with his customer's personal data.

DASIT's realization of pseudonymous payment and delivery is based on the idea that personal data should only be disclosed on a "need to know" basis. Therefore a merchant learns only the user's pseudonym, to build customer relationships, and thus is able to link the content of the user's shopping basket (the goods to be ordered) to the pseudonym. However, since the customer is in full control of her identity, she can even use different pseudonyms for different shopping transactions at the same merchant's, and thus prevent the merchant from linking her transactions. Finally, the merchant's transport agent learns only the customer's name and address, which is directly sent to him by the customer along with a merchant generated order ID. This order ID uniquely identifies the customer's shopping basket. It is the single information that is shared between the merchant and the transport agent and serves as a link (for the transport agent) between the goods to be delivered and the user's name. So, the basic workflow can be summarized as follows: The customer orders her desired goods, thereby generating an order ID. The merchant prepares a package with the ordered goods, labels the package with the order ID and hands the package over to his transport agent. The transport agent resolves the order ID into the customer's name and address, relabels the package and afterwards handles the package just as any other "normal" package.

Another way of solving the delivery problem for pseudonymous shopping would have been to use a P.O. box at the post office. However, this would have introduced inconvenience to the customer, since first, she would have to apply for a P.O. box, and second, go to her P.O. box to pick up her package. Thus today, home delivery, as seen in DASIT, seems more natural and also more customer friendly.

But pseudonymous delivery of goods is only half of the deal, since the goods must still be paid. In general, the merchant needs some information or evidence that assures that he will receive his money. Normally, such information is the customer's name and address, which allows the merchant to sue his customer, if she refuses to pay. However, this scheme would contradict our efforts within DASIT to protect the customer's privacy, since we seek to disclose as few as possible personal data. Fortunately, there are Internet payment systems available that hide the payer's identity from the payee, while giving the merchant "hard" evidence that he will be paid. One of these systems is the 3KP-SET payment

protocol which we used in DASIT. By using 3KP-SET, the merchant immediately receives a digitally signed guarantee from his customer's bank that he will receive his money. This guarantee is given only after the customer has authorized her bank to do so, which is part of the 3KP-SET protocol. Since payment is ensured by the customer's bank, the merchant does not need to know the customer's identity as a payment guarantee.

Beside pseudonymous shopping, DASIT also offers "normal" shopping, i.e., shopping under one's real name. In this case the shop distinguishes between two kinds of personal data. First, data that is necessary to carry out the service, and second, data that is not necessarily needed by the shop, however requested for other purposes, such as marketing. For the latter, German data protection law requires the customer's explicit consent in order to allow processing of her personal data for the stated purpose(s). This consent must be given deliberately, and in particular, failure to give a consent must not permit access to the service. Furthermore, a consent must be verifiable afterwards, i.e., non-repudiable. This is achieved through an electronic signature, for approving the collected data, the stated purpose, named recipients, and other privacy related information.

Customers were provided with electronic key-pairs for authentication and for electronic signatures. However, since a signed consent is only necessary for the processing of personal data, pseudonymous identities were not provided with signature keys, since they do not produce personal data per se. The necessary public key infrastructure was established by a DASIT certification authority (CA) which additionally provided the customers with pseudonymous email accounts, used, for instance, for acknowledgements of orders conducted under pseudonyms. Since the DASIT CA is the only party that can link the users' pseudonyms with their real identity, it also serves as a mediator in case of conflicts that might arise when users were shopping pseudonymously, e.g., package was not delivered, or its contents were broken.

Among other scenarios, the scenarios described above have been tried out in a field trial, started in May this year, where users could test drive the DASIT system. Evaluation of this field trial is on the way, and final results can be expected within the 4th quarter of 2001.

[info]

- DZ BANK:
<http://www.dg.dzbank.de/oir/oirsite.nsf/index/2A2BA07E2F819B15C1256AA0005DA10F?OpenDocument>
(in German; including reference to some consumer survey results)
- SIT: <http://sit.gmd.de/MINT/projects>
- Provet group: http://www.uni-kassel.de/fb10/oeff_recht/projekte/projekteDasitEn.ghk

[9&5]

Creating Consumer Confidence: Current Efforts towards International Quality Criteria for E-Commerce

Dirk Klasen (klasens@vzbv.de), Berlin, Germany

/consumer protection/electronic commerce/crossborder/standards

How is it possible to raise consumer confidence? That's the key question in all current discussions on B2C e-commerce. Several codes of conduct and trustmark systems have been developed to provide consumer-friendly conditions on the internet. There is not yet any global agreement on a minimum standard, although there are various initiatives to reach one. The article describes the more important developments at the international level.

Looking back over the last three years, one can say that not only B2B E-Commerce is a growing market but also commercial transactions involving private consumers on the Internet. It is a fact that, for instance, in the United States, Australia and the UK consumers are apparently taking advantage of electronic shopping more often than in other developed economies. The conclusion that there are reasons of mentality for those differences seems to be wrong. One simple answer is that for e-consumers in the "more advanced" English speaking countries the language problem doesn't play the same role as in other countries where most consumers prefer websites in their own language and, therefore, can access a small part of the mainly English speaking internet shopping world.

Another mistake in many debates is the assumption that there are fewer problems for consumers shopping electronically in the US or the UK. In some areas this observation is true but it has obvious

reasons. For instance, the often mentioned hesitance of German consumers to use their credit card for online transactions is a result of a lacking practical procedure making it easy to claim the misuse of the credit card by third parties or the e-trader and to get the money back in an easy and fast way without additional charges. Consumer-friendly chargeback systems could help and the existing systems in the US or the UK make it easier for consumers to use their credit card. But our sister organisations in countries with chargeback systems report a number of deficits, i.e. in those countries we are also far from a perfect world.

Such deficits exist not only in the area of payments. A recent of Consumers International, the global umbrella of consumer organisations, shows that very basic and serious problems still exist in e-commerce. Some key facts from this study that covered more than 300 items bought domestically as well as cross-border in ten countries: 28 % of traders gave no geographical address, 13 % left the customer without any information about the total price, 34 % didn't mention a delivery time, 8 % of items never arrived (!), 12 % had no returns procedure, 50 % of traders failed to give information on rights of withdrawal, 28 % failed to mention privacy policies, 20 % didn't describe their payment security practices.

The e-business world wishing to trade fairly and consumer organisations have a common interest in the existence of globally effective internet minimum standards to raise consumer confidence and avoid conflicts or solve those conflicts in a mutually satisfying manner. Meanwhile, national as well as EU legislation has come into force that could be a reliable framework for e-traders and consumers as long as only countries having such legislation are concerned. In this respect, the main problem seems to be the rapid implementation of existing legislation in the daily practice of e-traders. But the legal measures taken at the national and the EU level have their limits where transactions beyond the EU borders are concerned. Due to different legal systems and especially the different role of self-regulation and co-regulation as well as different views on the level of consumer protection, international agreements on minimum standards for B2C e-commerce accepted by customers and companies are hard to achieve.

The most geographically far reaching attempt was made by the OECD countries when the ministers of its member countries agreed to recommend *Guidelines for Consumer Protection in the Context of Electronic Commerce*. Although these guidelines don't meet all the necessary requirements of the consumer side, some provisions, e.g., on information about the business or information about the transaction, are suitable for use as an orientation for dotcoms dealing with orders from private consumers. Other international efforts for general B2C standards in e-commerce being discussed under the roof of the ISO, the International Organisation for Standardisation. Within the rules of international standardisation procedures, ISO intends to develop standards, e.g., on the type of information about the merchant, the products/services and the transaction, the timing of information disclosures, the collection, use and disclosure of personally identifiable information or procedures of handling complaints.

At the global level, the bigger companies are also trying to develop their own solutions to foster online business. The platform is provided by the *Global Business Dialogue on e-commerce* which enjoys the attention of many government representatives. Part of these activities is the area of consumer confidence that has led to position papers on Alternative Dispute Resolution (ADR), trustmarks or data protection.

The international consumer world is debating consumer aspects of e-commerce especially in the *Transatlantic Consumer Dialogue* of EU and US consumer organisations which was started in September 1998. In the meantime, this regular dialogue has resulted in a lot of common opinions and positions on e-commerce covering areas including disclosure of information, privacy, children and internet, chargeback systems, jurisdiction, requirements related to ADR systems.

At the EU level, the member states have taken the necessary legal steps to create a basic framework for electronic transactions involving consumers. The most important elements are the distance selling directive and the so-called e-commerce directive. Additionally, the European Commission is anxious to promote discussions on systems for ADR based on recommendations which are to provide the criteria for reliable and acceptable ADR systems. Another political priority in e-commerce is the introduction of an accreditation procedure for online trustmark systems.

Consumer organisations regard trustmarks as a suitable instrument to give assistance to consumers in a jungle of e-merchants who are often unknown and located in areas of the world on which the consumer has no information concerning legislation or usual trading practices. However, trustmarks

themselves are not any guarantee that the business decorated by a trustmark will trade fairly and in a transparent and consumer-friendly manner. The more trustmarks exist the more it is necessary to find basic rules which trustmarks have to follow to be of genuine guidance for consumers. A separate problem is, of course, that recommended trustmarks need to become well known to the public so that users can rely on them. In Germany, there are currently about 8 to 10 trustmarks on the market. Therefore, the leading German consumer organisation AgV (now VZBV) has agreed to discuss quality criteria for online B2C transactions with the German industry initiative D 21 and these criteria have become the basis for a D21 recommendation for trustmarks to meet the minimum standards. This has been made public on the D21 website and a special Monitoring Board was created to observe the activities of the national trustmark providers and to provide a forum for the discussion of views on specific problems.

The European Commission has proposed a similar but more binding approach. Last year, the Commissioner for Health and Consumer Protection, David Byrne, started a so-called e-confidence initiative and set up an e-confidence group consisting of many representatives of business and one of the consumers. These discussions have failed due to the inability of the business side to reach a common position on several points, such as a third party assessment and monitoring of trustmarks.

As a consequence and in order to keep the small chance of a practical and acceptable solution, the EU industry association UNICE and the EU consumer federation BEUC launched a new round of negotiations specifically on basic quality requirements for trustmarks and their assessment by third parties in May 2001. These negotiations will probably be finished in September and could be a step forward to more transparency in the market.

In connection to e-commerce quality requirements some national activities are worth mentioning. The Dutch *Electronic Commerce Platform* tries to include all stakeholders to promote the use of the internet in economic life. One outcome of these efforts was the development of a *Model Code of Conduct for Electronic Commerce*. In Australia a group of experts chaired by the government has developed a *Best Practice Model for Business* that is also supported by the Australian Consumers' Association. Although it is a kind of non-binding self-regulation the Australian government has announced that it will closely observe the implementation of that model. Well known in North America is the Better Business Bureau and its *BBBonline Code of Online Business Practices*. BBBonline is also running a *Reliable Seal Program* and a seal covering the issue of privacy.

Another quality seal offered by *TRUSTe* has its focus on the privacy policies of e-companies. The *Better Internet Bureau* located in Canada deals not only with the certification of procedures for B2C transactions but also with the content of websites, for instance in relation to sexual, racial or religious aspects. Using a logo called *Webtrust*, the certified public accountants associations are operating a trustmark in several industrialised countries. Their criteria include not only questions of transparency and terms and conditions but also the privacy policy of an applicant.

Last but not least *Webtrader* has to be mentioned, a project launched by the UK Consumers' Association and joined up to now by consumer organisations of seven other EU member states. This logo combines the independent image of consumer bodies and their experiences in dealing with consumer complaints with a certification of companies who wish to increase consumer confidence in their websites.

Other interesting codes of conduct and ideas for quality criteria are regularly published and updated by the European Commission on a specific website.

The key question of all these initiatives will be if there will be a common global minimum standard for B2C e-commerce in the world wide web in the foreseeable future and how fast the consumers will become familiar with reliable trustmarks based on that global standard.

[info]

- Bundesverband der Verbraucher-Zentralen und Verbraucherverbände (Federation of German Consumer Organisations) www.vzbv.de
- <http://www.consumersinternational.org>
- <http://www.oecd.org/dsti/sti/it/consumer>
- <http://www.iso.ch>
- <http://www.gbd.org/nn/index.html>
- <http://www.tacd.org/>
- http://europa.eu.int/comm/consumers/policy/developments/dist_sell/index_en.html
- http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html

- http://econfidence.jrc.it/default/show gx?_app.page=show.html&Object.object_id=EC_FORUM000000000000001A3
- <http://www.initiated21.de>
- <http://www.unice.org>
- <http://www.beuc.org>
- <http://www.ECP.nl>
- <http://www.ecommerce.treasury.gov.au/html/ecommerce.htm>
- <http://www.choice.com.au>
- <http://www.bbbonline.com>
- <http://www.truste.com>
- <http://www.better-internet-bureau.org>
- <http://www.webtrust.org>
- <http://whichwebtrader.which.net/webtrader>
- http://econfidence.jrc.it/default/explore.gx?Object.object_id=EC_FORUM000000000000008E0

[9&6]

Security & Trust: Taking Care of the Human Factor

Florian N. Egger, (F.N.Egger@tue.nl), Eindhoven University of Technology & ecommUSE, Eindhoven; Dennis Abrazhevich (D.Abrazhevich@tue.nl), Eindhoven University of Technology, Eindhoven, The Netherlands

/consumer perceptions/security

In the e-business chain, the last link that needs to be convinced of the security of an online transaction is the end-user. That is why this article puts forward a user-centred perspective of the problem of trust in online payments, derived from the discipline of Human-Computer Interaction (HCI). We will first offer a general account of e-commerce system design, showing that there is more to trust than only security. The last part gives some recommendations on what can be done to increase consumers' trust.

Trust: More than Security

When examining barriers to the adoption of e-commerce, numerous studies have singled out consumers' lack of trust as a major factor. Some people reduce the trust problem to one of security, arguing that, if security issues are resolved, people will be happy to transact online. However, when the trust problem is broken down into its constituents, privacy, ease-of-use or the credibility of information on the web are revealed to be as important to consumers as security.

As far as the introduction of a new e-payment system is concerned, one should not underestimate the power of the media and reputable institutions in approaching consumers and assuring them of the system's security. Since the average consumer is unlikely to be able to assess the objective security of, say, an encryption algorithm, this issue remains, to a large extent, one of trust – namely trust in familiar information sources. Thus, a well-orchestrated marketing effort would help give consumers enough pre-interactional trust to understand, accept and use the new system.

Meeting Consumers' Trust Concerns

What has been observed in user tests of e-commerce web sites is that the assessment of security typically happens very late in the trustworthiness evaluation process – namely, just before placing the order. Of course, most of the interaction with a commercial web site aims at establishing whether a particular merchant offers products or services that meet the customer's needs. While looking for information, a number of cues are picked up by the user – in both explicit and implicit ways. These cues, be they graphical or textual, give an indication of the merchant's professionalism and competence. It is only when a transaction is envisaged that medium-trust customers will explore the terms and conditions, as well as privacy and security policies.

This risk assessment phase goes much further than merely assessing the security of online payments – it covers the handling of confidential data by the company, warranties and after-sales service, as well as the customer's liability in case of fraud.

In terms of user interface design, one should therefore not assume that having a padlock appear at the bottom of the browser is enough to make customers feel safe to transact. Having detailed step-by-

step payment procedures with links to additional security information is likely to work better than having a system that offers inadequate feedback and, thus, limited control. Presenting key information in an understandable way where and when consumers need it most is an information architecture challenge fit for HCI design.

Top-Down & Bottom-Up Design

To maximise the adoption of a new e-payment system, it is crucial that the human factor be actively and systematically taken into account during the design of that system. A top-down approach is one that centres primordially on business strategy and commercial arguments. Most importantly, it also implies a heavy stress on the development of new security solutions in terms of hard- and software. Thus, a top-down approach may very well produce a system that works efficiently but it does not guarantee that the system will be trusted and used.

A bottom-up approach centres around the system's end-users – not only on their functional requirements, as it is the case in traditional ergonomics or HCI, but also on their preferences, concerns and expectations. It is noteworthy that such a user-centred approach does not only inform the design of the user interface. Indeed, it also gives valuable insight into how and via which communication channels the system should be presented when it is launched.

The bottom-up design approach can be very effective to test the acceptance of new payment technologies by consumers. For example, the ING Direct bank of Canada has conducted extensive testing of people's reactions to using a biometric device for authentication in their electronic banking system. The system included a thumbprint scanner embedded in a computer mouse and developers were unsure whether people would accept this technology in exchange for a higher level of security. The user tests indicated that their customers were actually quite receptive to this technology and not as concerned about issues of privacy when using the biometric devices as had been expected.

Designing the Trust Experience

Trust in payment systems is influenced by factors such as anonymity, security, reliability, the amount of control that users have, as well as the reputation of the entity that introduces the system. Below, we introduce a number of guidelines that address the different facets of security required for e-payment systems in an Internet environment. Issues of trust and security are connected to exchange, storage and management of the payment- and user-specific information. To engineer a certain level of trust in terms of perceived security, one should:

- Take into account the context of use and domain of application of the system being designed. Context of use can be viewed as an important requirement for the design. Different applications require diverse levels of security. Buying flowers can be done with a credit card with basic cryptographic protection, while electronic banking needs more sophisticated authentication and security mechanisms.
- Provide a clear and prominent policy on security:
 - Provide clear visibility of the security techniques employed. These should clearly be explained to the end-user. This can be done by providing textual information describing which security solutions have been implemented, as well as by displaying the logos of reputed institutions or solution providers.
 - Explain security measures in management and storage of the data.
 - Establish customer support line on security related issues.
 - Supply regular information updates on changes and upgrades in security.
- Take into consideration security issues specific to the type of payment system.
- Address security issues specific to a single payment and to the system's operations in general:
 - E.g. provide the ability to deactivate passwords or block accounts offline.
 - Giving user access to their data, allowing them to change it, and timely delete outdated information can assist in building trust relations with customers.
- Be aware of trade-offs between security and ease of use:
 - Too heavy solutions may hamper ease of use and have a negative influence on trust. In addition, the use of extra hardware and software components may be seen as an additional barrier

to adoption, given the lack of convenience and the costs involved. This would complicate the process of acquiring new customers and vendors and, thus, reduce the customer base. This may be one of the reasons why SET has not been popular so far. Hopefully, solutions where intrusion in customers' paying experience is minimised will gain more popularity, especially if they help to solve some of the vendors' problems, such as chargebacks. Possible candidates for such acceptance are 'Verified by Visa' or Mastercard's SPA.

- Try to minimise the security costs (both financial and temporal) imposed on users.
- Create a security management culture. This can be done by educating employees and implementing strict information handling policies within the company.
- Have a trust recovery plan in the event of a security breach likely to undermine trusted relationships with customers. In many cases such a plan will consist of enacting the company's trust policies, providing financial compensation, as well as reassuring customers through the media.

[info]

- Papers on trust in e-commerce: www.ecommuse.com
- Online Trust discussion group: groups.yahoo.com/group/online-trust
- ZDnet News: Biometrics gets thumbs up from Microsoft. news.zdnet.co.uk/story/0,,s2079521,00.html
- User-Related Factors in Electronic Payment Systems www.ipo.tue.nl/homepages/dabrazhe/ps/
- Verified by Visa: www.visabrc.com/doc.phtml?2,190,942,942_vbv_overview.html
- Mastercard's SPA: www.mastercardintl.com/about/press/pressreleases.cgi?id=423
- Abrazhevich, D. (2001a) Classification And Characteristics Of Electronic Payment Systems in Electronic Commerce and Web Technologies 2001, Proceedings, LNCS 2115, K. Bauknecht, S.K. Madria, G. Pernul (eds.), Springer
- Abrazhevich, D. (2001b) A Survey of User Attitudes towards Electronic Payment Systems. Proceedings of Joint AFIHM-BCS Conference on Human-Computer Interaction IHM-HCI'2001, Volume 2. Vanderdonck, J., Blandford, A. & Derycke, A. (eds.), Toulouse: Cepadues-Editions.

[9&7]

Mobile Payments in the Baltic States

Ülle Adamson (Ulle@biceps.org), Kaido Kaarli (kaido.kaarli@intergate.ee), Stockholm School of Economics in Riga, Latvia

/mobile telephony/electronic payment systems/mobile phone payment systems/
Estonia/Latvia

The Baltic States, three small countries with total population of 7.6 million located between Scandinavia, Russia, and Poland, can be considered an active area in the development of mobile payments, with Estonia taking the most initiative. The most successful application of mobile payments has been the mobile parking service in Estonia, which has been available since July 2000. Remarkable progress has also been made in the area of mobile banking. This article provides an overview of all the ongoing activities in the area of mobile payments in this fast developing region.

Real world payments via mobile phone: mobile parking

Estonian Mobile Telephone (EMT, majority owned by Telia and Sonera) was the first company to start providing mobile payments in the Baltic States. The company developed a mobile payment system for parking that started operating on July 1, 2000. For a year, the company offered only a system that simply added the service costs to one's phone bill. The system operates as follows: by calling a certain number, the client opens a virtual parking account and credits it with a certain amount. In order to start parking, the person has to send a SMS to a specified number with the car number and the code of the parking zone. In case parking lasts longer than expected, the client can conveniently add money to his or her account by calling a specified number. A call to another predetermined number finishes the parking or it ends automatically after a specified time, or 4 hours, if not extended. Also, the car has to be marked with a special sticker. The service is open to all private persons with contracts or pre-paid mobile phone cards. It has been quite popular and on average 15% of all parking payments in Tallinn were made using this system during the last twelve months. Since

July 2, 2001 **Radiolinja Estonia**, another mobile operator (owned by Radiolinja and Elisa Communications, Finland), has licensed this software from EMT to offer the service to its own clients. The EMT parking service was chosen in 2001 by the GSM association as a nominee in the category of 'Most innovative wireless service for customers'.

Nevertheless, the company has experienced a few problems with the solution. The main problems are the following: first, people using company phones cannot use mobile payment services, unless their employer approves this option; second, the percentage of mistakes made while sending SMS messages is relatively high (for example, a typical mistake is that a customer types letter O instead of number zero when sending his or her car number, and as a result he will be charged a fine for not paying for the parking). In this case, there is no credit risk involved for the mobile operator, because according to the contract EMT has to pay to the town authority at the end of the following month. Furthermore, EMT is not responsible for covering unpaid bills. However, it would be difficult to enforce such terms for private merchants. In sum, the system involves several shortcomings, while being quite simple to develop.

On June 8, 2001, EMT opened also an alternative system, which is currently offered for mobile parking, but could be easily implemented also for other services. In the new version, the charge is made to a special mobile account, kept by the operator. In order to start using a mobile account, a user has to accept the agreement in her internet bank (an internet banking service provided by the local universal banks). Then it is possible to load the mobile account with a pre-determined amount by sending a SMS to special number. Thereafter, one can pay for services using the money on the m-account. Currently, EMT is working together with both of the leading Estonian universal banks, which together have about 90% market share. EMT has retained control over the organisation of payments, while only co-operating with the banks to create a convenient transfer of funds from bank accounts to m-accounts. The shortcoming of this system is that it is difficult to provide the service to the clients of other operators, as they are not provided with EMT's m-account (see also Figure 1).

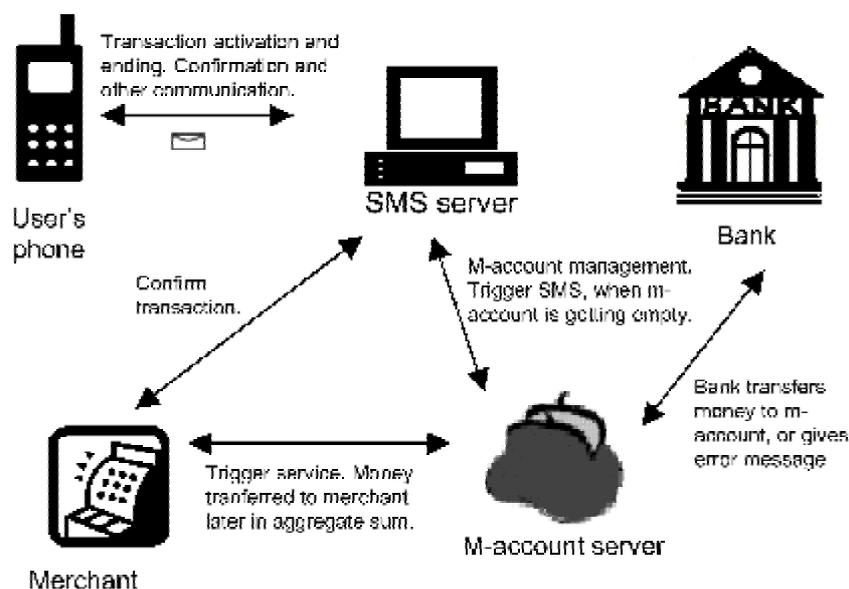


Figure 1: The payment system developed by EMT

Before using, the service must be registered at the user's internet bank (an internet banking service provided by the local universal banks). The user has to specify the phone number payments will be using and the default transfer sum. Additionally, the user has to accept responsibility for use of his phone by other people.

Q-GSM (majority owned by Tele 2 AB, Sweden) started providing its self-developed mobile parking service on June 25, 2001. The systems functions in the same way as EMT's first solution, where the parking charge is added to the phone bill, yet prepayment is needed if the services are used for over EUR 32 per month. Currently the service works only in Tallinn (Estonia), but it will be extended

shortly to other major towns in Estonia. As stated by Timo Mitt, Q-GSM's Development Manager, the company further plans to develop a new system in co-operation with banks keeping for itself only the core of mobile communication solutions part of the business. All the payments made with mobile phone automatically transfer money from the user's bank account to the merchant. In this way the mobile operator is not involved in moving money, but provides only the transaction medium. At the same time, the solution would be unreasonable for small payments since it requires a bank transaction each time a payment over the mobile phone is made, which costs approximately EEK 1 (EUR 0.06) for the bank. Consequently, the payment would become too expensive for small sums, e.g. less than EEK 10, keeping in mind that the operator also wishes to receive some commission, the SMS fee for example. The system is still at the development stage and it is unclear whether it will be launched in future.

Pre-paid card top-up service

Latvian Mobile Telephone (LMT) in co-operation with Hansabanka (belongs to Hansabank Group, owned by Swedbank, Sweden) is providing a service, which offers a possibility to add money onto a prepaid mobile account straight from one's mobile phone. The solution is based on the Hansabanka mobile banking system, which is described below. In order to start using the service, a user has to predefine the payment in the Hansabanka internet bank Hanza.net.

Mobile banking

Being successful in internet banking (around one fifth of the population in Estonia uses internet banking services), both leading universal banks in Estonia have also developed a WAP bank solution. **Hansabank's** WAP bank allows viewing information about bank accounts and making pre-defined payments. Payment has to be specified in the internet bank Hanza.net, but the amount and description of the payment can be changed. A user is identified through her SIM card, username and a fixed password (instead of a changing password from the code card with 24 6-digit codes). Currently, the service is offered only for the leading mobile operator EMT's clients. (There are a total of three mobile operators active in Estonia). In addition to the mentioned services, **Ühispank's** (the Union Bank of Estonia) WAP bank also provides a possibility to make any domestic payments. In this solution, the user is identified by a random code from the code-card in addition to a fixed password.

Hansabanka in Latvia has also recently launched its mobile bank, which offers a possibility to make predefined payments, which cannot exceed USD 1500 and have to be specified in the internet bank. To make a predefined payment, the user has to send a message "PAY#name_of_payment#amount#description" to a special number. In case the payment can be made, the bank sends back confirmation message asking for a code from the internet bank code card with 24 6-digit codes. Confirmation message is "PAY#name_of_payment#code".

Electronic bill presentment and payment

On May 2, 2001 in Latvia, **Nacionlais Maksajumu Centrs** (the National Payments Centre, owned by Swedgiro Group, Sweden) together with mobile operator Tele 2 launched a service, which allows the regular payment of monthly bills over mobile phone. This service uses banks' direct debit function. A user gets an SMS about the arrived bill, and by simply sending a reply SMS, the bill is paid. To register for the service, a customer has to sign a contract with her bank or phone operator. Currently the service works at three banks: Unibanka, Baltijas Tranzitu Banka and Saules Banka, that cover about a quarter of retail banking in Latvia. NMC is a company providing bill management services to companies with a big customer base by organising the bills to customers and having relationships with all the local banks. If successful, the solution will also be applied in other countries, for example in the Estonian sister-company *Maksekeskus*.

Overall, one can see very active developments in the field of mobile payments of all kinds. There is little information publicly available about the usage of all those services partly due to being on the market for a very short time. Practice has shown that a special service such as parking can become very popular. The Baltic countries seem to be a place to be closely monitored as a testbed for new services.

[info]

- The site of Estonian Mobile Telephone <http://www.emt.ee>, specifically:
<http://www2000.emt.ee/eng/txt/uudised.phtml?nt=34>
<http://www2000.emt.ee/eng/txt/uudised.phtml?nt=33>
- The site of Hansabank in Estonia http://www.hanza.net/abi/en/hzn_wap_abi_eng.html,
http://www.hanza.net/abi/en/m-konto_abi.html
- The site of Hansabanka in Latvia http://www.hansabanka.lv/cgi-bin/www/engl/pakalp/pr_5_4.php and
http://www.hansabanka.lv/cgi-bin/www/engl/pakalp/pr_5_4.php.
- The site of Ühispank in Estonia <http://www.eyp.ee/pages.php3/1301031302>
- The site of GSMWorld <http://www.gsmworld.com/events/awards/nominees.html>
- *Application of Mobile Payments in Estonia*, Bachelor Thesis, the Stockholm School of Economics in Riga, Latvia, January 2001. Contact the authors of this article.

[9&8]

The Payment Blues of German Internet Merchants

Leo Van Hove (Leo.Van.Hove@vub.ac.be), *Free University of Brussels, Belgium*

/review/Internet payment systems/survey/merchants/Germany

A report by Internet research firm Berlecon Research paints the current state of the German online payment environment and looks at the problems and needs of local Internet merchants. The report shows, among other things, that electronic commerce in Germany today bears striking resemblances with traditional mail order, both in terms of the problems faced by merchants and the means of payment preferred by customers. New payment systems designed for the Internet are still hardly used. However, Berlecon Research's evaluation of the outlook for mobile payment service paybox is fairly positive. It also hopes that the introduction of 3D-SET together with the liability shift towards the issuing bank will alleviate some of the problems faced by merchants, notably chargebacks.

This Spring, Berlecon Research (see [info]-section) published a 100 pp. report entitled "Kassieren im Ecommerce – eine Analyse relevanter Zahlungssysteme aus Händlersicht" (Receipt of payment in ecommerce – an analysis of relevant payment systems from the vendor perspective). As the subtitle of the study indicates, the goal was to analyse the online payment systems that are available today in Germany, and this primarily from the point of view of Internet merchants. The authors, Petra Bock and Dorit Spiller, emphasise – and correctly so – that so far consumer fears have received the bulk of attention in surveys and that facts and data about the experience of merchants are all too rare.

The Berlecon Research study aims to fill that gap. To that end, a survey was conducted among 680 online merchants, of which 78 (11.5%) returned the questionnaire. However, because the larger online shops were clearly underrepresented, the researchers decided to only take into account the answers of the 69 smaller shops (defined as shops with no more than 6 employees), and to surf the Internet themselves in order to obtain an overview of the payment systems offered by the 31 largest online shops.

Before turning to the analysis, let me first summarise some of the more interesting facts and figures. An important finding is that the German online payment market is dominated by traditional 'offline' payment systems. New payment systems such as digital tokens or *paybox* (a mobile phone based payment system [see ePSO-N 1&6]) hardly play a role. Even credit cards are not very popular compared to other countries (but then the degree of penetration among consumers is also lower in Germany). In the smaller online shops, the most popular means of payment is good old cash on delivery (COD) – with no less than 40% of the total number of payments. Payment by means of a credit transfer after receipt of the goods ('Rechnung') is also popular (28%). Direct debit ('Lastschrift') is good for 13%; credit cards only come in fourth place. When larger shops are included, the picture is somewhat different: Rechnung now comes in first place (41%), but COD is still the second most popular option (20%). The prevalence of Rechnung results from the fact that online orders placed with traditional mail order companies – 90% of which are post-paid via credit transfer – account for one-third of German e-commerce.

The report also shows that there is not always a good agreement between the payment systems offered by merchants and those preferred by consumers. For example, whereas 75% of the smaller shops offer prepayment ('Vorkasse') via either credit transfer or cheque, this option only accounts for

7% of the total number of payments. Also, whereas 84% of the larger online shops accept credit cards, it is significantly less popular among consumers. Finally, the report plays down popular fears about the lack of security of Internet payment systems: only 2% of the merchants in the survey have experienced abuse of stolen credit card numbers. Far more important for merchants is the sometimes low 'payment morality' of their customers: goods are not collected, bills are not paid, fake orders are placed to harass people, etc. In short: the typical problems experienced by mail order companies.

After presenting the facts, the report first gives a comprehensive overview of the advantages, costs and risks associated with the most important payment systems. As it is impossible to go into detail here, let me just stress that the authors do an excellent job in showing, for each of the payment systems, how the risks are divided between merchant and customer. This makes it easy to understand why prepayment is not very popular with consumers, and why smaller online shops have a clear preference for systems where payment is guaranteed. The authors point out, for example, that 95% of the smaller shops offer COD, compared to only 55% of the larger shops. They argue that this is because non-payments can be far more damaging for smaller shops, which often do not have the financial strength to hire collecting agencies or to go to court in an attempt to recover the goods. The authors also show that many of the so-called new payment systems such as *paybox* are in fact not that new in that they rely on existing systems such as direct debit, and thus basically present the same risks. However, some providers assume part of the risk (*paybox*, for example, takes over withdrawn debits) and/or offer additional services (such as bill collection) or additional security measures (such as solvability checks).

In a following chapter, the authors tackle the same problem from a different angle. They list what they call "die sechs Essentials des elektronischen Bezahlers" (the six crucial requirements for an online payment system; namely secure data transfer, authentication, non-repudiation, ease of use, diffusion, and guaranteed payment), show how these are interlinked, and then try to assess how each of the payment systems scores on these points. They also provide a thorough overview of service providers to which the payment process can be outsourced (in whole or part). Again it is impossible to summarise everything, but three points struck me. First, the fairly positive stance towards *paybox*. The authors point out that for a recently introduced system the acceptance among merchants is already quite high: 19% of the larger online shops support the *paybox*-system. Among smaller shops the acceptance is today even lower than that of digital coins (1% and 3% respectively), *but* an additional 31% plan to install *paybox* in the near future – which places it at the top of their list. Second, where the Geldkarte electronic purse and other smart card-based solutions are concerned, Berlecon Research is sceptical and sees the need for smart card readers as a severe bottleneck. Third, the authors are convinced that 3D-SET (which does not require the cardholder to download software) stands a good chance at gaining increased acceptance since it will free merchants from the chargeback problem thanks to the initiative by Visa to shift the liability to the issuing bank. Under the new rules, if they have delivered correctly, merchants will no longer have to bear the costs of chargebacks, irrespective of whether the cardholder has a SET certificate. However, according to Berlecon Research a dark cloud above the future of 3D-SET is the danger that issuing banks might want to shift the costs to cardholders.

The final chapter of the report provides a checklist for merchants who have to select an online payment system for their shop (what type of goods do you offer?; what is your target population and which means of payment do they use?; how well do you know your customers?; etc.). The authors also point out that the widely diverging pricing models of the different systems make it very difficult for merchants to compare the costs involved. The report therefore concludes by presenting several cost simulations (for micro-, mini, meso-, and macro-payments).

Overall, this is clearly a very useful report for its target groups (merchants, providers, consultants), but also for interested observers. As a conclusion, let me quote a sentence towards the end of the executive summary that summarises very well one of the main messages: "Willkommen in der (Problem-)Welt des Versandhandels" – "Welcome to the (problematic) world of mail order". It will be interesting to watch whether 3D-SET and new payment systems such as *paybox* will indeed succeed in turning it into a different (and less problematic) world.

[info]

- **Bock, P. and D. Spiller**, "Kassieren im Ecommerce - eine Analyse relevanter Zahlungssysteme aus Händlersicht", Berlecon Research, February 2001 (available in German only). A press release and some graphs can be found at http://www.berlecon.de/pressroom/presseinfos/27_06_01.html.

- Berlecon Research is a Berlin-based market research firm focussing on the Internet. It was founded by Thorsten Wichmann, who also organises the Berlin Internet Economics Workshop. Their homepage can be found at <http://www.berlecon.de>.

ePSO Newsletter – Issue 10, November 2001

Focus: Security (III)

[10&1]

Editorial: Authentication, Privacy and Regulation

Simon Lelieveldt (simonl@wxs.nl), Amsterdam, The Netherlands, and Arnd Weber (arnd.weber@itas.fzk.de), ITAS, Karlsruhe, Germany

/security/privacy/regulation

This issue focuses on authentication and privacy. The development of credit card charge backs is addressed, these being a major driving force for proposals such as 3D-Secure (Verified by Visa), SPA/UCAF, and pseudo card numbers. The pros and cons of these technical solutions are reviewed. Furthermore, this issue addresses the achievability of unobservable purchases and payments on networks. In addition there are comments on the demise of Flooz and Beenz, there is a review of the new “Blue Book” of the European Central Bank, and the ePSO Conference taking place in Brussels on February 19, 2002 is announced.

We start this issue with an article by Oliver Steeley on the latest efforts of the credit card companies to improve authentication of payments on the Internet. Oliver compares the initiatives by VISA and Mastercard. It is interesting to read in Oliver Steeley’s article how the large card schemes are trying to resolve the problem of safe payments in different ways. With Oliver Steeley we wonder why – as with SET – the card schemes did not launch a joint effort from the very beginning. Perhaps fear of more anti-competition enquiries has driven them to an initial development of separate protocols, possibly with a future harmonised framework up their sleeves. This would allow the schemes to act responsively to the market calls for harmonisation instead of being accused upfront of being monopolistic.

The topic is continued with an interview with Tilo Schürer of Bankgesellschaft Berlin. He points out that charge backs on the Internet, a significant problem in 1999, have actually diminished. Tilo Schürer talks about the reasons for the decrease, and spells out why for his bank, 3D-Secure would be the preferred approach compared to SPA/UCAF.

On this topic it is also worthwhile to monitor the behaviour of Microsoft. This summer Microsoft has signed licensing agreements with both Orbiscom and Coyota to be able to use the pseudo card number technology for protection of payments made as a part of the Passport-service to consumers. Perhaps this move will be decisive in establishing pseudo card numbers as the de facto payment protection standard. It will however also raise new questions, both with respect to competition (will the Liberty Alliance then back the other methods?) and with respect to privacy/security (is Microsoft Passport secure enough and does it respect privacy?).

In the articles by Victor Dostov and Hannes Federrath we show the technical level of privacy protection that is possible today. Typical approaches today are that a company promises not to sell data, or a government regulates that using data for other purposes than those mentioned during collection is illegal. Of course, this means that quite a lot of data are collected nevertheless. Also remember that on networks, both hardware and software produce plenty of traces, such as IP numbers, the network cards Media Access Control addresses, Microsoft product IDs, etc. These can be used to trace users [Reavis 1999]. As opposed to trusting promises and regulations made by companies or governments that data will not be abused, the two articles show that it is possible to avoid traces of purchases in the first place. Read Victor Dostov’s article about pseudonymously opened accounts and untraceable electronic money from his Russian company Paycash. You may wonder what good untraceable money is if providers or governments store IP addresses. Also the merchant needs a delivery address, either in the physical world or an IP address. So providing an untraceable payment is not enough if the delivery can be traced by using addresses. Exactly this problem is addressed in Hannes Federrath’s article about so-called Mixes. The articles have a message to regulators, in particular those who want to encourage the use of technologies avoiding data traces in the first place: this is how it can work. From the articles it also becomes apparent that untraceability cannot be achieved without some costs. Also, an electronic money technology reduces a buyer’s power to undo a

payment, a feature addressed in the interview with Tilo Schürer. Unless anonymous accounts were used for postpayments in the first place – see Victor Dostov’s article regarding account opening.

The electronic Payment Systems Observatory not only analyses new developments, but also failures of promising candidates. In this issue Hugo Godschalk reports on the demise of two such systems, the Beenz and Flooz digital currencies.

The editors of this newsletter would also like to draw your attention to the forthcoming ePSO Conference on February 19, 2002 in Brussels. Find more about it in the contribution by Ioannis Maghiros. As usual we close this issue with a review by Leo van Hove. He has gone through the European Central Bank’s 750 page report on the “Payment and Securities Settlement Systems in the European Union”. Leo van Hove’s article conveys his impression of the qualities of the new “Blue Book”.

[info]

- Microsoft Gives Boost to Surrogate Card Numbers: <http://www.banktechnews.com/btn/articles/btnoct01-1.shtml>
- Reavis, Jim: How you get tracked on the 'Net. Network World Fusion 1999
<http://www.nwfusion.com/newsletters/sec/1101sec2.html>
<http://www.nwfusion.com/newsletters/sec/1108sec1.html>
- Marc Slemko: Microsoft Passport to Trouble. 2001/11/05. <http://alive.znep.com/~marcs/passport/>

[10&2]

Guaranteed Transactions, the Quest for the ‘Holy Grail’

Oliver Steeley (oliver.steeley@consult.hyperion.co.uk), Consult Hyperion, Guildford, United Kingdom

/credit cards/Internet payment systems/security

In a change to their previous strategy of collaboration, Visa and Mastercard have recently announced their own separate initiatives with regards to securing Internet transactions. 3D-Secure and SPA/UCAF are variations on a theme of passing the cardholder back to their card-issuer to authenticate themselves before the merchant seeks an authorisation. This is one more step in a long and arduous journey, which shows no signs of coming to a speedy conclusion.

The legend of the search for the Holy Grail became the principal quest of the knights of King Arthur and has endured for hundreds of years in western literature and arts. It may now only be 5 years since the card schemes published the specification for the SET protocol, but for many in the Internet transactions industry, it feels like centuries. The quest for mass deployment of a protocol for guaranteed transactions in a cardholder not present environment continues, as the knights of the ‘rectangular table’ in the card schemes gallantly battle on.

To celebrate the 5th anniversary of the beginning of their crusade, this article looks at two of the most recent developments in the saga from the main protagonists, VISA and Mastercard and highlights the difficulties they face.

3D-Secure

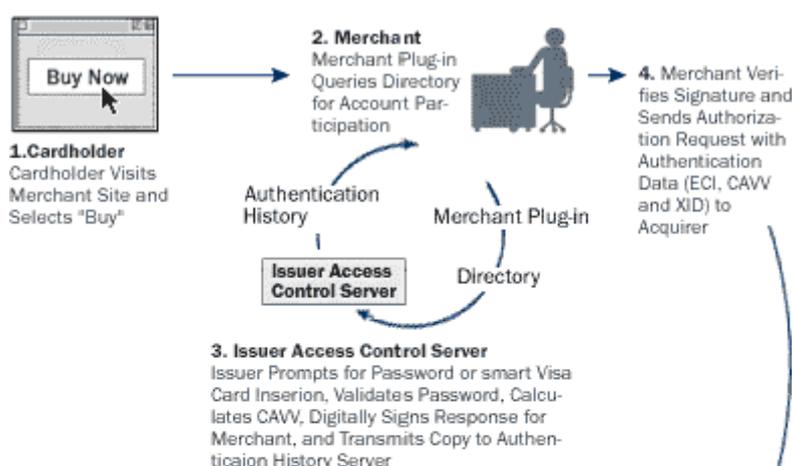
A recent press release from Visa points out that Worldpay are the first solution provider to implement 3D-Secure in Europe. Worldpay's 11,000 online retailers world-wide will be able to take advantage of the protection that Visa is offering from cardholder repudiation. Regardless of whether the cardholder is 3D-Secure capable or not, 3D-Secure merchants will no longer be liable for card not present charge backs from April 2002 in Europe and April 2003 globally.

The transaction flow for a 3D-Secure (“Verified by Visa”) transaction is summarised in the diagram below. The solution requires no software to be loaded onto the cardholder’s PC although it does require the cardholder to register a “password” or some other authentication mechanism (such as a smart card) with their issuing bank to enrol in the scheme.

At the point when the cardholder hits the “buy” button on a merchant web site, a plug-in is activated (on the merchant site), which queries the VISA directory server to determine whether the cardholder is enrolled in the scheme. If they are, then the merchant plug-in is given the web site address of the ‘Issuer Access Control Server’. The merchant plug-in then sends an authentication request to the issuer via the cardholder’s browser such that a pop-up window appears to the

cardholder. This pop-up window contains details of the purchase and prompts for the authentication information. The issuer validates the authentication information and formats an authentication response, which is digitally signed and returned to the merchant. This response will include a unique cryptographic value based upon the transaction data called the 'Cardholder Authentication Verification Value' or CAVV. A copy of the authentication response message is also sent to the Authentication History Server. When the merchant receives the authentication response, the merchant validates the digital signature of the issuer, returns the positive response to the storefront software and submits an authorisation request to the acquirer. This authorisation request includes three additional pieces of information from the Issuer's authentication response. These are the CAVV, the Electronic Commerce Indicator or ECI (which identifies this as an Internet Transaction) and a unique transaction identifier called the XID. The acquirer maps these pieces of data into the existing Visanet fields for an authorisation request message and passes it into Visanet. Visanet then verifies the CAVV with the copy stored on the Authentication History Server (although this element of the service is not yet live) and forwards the authorisation request to the issuer. The issuer receives the authorisation request with the authentication information and processes the transaction in the normal way. The whole process takes 10-15 seconds.

Online Purchase Environment



Traditional Card Payment Processing

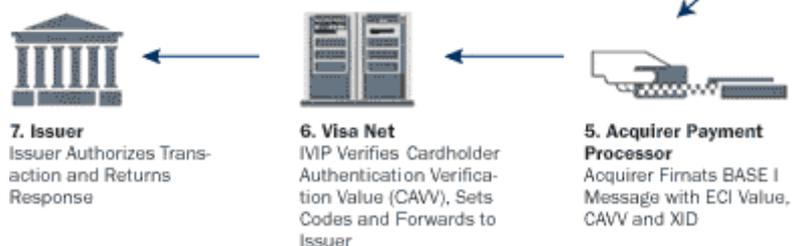


Figure 1: 3D-Secure

SPA

In May 2001 Mastercard announced its own Secure Payment Application (SPA). SPA is based around the Universal Cardholder Authentication Field (UCAF) and has been designed to minimise integration and deployment costs to the merchant. Fundamentally, UCAF is a 32-byte field with a flexible data structure that can be tailored to support a variety of security and authentication approaches including SPA, biometrics, smart cards, digital certificates and others. Mastercard has

designated Data Element 48, sub-element 43 to contain the UCAF. In a SPA transaction, the UCAF field is populated with a unique cardholder authentication value for each transaction that can be verified by the issuer as part of the authorisation transaction. Merchants and acquirers are simply responsible for collecting this value and including it with other information when they submit an authorisation request.

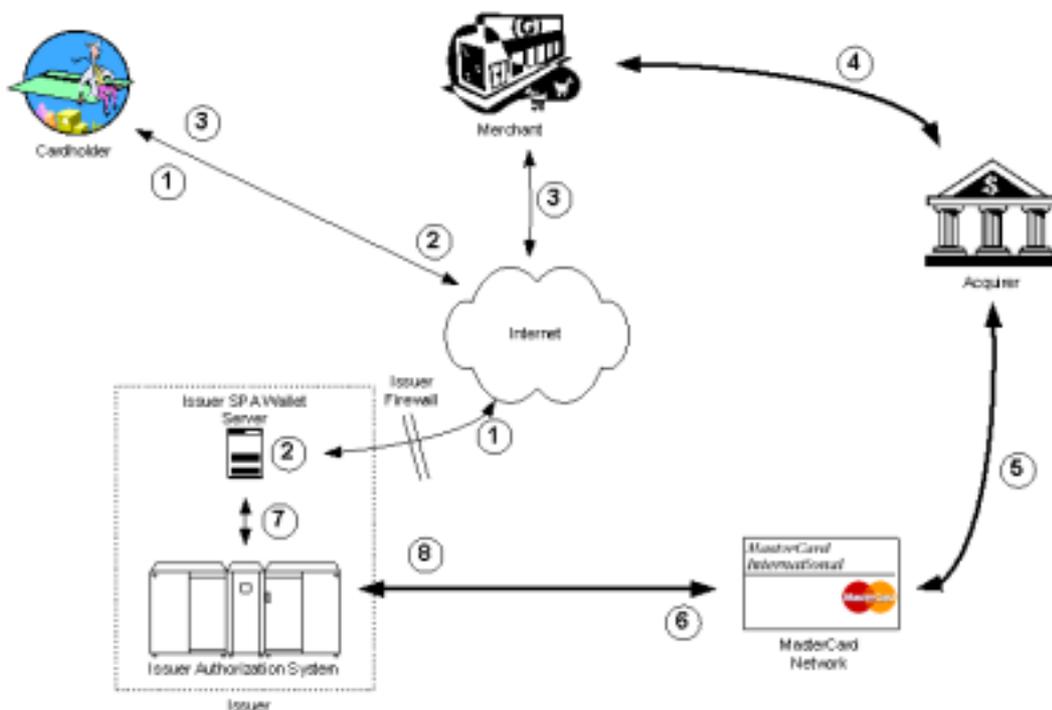


Figure 2: SPA/UCAF

The diagram above summarises a SPA transaction. Similar to ‘Verified by Visa’ a cardholder enrolls for SPA with their issuing bank and the exact choice of authentication method is at the discretion of the issuer. During the shopping experience, when the merchant server requests the payment card details it also includes some hidden fields. These hidden fields include:

- The merchant name, ID, Address and country code
- The sale amount
- An unpredictable number (optional)
- Authentication Data (Blank UCAF)

The cardholder PC will need an applet or wallet application to detect these fields when sent by the merchant site. The wallet will then submit an authentication request to the issuer. The issuer then validates the customer in the agreed manner and generates a transaction specific token value to include in the UCAF field and to store ready for an incoming authorisation request. The SPA wallet then populates the hidden fields on the merchant site in order that the merchant can submit an authorisation request that includes the UCAF value via the acquirer into Mastercard’s network and back to the issuer. If the value in the UCAF field matches (either comparatively or cryptographically according to the authentication method used) the value held at the bank for that transaction, the authorisation proceeds to be processed in the normal way.

Conclusions

It does seem paradoxical that for EMV and SET the card schemes even created jointly owned companies to manage interoperability (EMVCO and SETCO) and compliance issues, yet banks that issue and acquire both VISA and Mastercard and merchants that accept both schemes through their acquirer may need to deploy two separate protocols. Exactly how AmEx plan to join the fray remains unclear at this stage.

Whether this fragmented approach by the card schemes will facilitate speedy deployment or simply create further confusion and inaction amongst banks and merchants remains to be seen. Perhaps by “splitting-up” and looking in differing directions the knights are increasing the chances that one of them will triumph in their quest. What is clear is that the quest is far from over.

[info]

- <http://www.greatdreams.com/arthur.htm>
- http://usa.visa.com/business/merchants/verified_online_purchases.html
- <http://www.mastercardintl.com/about/press/pressreleases.cgi?id=423>
- <http://www.mastercardintl.com/spa/demo/details.html>
- <http://www.mastercardintl.com/spa/demo/features.html>
- <http://www.cardforum.com/html/ccmissue/sep01cov.htm>
- <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2811269,00.html>
- <http://www.worldpay.com/>

[10&3]

Interview: Largest German Credit Card Issuer on Massive Reduction of Charge Backs

Ulrich Riehm (ulrich.riehm@itas.fzk.de) and Arnd Weber (arnd.weber@itas.fzk.de), ITAS, Karlsruhe, Germany, talk to Tilo Schürer (tilo.schuerer@bankgesellschaft.de), Bankgesellschaft Berlin, Germany

/credit cards/security

Tilo Schürer is responsible for product management in the field of electronic business at Bankgesellschaft Berlin. At the beginning of 2000 Schürer pointed in an internal study at the drastic increase in charge backs in Internet business. In the interview he points out that the charge back problem has massively lost importance during recent years. The decisive measure was not improved technology but economic penalties imposed by the credit card organisations. In the interview, there is also a discussion of the viability of new authentication measures (e.g. 3D-Secure or SPA/UCAF). Schürer subsumes that charge back figures are currently so low that the banks could theoretically announce zero liability, at least once a new user of the Internet has registered for a new authentication process.

Bankgesellschaft Berlin is Germany's largest credit card issuer with c. 1.3 million Visacards and Eurocards. They are only issuer, for the acquiring business their partner is B+S Cardservices in Frankfurt. The holding Bankgesellschaft Berlin consists of the Berliner Bank, the Berlin State Bank, Berlin Savings Bank, the Weberbank and the Allbank.

ePSO-N: Mr. Schürer, in March 2000 you sounded the alarm bells. According to your investigation Bankgesellschaft Berlin was making large deficits on Internet-based credit card payments. Can you explain briefly how this came about?

Schürer: If we look at the development of the total number of charge backs, these were under 1,500 in 1997. In November 1999 they achieved a peak of 3,026. The increase was due largely to “MOTO” [Mail Order Telephone Order] payments, which in Germany as a rule means payments from Internet business. The number of charge backs from the MOTO field almost doubled annually from 1997 to 1999. This meant that the MOTO business had been running deficits with a strong tendency to increase for three years. If this development had been allowed to continue, the entire credit card business would have started running losses within fewer than five years. In this situation, it seemed right for me to sound the alarm.

ePSO-N: And how is the situation today?

Schürer: Charge backs from MOTO transactions are diminishing rapidly. This Summer we had 500 to 900 charge backs monthly. This means we have reached the level of 1997. The fraction of charge backs for all Internet transactions in summer 2001 is 0.5%, a year ago it was still c.1%. Since 2001 we have again been making profits. There has been a massive reduction of the number of charge backs for credit card payment on the Internet in 2001. The problem has thus diminished considerably.

ePSO-N: What quality is the data which you used for your assessment?

Schürer: For some time now there has been a so-called ECI flag (Electronic Commerce Indicator), which has to be displayed during credit card transactions on the Internet by merchants and is transmitted via the network of the credit card companies to the banks issuing the cards. However this has only been used correctly and more or less regularly for one year now, so that we could use this indicator as the basis for our assessment from the beginning of 2001 on. Prior to this we relied on special Merchant Category Codes, but that was problematic since a merchant sometimes accepts orders both by traditional means and over the Internet. Now we know that 4.8% of the total number and 4.3% of the total value of all credit card transactions come from the Internet. Those were the figures for August 2001.

ePSO-N: What are the reasons for the high number of charge backs?

Schürer: Unfortunately there is no exact research. Our colleagues from the call centre who receive the applications for cancellations think that about half the MOTO charge backs are from the “red light” area. In some cases the customer does not recognise the merchant on his credit card statement since there is a payment service provider intermediary and the merchant himself does not appear on the statement. A large share of charge backs are also due to so-called recurring payments, such as those caused by subscriptions. A number of Internet providers do not make it sufficiently clear to their customers that the provision of the credit card number automatically creates a regular subscription. Following the second debit at latest the customer then attempts to retrieve this payment from the merchant or the bank which has issued the card. Unfortunately this results in many charge backs, especially in those cases where the merchant does not cancel the regular debit despite termination by the customer.

ePSO-N: Does it have to be assumed that applications for charge backs from customers usually have a fraudulent intent?

Schürer: No, by no means. Of course there is the fraudulent statement that one is not responsible for a transaction, but we do not know their number. Fraud not only takes place on the customer side but also on the merchant side. We estimate that there are equal numbers of customers and merchants involved. Since transactions coming to not existing or closed card accounts are automatically not being processed we do not have a charge back problem on these cards. Fraud can sometimes happen in case card data is being stolen and misused.

We have to consider that the charge back rates for distance selling will by definition be greater than at the point of sale where the goods are handed over directly. In distance selling there will always be faulty shipments, shipments are lost or returns are not reimbursed. The charge back rate on the Internet is now 15 times the size of that at points of sale. In 1999 it was 70 times the size. We are obviously not yet satisfied with this rate, but the upward trend has been stopped and consolidation is clearly discernible.

ePSO-N: Which role does cross-border commerce play in the charge back problem? One may assume that the charge back rate in this field is particularly high due to problems of identification of both the customers and the merchants in cross-border commerce?

Schürer: For us, charge backs were mainly a problem of transaction in US dollars. Since especially with large merchants the so called country codes may not really mean much, we just looked at the currency of transactions. Of the MOTO transactions with US dollars in November 1999, almost 7 percent led to charge backs. For transactions in German marks during the period examined we never had a value higher than one percent. In Summer 2001 the charge back share from Internet business in US dollars was 1.5%, in German marks it was 0.3% and for other currencies 0.6%.

ePSO-N: Which costs do you incur for a charge back?

Schürer: We always examine each charge back, even for the smallest transactions. To our knowledge not all banks do this. Some simply write off disputed transactions up to a certain sum without passing these payments back to the acquirers or merchants as charge backs. This brings with it the danger that these cancellations never come to the attention of the credit card organisations or the merchants and thus that no counter-measures are adopted. From the long-term perspective we do not believe that this makes sense.

For each requested charge back a fax is sent to the acquirer. If there is any need, he sends an enquiry to the merchant. The acquirer then returns the fax, if necessary with attachments. Then we again contact the customer. We always require a written statement from our customers. One third of our cases is solved because the customers never send such a statement. Due to processing the faxes and the written statements a charge back costs us roughly 100 German marks – this value is the same as that given by VISA and Mastercard. This value was also the basis of the win-loss estimate already mentioned.

ePSO-N: In your alarm of March 2000 you demanded the use of authentication procedures in Internet transactions such as digital signatures. In the mean time SET has in our opinion hardly broken through. How did you manage to reduce the charge back rate?

Schürer: The most important counter-measure were the penalties of the credit-card organisations for merchants with too high charge back rates. VISA has for example blacklisted all merchants whose transactions have led to charge backs of over 5%. This Summer the threshold for blacklisting was even lowered to 2.5%. The acquirer of a merchant on the blacklist has to pay \$100 for each charge back. VISA passes \$70 of this on to the issuer for administration costs. It is another matter whether the acquirer can reclaim his money from the merchant. If a merchant stays on the blacklist for more than 2 months, the acquirer has to pay \$200 to VISA. These were the decisive measures to get a handle on the charge back problem. It led to a dramatic strengthening of security measures by many Internet merchants and to an improvement of their customer service processes. The credit card organisations for instance urged merchants to improve the security of their services. They pointed out that merchants should erect firewalls, perform a security audit, and that the administrator of the credit card database should have to submit a criminal record etc.

Several Internet merchants had to reduce their range of products or services or stop accepting credit cards due to unchanged high charge back rates.

As a technical process in mass application, SET has not yet played any major role. Only to the extent that it was possible to provide a technological alternative in support of the “penalty programme”. For merchants using SET for VISA payments inside the EU there has been a very extensive guarantee of payment in effect since 1 June 2001 for all payments (SET and SSL). Even so, SET transactions continue to be negligible.

ePSO-N: There are signals from the EU that interchange fees have to be reduced. Will this have any impact on the profitability of Internet business?

Schürer: It is assumed that the intervention of the EU will lead to a reduction of the interchange fee from about 1.5% to 0.75%. This might mean that the profitability of the MOTO business will again enter a critical zone. If current developments continue, the credit card segment of the Internet will still be profitable at 0.75%.

ePSO-N: How do you see the future for credit card payments on the Internet in general?

Schürer: Generally speaking, I would say that the credit card is the most customer-friendly payment means for the Internet. Banks should advertise with “zero liability” as is the case in the US or for Barclays Bank, instead of stoking fears related to credit card payments on the Internet. Some of my colleagues are afraid that this could cause charge backs to increase once more. In Germany there is need for a change of thinking on this matter.

ePSO-N: There is now discussion on procedures to further reduce credit card fraud on the Internet, such as 3D-Secure from VISA and SPA from Mastercard [cf. ePSO-N 8&2 and 10&2]. If one considers introducing something new, wouldn't it be sensible to analyse exactly what the problem is, i.e. to examine existing charge backs more closely? So that one can choose a method which really solves the problem?

Schürer: It is extremely difficult to identify the exact causes for a charge back. We thus rely on the statistics provided for us by the credit card organisations. These uniformly come to the conclusion that at least 75% of all Internet charge backs could be prevented by a certain authentication of the card holder. For this reason both VISA with 3D-Secure and Mastercard with SPA/UCAF see an urgent need to employ new authentication processes to further reduce charge back figures.

ePSO-N: Does it matter to you which of the new processes is used for Internet payments?

Schürer: Indeed it does. Let us look at Mastercard SPA. Here the Universal Cardholder Authentication Field (UCAF) is created by a SPA wallet server and transmitted via the acquirer to the issuer. This means that the customer has to install a plug-in and then authenticate himself on purchase. However, installation is a barrier. There are bound to be customers who will refuse for fear or ignorance. Another disadvantage of SPA is that to transmit UCAF the data sets passing between the merchant and the acquirer have to be supplemented with a field, at least in Germany. This usually means that expensive programmers (e.g. for COBOL) have to alter the host programmes. This is something people dislike doing and depending on the installation can easily lead to enormous costs. Comprehensive changes to the systems are also needed on the acquirer side. This may damage the overall acceptance of SPA/UCAF.

One could employ Pseudo Card Number systems (PCN). Unfortunately these create a number of back office problems. For instance at Amazon each customer would have a large number of credit card numbers and that would create problems for complaints.

I regard VISA 3D-Secure as the best procedure. Here too the customer authenticates himself, e.g. by means of a password. This means that the card holder has to be registered, as in SPA. However, checking takes place outside of the existing merchant and issuer systems. Following positive authentication a special server belonging to the issuer (the so-called Issuer Access Control Server) signs a message to the merchant. The merchant receives a digitally signed authentication certificate – analogous to the manually signed payment receipt at the POS. VISA 3D-Secure is thus a process which creates hardly any effort on the part of the card holder and the issuer and could thus be introduced highly cost-efficiently.

The banks could then at least announce zero liability once an Internet user has registered for an authentication process.

ePSO-N: Mr. Schürer, many thanks for the interview.

[info]

- Bankgesellschaft Berlin: www.bankgesellschaft.de
- Schürer, Tilo: Die Kreditkarte im Internet. In: Ketterer, Karl-Heinz; Stroborn, Karsten (eds.): Handbuch ePayment. Zahlungsverkehr im Internet: Systeme, Trends und Perspektiven. Fachverlag Deutscher Wirtschaftsdienst, 2002

[10&4]

Hi-tech Payment Technologies in Russia: The Case of Paycash

Victor Dostov (vd@paycash.ru), Paycash Group, St. Petersburg, Russia

/electronic money/privacy/Internet payment systems/Russia

Paycash is a Russian-born Internet payment system based on digital cash. With Paycash, an account can be opened pseudonymously on the Internet. The payments are untraceable, though payments of a single "Paybook" can be linked. In Russia, 200 shops are connected, and more than 400 transactions per day are processed. The company is expanding its business to abroad.

Although the Russian e-commerce market is comparatively small, estimated as a few million dollars per month, modern Internet payment systems are blooming. About 15 systems are competing in a growing market. Reasons are small penetration of traditional payment tools (cards, cheques, private bank accounts), and a high fraud rate which demands something more secure than bare credit card schemes. One of the top players is Paycash, with a system of digital cash. The Russian holding Alkor has rights to the Paycash technology.

The History

In the 1980s, David Chaum proposed digital cash. The main idea was to use digital coins minted by a financial entity. Chaum patented so-called blind signatures which make sure the issuer can't trace the circulation of coins. Practical implementation was slow, however. In 1996 in Russia a group of private investors from Tavrichesky Bank understood that the Internet is flooding this world, including Russia, and some Internet payment tool is needed badly. After short research, digital cash was targeted as a

most advanced technology. The bank established contacts with Chaum's company Digicash, but in vain. So in 1997 Tavrishesky decided to create its own digital cash technology. A group guided by Ildar Khamitov started working on a new payment technology called Paycash.

How Does Paycash Work?

The user first downloads a Wallet from the Paycash server. While running it for the first time, the user types on the keyboard randomly, in order to create the Wallet's keys. A private key will be used to digitally sign all orders to the bank. In fact, the Wallet may use numerous key pairs. E.g., every paybook has its keys used to sign all operations with it. Then, the client orders the bank to open an account, which can be done pseudonymously. This is due more to the difficulty of getting reliable personal information via the Internet than for other reasons. Money can be deposited on the account by common methods, e.g. cash deposit or a Western Union transfer, or, for privacy freaks, with anonymously bought scratch cards. Paycash can be used at the Tavrishesky bank, Guta bank, Russalvbank and another financial institutions which are Paycash's financial partners.

During withdrawal, a newly generated random public key is sent to the bank in a blinded way, as the seed for what we call a Paybook. The user also sends a transfer order. The bank deposits on the Paybook the amount requested. The value is encoded with the help of the powers of the signing operation, for example, for creating five units the bank signs five times. Then the bank deducts the amount transferred from the account. The bank sends the signed Paybook back to the client who unblinds it. Now the client has untraceable financial value in his Wallet.

For a payment, the Wallet sends to the bank through the payee a part of the Paybook, which contains the necessary amount for a given payment. The payee forwards the Paybook information to the bank, which, in turn, searches for the Paybook's database record corresponding to Paybook's public key. If it does not yet exist, the bank creates the record. The latter is used to check for availability of funds and for double-spending. Thanks to the novel method of multiple signing, less storage space is used than in Chaum's original method, in which individual coins for each denomination have to be stored.

With this method, the bank knows from which Paybook payments have been made, but does not know where the money originally came from. It is obvious that all the payments made by means of the same Paybook can be easily linked to each other by the bank via the corresponding virtual account. This can be avoided by creating multiple Paybooks, each replenished from one or many accounts.

The last step of a payment is that the bank deposits the amount on the recipient's account. The whole procedure is described in detail in Khamitov's paper [see info].

Withdrawing money from the system needs some identification of the person who receives the money. For the moment, there are no special methods to withdraw money absolutely privately, as there is insufficient demand for this, and there are also clear legal obstacles for such procedures.

Paycash has a unique feature of fully auditable transactions. In contrast to traditional Internet banking, where a bank (or bank insider) may, at least technologically, unilaterally change client records, forging client balances with no formal proof of this forging available to the client or court, in Paycash, all transactions have the bank's, the payer's and the recipient's signatures which can be audited by a court should a conflict arise. It means that all three transaction parties in Paycash are equal in their rights and guarantees.

If a user loses his private keys, he loses the possibility to make order to the system and, correspondingly, any control over his money. To avoid this, in the latest Paycash version the Bank's accounts may be optionally associated with some personal information which allow the owner to prove his or her rights in case of keys being lost.

To build technology independently of Chaum's system, in Paycash his patents are bypassed or surpassed, and new solutions have been patented, see [info].

Every Wallet allows the transfer of money to another Wallet, the transfer of money in and out the system, etc. The merchant wallet is only slightly different from the basic Wallet and is provided with an API allowing interaction with e-shop software.

A Wallet has a size of 3 MB. This can be critical for mobile applications. Paycash managers do not plan a mobile client until the end of 2002, predicting that then wireless platforms will be powerful enough to handle a minimised Wallet.

Paycash is on-line system. One knows that untraceability could also be possible off-line, which, however, has its price, see Schmidt et al. The main reason why we have chosen to develop the on-line system is that in the off-line system the customer cannot be anonymous when withdrawing money for later double-spending detection.

Business Situation

The system started working as a pilot project in 1998, with an industrial version launched at the end of 2000. Currently, the system has about 200 e-shops connected, covering all practically all significant Russian e-commerce merchants. They offer a wide range of goods like books, CDs, software, etc. Services of ISPs, IP-phone, paging, insurance and Internet-casinos are also included in this list. The customer base is growing rapidly, with now more than 400 transactions per day from 30.000 Paycash-clients downloaded.

Paycash has developed two legal models. One, currently in use, is an agent scheme, in which the payment system operator is an intermediary between the payer and the recipient. Another legal framework, being developed in collaboration with the Russian Central Bank, considers electronic payment as a banking activity. It is to be expected that in 2001 electronic cash will be registered by the Central Bank as a type of banking prepaid financial product.

Is the project a success? From some points of view, yes. The reputation of the system is good both among specialists world-wide and among current customers. The system involves as partners numerous banks and financial organisations, providing easy conversion of "real" money into the system. Along with Alkor Paycash and up to ten representative offices in Russia, there are three joint ventures operating Paycash-based payment system abroad: Alkor Ukraine in Ukraine, NetMaks in Latvia and Cyphermint, Inc. in USA.

The system is growing fast and is financially successful, having raised about 10 million US-Dollars in private investments. However, the global e-commerce crisis has struck, and faster growth had been expected.

A very interesting and controversial issue is the role of privacy in the current legal and social environment. Sometime, privacy is associated with such activities as tax evasion, money laundering and, recently, terrorism. Correspondingly, there are calls for more control over payments. However, the role of payment systems such as Internet-based ones in the aforementioned fraud is exaggerated. Most grey and black money flows are in the traditional banking sphere. Second, as Internet systems only transfer information and use traditional banks for "real" money management, when putting money into a system and taking it out, the control is not significantly weaker.

[info]

- Paycash: www.paycash.ru, see also www.cypherland.com, for the USA see www.cyphermint.com
- For a description of the Paycash system in English, see Ildar M. Khamitov: PayCash Internet Payment System. www.paycash.ru/eng/press/paycash.zip
- More papers in English about Paycash are available at www.paycash.ru/eng/press/library.htm
- Jan Holger Schmidt, Matthias Schunter, Arnd Weber: Can Cash be Digitalised? In: Müller, G.; Rannenber, K. (eds.): Multilateral Security for Global Communication. Addison-Wesley, München 1999, pp. 301-320
- How DigiCash Blew Everything, Next! Magazine Feb 1999
- Some patents by Chaum:
 - David Chaum, Returned Value Blind Signature Systems, U.S. Patent 4 949 380, 14 Aug 1990
 - David Chaum, Blind Unanticipated Signature Systems, U.S. Patent 4 759 064, 19 Jul 1988
- Some Paycash patents:
 - Method For Making A Blind RSA-Signature And Apparatus Therefore. Patent no. 2153191, 20 Jan 2000, by the Russian Patent Office, International application No: PCT/RU99/00197
 - Payment Method And Apparatus Therefore. Patent application: 98120922, by the Russian Patent Office, granted, International application No: PCT/RU99/00264
 - Method For A Cardholder To Request Fulfillment Of An Obligation Associated With The Card And For The Issuer To Acknowledge This Obligation, Patent no. 2144695, 20 Jan 2000 by the Russian Patent Office
 - Method For Forming A Value Document, Patent application: 99122832 by the Russian Patent Office, pending

The author wishes to thank Arnd Weber and Ildar Khamitov for their valuable contributions to the article.

[10&5]

JAP: A Cloak of Invisibility on the Internet

Hannes Federrath (Federrath@inf.tu-dresden.de), Dresden University of Technology, Germany

/privacy/electronic commerce/

JAP is an Internet service designed to enable the unobservable use of the world wide web. In the future, JAP could also be used for anonymous shopping or banking. Invisibility is achieved by communication not taking place directly with the web server, but by detour through a so called mix proxy cascade.

What is JAP?

With JAP (Java Anon Proxy) neither a visited server nor a sniffer can recognise which user has requested which web site. Since many users access the anonymiser service simultaneously, the Internet connections of each user are hidden among those of all other users: Each user could be the origin of a connection. Not even the provider of the anonymiser service is able to determine which connections a certain user has made.

As a rule, at least three mix proxies will work in a cascade, each of which is operated by an independent institution which has declared a self-commitment not to store log files or transported connections, and not to exchange data with the operators of other mix proxies, which could lead to revealing the identity of a JAP user.

The average Internet surfer has a demand for security and privacy. Awareness of a problem is created by drawing his or her attention to the possibility of tracing his or her activities on the Internet. Countless items in the media are currently leading to increased sensitivity in this respect.

For firms, a major role is probably played by protection against industrial espionage. This might have its relevance during patent research or seeking information which might permit assumptions on future products of the enterprise.

Compared to other providers of anonymity services, JAP has the advantage of a high degree of security. In the case of so-called anonymiser proxies, at least the operator is able to observe the users without any problem. Only the Canadian company Zero-Knowledge Systems (ZKS) [info] with its product "Freedom" provided a service similar to JAP. However, ZKS stopped the service in October. ZKS members say this was a market-related decision.

The entire JAP project (client and server) was conceived as a open source project. This allows anyone interested to check the correctness and lack of error of the implementation.

Practical uses

The benefit for customers consists of the fact that they are able to continue to use the Internet for communication and data acquisition, but are now protected against observation:

- Against the Internet provider or the system administrator or boss at the office, who may normally record the entire communications or conditions of communication (with whom does someone communicate) and the contents of information (which information is communicated) of any user;
- Against the server contacted, which might wish to develop a user profile to improve marketing (spam);
- Against third-party servers (e.g. advertising rings), which might trail a user across several Internet sites to develop a broader profile of the interests of a customer (the transparent customer).
- Against secret services. The best-known example is the world-wide surveillance system for electronic communications "ECHELON" of the CIA.
- Against legal authorities and hackers: The Internet Service Providers may be required by law to record all Internet communication and to provide legal authorities with an interface for surveillance, by which means they have access to such data without the knowledge of the provider.

Collecting personal data on the Internet is always linked with very strong commercial interests. JAP is a suitable basis for refined Internet services. Examples are consultant and information services or special services in e-commerce. Services in the context of e-government, such as fora for discussions, are also conceivable.

Technical background

The system consists of a client program (JAP) which each user installs locally on his or her computer. It is also possible for several users to use a common JAP. If there is, for instance, a company-internal Intranet, JAP can be installed on one computer which is connected both with the Intranet and the Internet.

JAP functions as a proxy (e.g. for www browsers) and is connected with the anonymiser service via the Internet. This consists of several interim stations connected sequentially (termed "mixes" by their inventor, David Chaum). Each mix first collects the data packages of several users before re-coding them and outputting them re-sorted. The packages have multiple encoding, and re-coding consists mainly of decrypting.

A user is anonymous among all of the users of the anonymisation service. By means of re-coding the in-coming and out-going data packages have a different appearance. This means that an attacker monitoring all lines has no means of deciding which input data belongs to which output data. Each package has the same size so that it is impossible by this characteristic to combine input and output. The entire process is already secure if one of the mixes employed works correctly. To increase the credibility of the service, several mixes belonging to independent operators should be involved.

Mixes as the basis of anonymisation

The means of functioning of a mix is similar to that of a post office which opens every incoming letter to find enclosed another sealed letter, which it conveys to the address written on it, usually another post office. The next post office does the same actions until the letter delayed by this process finally arrives at its destination. In the world of the Internet the letters are data packages and the post offices are mixes. In order to ensure their relay, the sender must prepare the data packages accordingly, i.e. to pack them (encode), address them (with the address of the final destination), stamp them, etc. This must take place on the user's PC so that no-one else has any knowledge of the addresses on the innermost data packages.

Mix operators can be the data protection commissioners of the Federation or the States, citizens' net associations, religious organisations and particularly institutions whose business typically calls for discretion, e.g. banks, advice centres or the postal service. Obviously Internet Service Providers or security specialist companies could also operate such mixes.

The multiple encoding and re-sorting are however not sufficient. There is a range of other problems threatening anonymity. If one takes these into account, it is possible to develop a system offering protection against observation even by strong attack (big brother).

Conclusion

JAP enables its users to erase their own data trail on the Internet. The software provides self-protection against professional data collectors and firms making their money by selling personality profiles. JAP can be down-loaded and used free of charge [info]. Up to now, the project web page has been visited more than 250,000 times and the program has been downloaded 80,000 times. There are about 5,000 JAP users per day. At peak times there are up to 500 users simultaneously in the system, meaning that the surfing behaviour of each individual merges with that of all other users on-line at the same time.

In combination with an anonymous payment system, such as e-cash or scratch cards, this enables anonymous shopping on the WWW.

The development of JAP is taking place in very close co-operation with the Independent Centre for Privacy Protection in the German state of Schleswig-Holstein and being supported by the Federal Ministry of Economics.

Outlook

The JAP project will provide an “Anonym-O-Meter”. Unlike in other systems the users will be able to see how well anonymity is achieved, i.e. if enough users produce enough traffic.

JAP also plans to allow, in its final stage, users to fine-tune the trade-off between the level of anonymity achieved and the speed of response.

Furthermore, the system is also planned to provide protection against very strong attackers, who are for instance in the position to analyse traffic or to insert or delete packets and thus de-anonymise selected users.

[info]

- Chaum, D.: Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. CACM 1981, 84-88
- JAP: http://anon.inf.tu-dresden.de/index_en.html
- Zero-Knowledge Systems: <http://www.zeroknowledge.com/>
- Slashdot: ZeroKnowledge to Discontinue Anonymity Service: <http://slashdot.org/comments.pl?sid=22261&cid=2388977>

[10&6]

Failure of Beenz and Flooz Indicates the End of Digital Web-Currencies?

Hugo Godschalk (hgodschalk@paysys.de), PaySys Consultancy, Frankfurt, Germany

/electronic money/Internet

Saying the end of these pioneers indicates the failure of private currencies would be a rash conclusion and rather wishful thinking of players within the traditional payment industry (central banks included).

How do you recognise pioneers? They always die with an arrow in their back.

Two revolutionary online payments schemes closed their doors in August. Flooz.com terminated on August 8 without previous warning and went obviously bankrupt. Eight days later its rival beenz.com told their customers that they only had 10 days to spend their beenz money before terminating their member accounts on August 26. Most of the beenz-acceptingetailers then refused to accept it because beenz.com would no longer exchange the incoming beenz against cash. Beenz was founded in March 1998, Flooz imitated the system in September 1999. A short lifecycle, typical of pioneers entering terra incognita in the endless e-world?

Most web-commentators see parallels with the end of other e-payment pioneers like eCash and Cybercash stating that digital currencies as new payment schemes have lost the battle against traditional old economy payment schemes like credit cards. A rash job conclusion because you cannot compare digital currencies like beenz and flooz with payment systems like Ecash (DigiCash) or Cybercash denominated in old economy currencies like DM or Dollar. A currency is not a payment system. It would be mixing up content with packaging. Therefore it makes sense to have a closer look at the revolutionary features of beenz (and flooz).

Beenz and flooz were originally conceived as account-based payment schemes for micropayments on the internet. This is a basic difference to stored value e-money-schemes like Ecash. The balances, held by online shoppers and websurfers at beenz.com, were denominated in a new private currency (“beenz”). The currency could be transferred from one member account to another, but its negotiability was restricted. A beenz unit could be bought byetailers from beenz.com for a fixed exchange rate (1 \$ cent). Beenz-acceptingetailers could sell the units back to beenz.com for a lower rate (between 0.5 and 1 \$ cent). Etailers pumped the new currency into the virtual world as rewards to online shoppers or as gifts to websurfers. The customer could use his earned value points as money to buy goods or services at a memberetailer who accepted the currency. Although other loyalty schemes in the virtual and physical world are very similar to beenz, this scheme was the first to blurr “the line between incentive points and actual currency” [Weber, see info]. Beenz’own headlines pointed out its ambitious vision: “the web’s currency”, “a new kind of money”, “global digital currency”.

From the economic point of view an asset becomes more and more real money if the number of users and acceptors of the means of payment grows. If only one merchant accepts the asset it would be a voucher and not money. So multi-merchant acceptance of beenz supports the monetary

characteristics. (It is interesting to note that from a legal point of view the multi-merchant criterion is also used in e-money regulation). So multi-merchant loyalty systems are per definition on the way from voucher to money (surrogates). It depends on your perspective if you call it a loyalty scheme or a money scheme or both, because a money scheme with limited usage is at the same time always a loyalty scheme by restricting the usage of the money to certain merchants, consumers, products or geographical areas. This restriction of private money turns the purchasing power to these pre-defined areas and could accelerate turnover (bad money drives out good money). It is not possible to achieve this with traditional state money with 100% liquidity and acceptance prescribed by law of legal tender.

Account-based private currency within closed user groups with no or limited redeemability into national currency is not all the rage. All over the world so-called barter-exchanges are operating private currency systems for B2B-, B2C- or C2C-trade (e.g. LETS Local Exchange Trading Systems). So what is really new about private currencies like beenz and flooz, linking business to consumers?

New is the way of creating money and putting it in circulation. Barter and LETS currency is usually created by the accountholder using its (interestless) overdraft facility and transferring the money to another account for payment reasons. The creation mechanism of beenz is quite different. Merchants first exchange traditional cash to private currency and then put it into circulation by transferring it to consumers as a sales related bonus or as a gift. So this privately issued multi-merchant money is – in contrast to a one-merchant voucher – usually always backed by a 100% reserve of traditional money. Based on the natural imbalance between issued and accepted value per merchant a multi-merchant system can only operate with a higher clearing and settlement scheme, rules and regulations and an exchange rate for the incoming and outgoing money.

Customers could use beenz only for spending or to transfer it to other account-holders (gift or against cash). Customers did not have the right to redeem beenz against traditional cash at the issuer beenz.com. In case of terminating the system, “the member will not be entitled to any compensation of any kind for such invalidated beenz”. Exactly that happened in August. The fiasco of beenz and flooz nurtures the strict demands of the ECB for redeemability at par value against central bank money for e-money to prevent private currencies based on e-money. Of course, from the customers point of view redeemability is a very important topic and most e-loyalty schemes do not guarantee it. But what about my hard-earned miles of Lufthansa if they go bankrupt like Swissair? And why redeemability at par value and why against central bank money? (By the way, these questions underline that this controversial article of the e-money Directive is dictated by the ECB mainly for reasons of monetary sovereignty)

To become a global player beenz.com expanded from US and UK into a dozen of countries with regional operational centres (265 employees in 15 offices world-wide). The total “money” volume issued by beenz.com could be estimated to about 1 billion beenz (redemption value approx. 5 m. US \$). Also if 50% of all issued beenz were not redeemed, these figures show that the cash flow income of beenz.com could never cover its world-wide expansion or even the daily expenses. Shrinking initial capital in a market that is not growing fast enough may be one of the main reasons for its failure – as in the case of a lot of other dotcoms.

Additional to this quite normal weak point of dotcoms flooz had also to struggle with the problem of fraud. Flooz.com sold \$ 300,000 of its currency to creditcard thieves acting as pseudo merchants in Russia and the Philippines who paid with stolen creditcards. So flooz.com was not a victim of fraud within their own account-based system but of traditional fraud of another payment system.

Based on available information – the reasons for the failure of both digital currency schemes seems to be quite usual and not immanent to the new product.

We see very successful multi-merchant loyalty/money-schemes in the physical world. Some of them are based on back-office accounts with a card as access instrument (e.g. Airmiles in the Netherlands or Payback in Germany). Other schemes come up with stored value chipcards with e-money denominated in private currencies. In the physical world the hype of multi-merchant schemes has already started. In the virtual world of e-commerce it is still a niche. Beenz tried to make a link to the physical world. But it was obviously already too late to change the strategy from virtual to physical. The old economy law of the necessity of making a business case shot its fatal arrows into the courageous pioneers. Maybe beenz and flooz as private digital web-currencies were ahead of their time.

[info]

- Barter business: www.irta.com
- Beenz: ePSO Inventory DataBase (eps0.jrc.es)
- LETS: www.ex.ac.uk/~RDavies/arian/local.html , www.cyberclass.net/turmel/urlsnat.htm , www.strohalm.nl/bookmarks/alles.htm
- Private currency: Jérôme Blanc, Les Monnaies Parallèles, Paris 2000
- Thomas E. Weber, Beenz Slowly Gain Currency on the Net, Wallstreet Journal, 20.12.1999.

[10&7]

ePSO Final Conference on Consumer Online Payments: Trends and Challenges for Europe

Ioannis Maghiros (ioannis.maghiros@jrc.es), IPTS, Seville, Spain

/electronic payment systems/European Commission/ePSO

As part of the ePSO project deliverables, a one day conference entitled “ePSO Final Conference on Consumer Online Payments: Trends and Challenges for Europe”, will be held in Brussels on 19th February 2002. The conference will: (a) set the stage for state-of-the-art e-payment systems presentations; (b) allow actors to exchange views on existing trends and future developments, and (c) reinforce and extend the interaction links established by ePSO during its operation.

The growing importance of retail Internet payments for the adoption of business-to-consumer e-commerce emphasises the need for a systematic exchange of strategic information in order to reconcile the sometimes disparate views of market players. To facilitate this exchange has been a major objective of ePSO. A number of crucial issues have already been raised during the development of the Observatory and the ePSO final Conference will provide the stage for these issues to be presented and debated publicly.

The Conference will be a one-day event, 9.30 a.m. – 5.00 p.m. A total of five sessions is planned, beginning with a plenary session, followed by three parallel sessions, and ending with a final plenary session. While the Conference organisation is based on a unidirectional presentation style, care has been taken to encourage communication and interaction among participants.

Conference participation will be free, by invitation only and ePSO-Forum subscribers are most welcome to attend. The conference audience is expected to include representatives from the financial services, Internet services, telecommunication operators, standards bodies, supervisory authorities, retail and consumer protection associations as well as legal experts, ICT developers and suppliers, consultants, and academics.

The individual sessions have the following objectives:

Session 1: e-Payment Systems: Trends and Challenges for Europe (plenary session)

This session will provide the opportunity for main public and private actors to identify state-of-the-art solutions for the various challenges that the market faces as well as to set the stage for future developments in the field.

Session 2: Innovation and Regulation (parallel session)

Market players will present state-of-the-art tools and services in the e-payments field, emphasising their innovative characteristics and the solutions they offer to identified challenges. Long-term impacts of the use of the technology will also be addressed. Special emphasis will also be paid to infrastructure requirements.

Session 3: Standards and Interoperability (parallel session)

The many standardisation efforts and activities that will have an impact in the near future will be presented. Issues presented will include cross-border solutions (beyond the credit card), the importance of standards and the feasibility of a global interoperable solution (as opposed to a few islands of interoperability), new payment modes and channels and their standardisation needs.

Session 4: Security and Infrastructure (parallel session)

Key actors will present their efforts towards a secure infrastructure for e-payments. Requirements imposed by mobility and ubiquitous computing trends will also be addressed. New security

technologies (biometrics, strong authentication) as well as measures to enhance the consumers' perception of security will also be discussed.

Session 5: e-Payment Systems: Way Forward (plenary session)

Within this session the summary of the proceedings of the three parallel sessions will be presented with a view to prioritising requirements for standardisation and/or policy making activities. A presentation on the issue of "e-payment systems for digital goods" – a topic of particular interest for the future of an Information Europe – will close this session.

[info]

- ePSO conference site: <http://epso.jrc.es/conference/>
- Likely attendees are kindly asked to pre-register for the conference by filling-in electronically the form at <http://epso.jrc.es/conference/register.cfm/>. They will then receive a confirmation of pre-registration and soon after an invitation to the conference.

[10&8]

Meet the Heavyweight of Payment System Statistics: ECB's 'Blue Book'

Leo Van Hove (Leo.Van.Hove@vub.ac.be), Free University of Brussels, Belgium

/review/statistics/payment systems/settlement systems/EU/

Not counting the yearly statistical addenda, the previous edition of "Payment and Securities Settlement Systems in the European Union" dated back from 1996. In the meantime advances in technology have had a profound effect on payment systems. It was therefore a timely decision of the European Central Bank to publish an update of its 'Blue Book'. An overview and some personal observations are provided.

I readily admit it: this time I have not completely read the document that I had to review. But then the new edition of what has come to be known as the 'Blue Book' contains no less than 500 pages of text and another 200 pages of statistical data. Moreover, the Blue Book is not meant to be a report one reads from a to z in search of ground-breaking analysis. Rather it is a reference work one consults when in need of either data on or a description of a certain part of the payment system of a EU country. So I hope the editor will forgive me for having been selective in my reading.

There are basically three parts to the report: the chapter on the euro area, 15 country chapters, and the statistical tables in the annexes. The euro area chapter is a novelty compared to the previous edition. A first section provides an overview of the common institutional aspects, including the legal and regulatory framework on the euro-zone level. The bulk of the attention goes to the dual role of the Eurosystem as an overseer and service provider. The second section provides a description – on an aggregated level – of the usage of payment media by non-banks. On reading this section I could not help being struck once again by the major differences that exist among EU countries. For example, whereas credit transfers are the preferred non-cash payment instrument in more than half of the euro area countries (Finland leading the pack with a figure of 59% of all non-cash transactions), in 1998 they only made up a meagre 18% in France. However, on closer scrutiny some of these differences prove to be amplified by differences in reporting rules (see below). A salient observation is also the lack of popularity of electronic money: in 1999 only 0.3% of transactions were conducted using e-money, which nevertheless represents a doubling of the 1998 figure. The third section of the euro area chapter focusses on interbank transfer and settlement systems on the euro-zone level, both large-value and low-value. Needless to say, there is a very detailed description of TARGET. Also covered are: Euro 1, STEP-1, etc., but also international card organisations such as Europay and Visa and cross-border e-money initiatives such as PACE and the Ducato CEPS-pilot. The fourth and final section describes the various securities settlement systems.

The country chapters, which are written by the respective national banks, follow the same outline as the euro area chapter. Compared to the previous edition, just about all sections have been substantially expanded: section 2 in order to include e-money and card-based schemes; section 3 because of the introduction of RTGS systems; and section 4 in order to include a description of the trading structure and the clearing houses – the goal being to follow a security from when it is traded through to the settlement process. Note that systems are described as of November 2000.

Finally, the annexes contain both cross-country comparative tables and a set of statistical data for each country (covering the 1995-99 period). Researchers will be happy to learn that all data are made available for downloading in a format that can be imported into most spreadsheets.

On the whole, the Blue Book is obviously a reference work of great value for anyone doing research on payment systems in the EU. It remains the most comprehensive collection of data and text on the subject. And the euro area chapter is clearly an addition, transforming the Blue Book into more than just a compilation of chapters written by the individual national banks. However, this is not to say that the 700+ pp. 'heavyweight of payment statistics' wins by knock-out in the first round. Firstly, at times it has a surprisingly low guard. On analysing the data on electronic purses I found several inaccuracies. For example, the methodological annex states – and with reason – that where the item 'cards with an e-money function' is concerned “only the number of valid cards in circulation should be provided, not the number of cards issued, since this figure would not be very informative if empty or invalid cards were included” (p. 718). But only the data for Italy and Sweden appear to conform to this rule, thus seriously compromising cross-country comparisons. The comparative table (on p. 526) also does not mention that the bulk of Danish Danmønt cards are in fact disposable cards. In the case of Belgium, even an intertemporal analysis would lead to erroneous conclusions since the data for 1996-97 relate to the number of activated cards, whereas the data for 1998-99 relate to the total number of cards issued. The Blue Book owes it to its status to avoid these and other mistakes, which are now likely to start leading a life of their own.

Secondly, here and there our heavyweight champion would also benefit from working out a bit more. In the information age we are living in, it is disappointing to see that the most recent data relate to 1999, which is not such as to “facilitate the analysis of recent developments” (p. 7). I also expected the euro area chapter to offer explanations for the large intra-EU differences rather than mere descriptions – but this is perhaps a sensitive issue due to competence battles between the ECB and the National Central Banks. Such an analytical perspective would probably have the positive side-effect of improving the quality of the description. To illustrate, p. 28 states that “trailing in the number of credit cards in circulation was France with a mere 20 cards per 1,000 inhabitants”. My suspicion is that this is (again) a definition problem, with cards that elsewhere would be termed credit cards being classified as debit cards in French statistics (see p. 231). And according to Arnd Weber there are similar definition problems concerning the German payment card data (cf. p. 133 and p. 577).

Finally, I would like to call upon the ECB to consider introducing two novelties. First, as Knud Böhle has argued in ePSO-N 4, there is a huge lack of data that relate payment instruments and payment purposes. In the future it will become increasingly important for researchers to be able to make a distinction between, say, a credit card that is used in a shop and one that is used to pay a bill on-line. I would therefore urge the ECB to set up a framework enabling the collection of such data. At the same time the ECB should in my view also start collecting data on costs and prices – after the example of the Norges Bank; see [info]-section. An implicit message in the early pages of the Blue Book seems to be that the ECB is convinced that while the harmonisation and consolidation triggered by the introduction of the euro has so far been particularly prevalent in large-value payment systems, it might in the near future also affect retail payment systems. Given the large intra-EU differences in the use of payment media, there must inevitably be large differences in the level of efficiency of the countries' payment systems. It would therefore be most helpful to have a EU-wide instrument-board on costs and prices, if only to make sure that the harmonisation does not turn into a levelling towards the bottom. If a new edition of the Blue Book stepped into the ring with these two additions (and harmonised reporting rules), it would be outright unbeatable.

[info]

- **Böhle, K.**, On hype, sacred cows, data holes, and how to cope with them, *ePSO Newsletter*, No. 4, January 2001. epso.jrc.es/newsletter/vol04/6.html
- **European Central Bank**, *Payment and securities settlement systems in the European Union ('Blue Book')*, third edition, Frankfurt, June 2001. www.ecb.int/pub/bluebook/bluebook.htm
- **Van Hove, L.**, Payment statistics: Norges Bank show the way, *ePSO Newsletter*, No. 6, March 2001. epso.jrc.es/newsletter/vol06/8.html

ePSO Newsletter – Issue 11, December 2001

[11&1]

Editorial: The Vulnerability of Technology – the Achilles' Heel of Globalisation

Michael Rader (rader@itas.fzk.de), *Arnd Weber* (arnd.weber@itas.fzk.de), *Ulrich Riehm* (ulrich.riehm@itas.fzk.de) ITAS, Karlsruhe, Germany

/vulnerability/regulation/EMI/UMSA/ECLIP/technology assessment

While the main focus of this issue is on legal aspects of electronic payment systems, the events of September 11 have served to remind us of our dependence on technology and of its extreme vulnerability and have motivated two contributions. In this issue ePSO starts broadening its perspective towards e-commerce and payment integration. The E-commerce track of a major congress on Technology Assessment and the e-Society, and the ePSO workshop on payment integration into e-commerce serve as starting points. The focus compares the US and EU approaches to regulation of e-money and is completed by a review of a recent ECLIP study.

A mere quarter of a year later, it is clear that the unexpected and shocking attacks with hijacked airliners on the World Trade Center and the Pentagon on September 11 will go down in the history books as a turning point. If nothing else, the enormous loss of life and destruction resulting from the attacks reminded those of us living comfortable lives and concerning ourselves with such luxuries as electronic payment systems that the world is not the cosy place we would like to think, and that struggles for personal survival are far more commonplace than electronic shopping sprees. The attacks have also reminded us of two features of technology that we usually conveniently suppress in our awareness: in the wrong hands and for the wrong uses, technology can have devastating negative impact, and as witnessed by the temporary shut-down of the Wall Street Stock Exchange, many of the important institutions that determine our daily lives are crucially dependent on the functioning of highly sophisticated and extremely sensitive technology.

The events of September 11 set Luigi Sciusco to thinking about the required features of an attack-resistant infrastructure for payment systems. He argues for the development of contingency solutions rather than for the conventional secondary site. Vulnerability was one of the main topics of a major congress on technology assessment and the e-Society, which took place in Berlin from 17 to 19 October. Inspired by the presentations at this event, Arnd Weber outlines EU-level activities developed to shield citizens from the negative impacts of vulnerable technology. Knud Böhle reports on the conference as such, giving special attention to the track on e-commerce. Another report from Knud presents findings from a recent IPTS workshop on the Integration of Internet payment systems into e-commerce.

In departure from its normal format, which starts with the “focus”, this issue concludes with a mini focus on the legal aspects of regulating electronic money, in particular comparing the situations in the US and Europe. Anita Ramasastry, a professor at the Washington School of Law in Seattle introduces us to the US Uniform Money Services Act (UMSA), while Rufus Pichler, an attorney practising in the US but originating from Europe – Germany to be precise – compares it with the EU Electronic Money Institutions Directive. While electronic money in the US has in the past been regulated within the framework of laws created before its existence, the UMSA is a new state safety and soundness law creating provisions for the licensing of electronic money businesses. This issue, Leo van Hove's review happens to be on a publication in the legal domain and thus extends the focus. His subject is the second report from the Electronic Commerce Legal Issues Platform (ECLIP) of the European Commission, which examines potential for the improvement of the legal framework governing the development and use of electronic money.

Coming back to recent events, but on a somewhat lighter note, the past few weeks have seen the successful launch of two films in which wizards play a major role. Even more recently, in fact during the past week, we have witnessed the first official distribution – camouflaged as sale or presentation – of Euro coins. If memory serves well, there were plans to have an electronic Euro in circulation well before its real-world counterpart. Well, it looks as though unless one of those wizards can be lured away from the presumably bigger money to be earned from acting in the movies, we're still going to have to wait a while before we have the universally accepted electronic Euro.

Let us conclude by wishing our gratifyingly enlarged readership successful and prosperous New Year from the entire ePSO-N team.

**[11&2]
The Day After**

Luigi Sciusco, (sciusco@tiscalinet.it), Rome, Italy

/payment infrastructure/security/vulnerability

The tragic events of 11 September have changed the traditional scenario for business continuity management. What are the possible consequences of a military attack upon payment systems infrastructures? Do we have any possibility to react to this threat?

Contingency planning, for non military environments, usually deals with natural disasters (e.g. fire, flood, equipment or software failure) and sometimes with “limited” terrorism (e.g. a bomb in the main building). Before 11 September information security managers were not committed to think about a large scale military attack that simultaneously destroys primary and secondary EDP sites. They were much more involved in security countermeasures to prevent, mitigate and react against new “logical” attacks, because physical protection was considered a well known problem: it (only) required a lot of money for redundant systems. On 11 September some payment systems players were able to operate by their recovery sites, others were not because their key business people had died and their expensive secondary sites could not work, others did not have a contingency site. The effect on the smooth functioning of European payment systems was negligible and also in the U.S. the major systems were operating without interruption. However, in some cases, payment systems infrastructures had to face a liquidity shortage and operating times were extended to allow banks to input payments. But the attack was not intended against payment systems and therefore consequences on it were only a “side effect”. Payment systems were not strongly affected by it and the countermeasures were the “traditional” liquidity control instruments used by Central Bankers. Payment systems could also be (hopefully not!) the goal of a future attack and, in that case, nothing would work and Central Bankers could not use their tools to input liquidity in the system. Therefore we should try to design new, “terrorist-tolerant”, architectures. Anyway the attack had a serious effect on payment systems: oversight authorities and providers are critically assessing disaster recovery solutions against this kind of threats.

Payment systems today depend strongly on critical infrastructures: networks, automated clearing houses, real time gross settlement systems, etc. Are our payment systems ready to survive if one of these global infrastructures is not available for, let’s say, one week? I don’t think so. It is really hard to imagine what could happen. Whenever there is a major problem (no longer than just a couple of hours!) in one of these infrastructures, banks have to face a lack of incoming payments and this can generate a knock out effect in the system: banks that don’t receive payments need liquidity and stop outgoing payments. It is possible to induce a gridlock, a situation in which any participant has to wait for someone else to finish its task (send outgoing payments) and at some point everyone is blocked. Authorities usually provide liquidity to the market to prevent this situation and, if needed, activate gridlock resolution schemes. What happens if the payment infrastructure is completely out of service for ten days?

Secondary data centres and fault tolerant systems are very expensive and they are unable to face a large scale military attack. Secondary sites usually provide EDP facilities but they do not have backups for business people, it would be too expensive. If an aeroplane crashes on the primary site and nobody survives to restart and manage operations from the secondary site, the disaster recovery centre will be useless. Some payment systems providers immediately sent home an emergency team after the attack of 11 September: they stayed at home for one week and received their salary but now they are back in the office.

When we faced Y2K we discovered that credit cards companies have an excellent recovery solution based on paper forms. But they have a little problem: their current structure is able to manage manually not more than 5% of transactions. Payment systems today rely heavily on IT and we cannot even imagine a manual recovery.

We are dealing with “military” attacks and this could be the key word. Humans are bizarre: they like to invest their best technology, scientists and a lot of money to kill one another. For this reason

many improvements in our “civil” life come from military researches, also in this case. We would like to have reliable infrastructures and procedures that cannot be destroyed because they are completely distributed, all over the world. An attack could destroy a part of the infrastructure, that would not work, but the failure would not spread through the system. The infrastructure would be able to isolate the failure and to reconfigure by itself.

It sounds familiar: it looks like the network, created for military applications, that you used to download this newsletter. Do you remember that more than thirty years ago the RAND Corporation faced an odd strategic problem: how could the US authorities successfully communicate after a nuclear war? The RAND proposal (1964) for a network was built on two basic concepts: “have no central authority” and “designed from the beginning to operate while in tatters”. The principles were simple. The network itself would be assumed to be unreliable at all times and designed to transcend its own unreliability. Yes, the Internet architecture could be the great revolution for completely reliable payment systems infrastructures. In this respect infrastructures should shift from the “no single point of failure” logic to the “unlimited points of failure” paradigm. They already moved from mainframe solutions to distributed procedures, but today they could need to go forth to network applications: not to save money or improve efficiency but to give payment systems a chance to survive. The move towards network applications won't happen on the grounds of a mere technological shift. New architectures are generally established on the evolution of business requirements and the new requirement is: payment systems must work under all circumstances.

However be careful: I am not talking about downloading MP3 files, Internet payments, distributed denial of service attacks on major e-commerce web sites and so on. I am dealing with vital infrastructures used to transmit billions of Euros every second. I cannot imagine to develop such infrastructures with the existing methodologies and tools for network applications: confidentiality, availability, integrity, non repudiation, notarisation, time-stamping, guaranteed service levels, etc. are some of the key requirements for this kind of applications and today it is not easy to satisfy such requirements in a highly reliable way with network applications. Payment systems infrastructures could gradually move to network architectures. They could start developing a contingency solution based on network applications, with lower levels of service and security with respect to the “primary procedure” but allowing payment systems to work at an acceptable level, always. In this case payment systems would have to face an increased residual risk in contingency situation; it could be managed with new legal and organisational arrangements. But probably such a contingency architecture would be less and less expensive than a fully redundant secondary site. Besides this contingency solution would be usually available for testing and this could help a smooth migration towards the new architecture. Also the importance of staff working from home should not be underestimated as an application of network architectures to human resources.

[info]

- Design principles of the web (www.w3.org/Consortium)
- History of ARPANET (www.dei.isep.ipp.pt/docs/arpa.html)
- Short history of the Internet (www.forthnet.gr/forthnet/isoc/short.history.of.internet)

[11&3]

Worms, Disputes and Rolling Blackouts – Protecting the Citizen

Arnd Weber (arnd.weber@itas.fzk.de), ITAS, Karlsruhe, Germany

/electronic commerce/electronic markets/security/vulnerability

This article compiles some fields of current and potential future activities by the European Commission in the area of vulnerabilities of the “Information Society”. First, some Commission actions on computer incidents are reviewed. Second, activities in the field of trans-border dispute resolution are addressed. Third, a new field is addressed in which no concrete actions have taken place so far: potentially disastrous interactions between liberalisation in the energy sector and the availability of power for electronic networks and computers.

Vulnerabilities

David Wilkinson, Director of the European Commission’s Joint Research Centre’s “Institute for the Protection and Security of the Citizen” in Ispra, Italy, has pointed out that computer incidents increased from about 21,756 in the year 2000 to about 15,000 in first half year 2001 alone, e.g. incidents such as the recent Goner Worm (see CERT [info]). He also reported about vulnerabilities of information systems (e.g., a known way for an attacker to pass a firewall). The number of vulnerabilities grew from 1,090 in the year 2000 to about 1,000 in only the first half year 2001. Accordingly, the European Commission wants to take action and foster the discussion about European co-ordination among existing and future Computer Emergency Response Teams (see EWIS [info]). Finally, Wilkinson mentioned the operating system insecurity causing many intrusions and affecting all on-line citizens [info]. It remains to be seen what action the Commission will take to address that issue.

Trans-border Dispute Resolution

At the eSociety conference in Berlin [see next article] Wilkinson also pointed out to “FIN-NET”, a network for facilitating out-of-court consumer disputes in financial services when the service provider is established in a Member State other than that where the consumer lives. The Commission has also taken action to support alternative dispute resolution with the “European Extra-Judicial Network” pilot launched Oct. 16th, 2001. EEJ-Net’s objective is to facilitate consumer redress in disputes originating from trans-border purchases (see [info]).

Rolling Blackouts

A new type of vulnerabilities of networks has been spelt out by Marcelo Masera and Marc Wilikens, also from the Joint Research Centre in Ispra, and Marcin Wardaszko from the Academy of Entrepreneurship and Management in Warsaw, Poland. “Rolling blackouts” could be due to an attack which evolves like this: Suppose you can buy electricity over the WWW from a provider, such as an electricity provider or a trading company. Imagine an attack is made on the servers or end-user devices used. Then users not only can no longer order electricity, perhaps they can’t even use their computers if the servers don’t allocate electricity, and maybe not even make a telephone call.

You think the scenario is unlikely? Trading of electricity energy on the Web has already started. “Electronic or screen-based trading plays an increasingly important role in worldwide wholesale as well as retail electricity markets,” as Stefan Strecker writes on his homepage dedicated to electricity trading. Trading not only happens on a large scale, as by Enron and its partners, but also in the B2C market, e.g. in the UK. Here uSwitch.com gives you a choice to change your provider on-line. Or have a look how you can mix your power when buying from “E.ON” who give you a choice to select between wind or atomic energy etc. Maybe you don’t really use your browser to select electrons but rather only the price, in the case of E.ON. But the examples show that purchasing energy might evolve much like telephone providers can increasingly be selected call-by-call. The providers will certainly aim at protecting their servers, but how to prevent denial of service attacks or virus attacks on PCs? So the question is whether such attacks could take place just like the recent power blackouts in California happened, where deregulation was said to have led to the lack of reserve facilities. Similar problems

had already emerged in a Scandinavian energy crisis in the mid '80ies [see Wardaszko]. Therefore “re-regulation” of the field has been discussed. Or, as Silvio Funtowicz, also from Ispra, put it: “We knew about these problems. Why did we not prepare ourselves?”

[info]

- Carnegie Mellon University’s CERT Coordination Center: <http://www.cert.org/>
- E.ON: <http://www.eon-energie.com>
- European Commission’s Early Warning and Information System forum: <http://ewis.jrc.it>
- European Commission’s eConfidence forum: see <http://econfidence.jrc.it> and the press release of Oct. 16, 2001 at http://www.europa.eu.int/comm/consumers/policy/developments/acce_just/index_en.html
- FIN-NET: Financial services: Commission launches out-of-court Complaints Network to improve consumer confidence: http://europa.eu.int/comm/internal_market/en/finances/consumer/adr.htm
- Funtowicz, Silvio: Comment made at the conference “Innovations for an e-Society. Challenges for Technology Assessment”, Berlin 17-19.10.2001
- Masera, Marcelo; Wilikens, Marc: Trust and Vulnerabilities in the Information Infrastructure. Paper available at: <http://www.itas.fzk.de/e-society/preprints/vulnerability/MaseraWilikens.pdf>
- Stefan Strecker’s homepage with links on electricity trading: <http://stefanstrecker.com/>
- uSwitch: <http://www.uswitch.com>
- Wardaszko, Marcin: Rolling blackouts threat to the information society. Paper available at <http://www.itas.fzk.de/e-society/preprints/vulnerability/Wardaszko.pdf>
- Wilkinson, David: Protection and Security of Citizens in the Information Society. Paper available at: <http://www.itas.fzk.de/e-society/preprints/vulnerability/Wilkinson.pdf>

[11&4]

Innovations for an e-Society. Challenges for Technology Assessment – A Note on the E-Commerce Track of the Conference

Knud Böhle (knud.bohle@jrc.es) IPTS, Seville, Spain

/electronic commerce/electronic payment systems/electronic markets/digital goods

The conference “Innovations for an e-Society. Challenges for Technology Assessment” was organised by ITAS (Institute of Technology Assessment and Systems Analysis of Karlsruhe Research Centre) and VDI/VDE IT (organisation of German Engineers) on behalf of the German Federal Ministry of Education and Research. The conference took place in Berlin, October 17 to 19. Almost 100 presentations were given. In this article we will look at some presentations from the “e-commerce” track. Presentations stressed that the Internet is far from being a frictionless market place, and payments for digital goods are an underestimated problem. Difficulties of appropriate legislation came up in the talk about eBay vs. Bidder’s Edge. The conference proceedings will be available online (see [info]).

This “e-commerce track” covering 12 presentations from six countries was chaired by Jean-Claude Burgelmann (IPTS) and Pascal Verhoest (TNO-STB). The latter also presented findings of the EBIP-Project (Electronic Commerce Business Impacts Project) in his invited talk. In this B2B project, with OECD, IPTS, TNO and others partnering, 179 case studies in 17 sectors and 10 countries were carried out, investigating the impact of the Internet on traditional industries. To mention just one result, horizontally as well as vertically co-ordinated market systems are increasingly organised as networks. This, however, goes together with “lock in” effects e.g. into integrated IT systems or into marketplaces. The switching costs are in both cases high. Network externalities also go together with risks of new dependencies and exclusion, making the change to alternative suppliers difficult. All in all, instead of a pure trend towards “value networks”, EBIP expects hierarchies with network characteristics.

While the invited talk was about B2B, the remaining contributions dealt with the B2C-sector. Michael Latzer and Stefan W. Schmitz of the Austrian Academy of Science, Vienna, gave a convincing talk B-2-C e-commerce: a frictionless market is not in sight analysing the difference between the technical potential of the Internet to allow for perfect markets and the many impediments and business strategies that inhibit it. At present the Internet even seems to foster information asymmetries and lack of market transparency. Studies show that a strong concentration on few market leaders is taking place. In this context also, the assumption that lower sunk costs facilitate market entry

in e-commerce was questioned. Although the exogenous, initial technology dependent costs are relatively low, the endogenous sunk costs increase (e.g. for marketing and advertising). Facts also tell of price discrimination on the Internet, in general an indicator of low competition. Companies are able to deliberately avoid price comparison mechanisms and to lock customers in by e.g. personalisation of WebPages. Despite the indication of market insufficiencies, the authors don't strive for a new interventionism and warned not to replace market inefficiencies by regulatory inefficiencies.

Elad Harison of MERIT (Maastricht Economic Research Institute on Innovation and Technology) analysed the most interesting law suit eBay vs. Bidder's Edge, a small competitor of eBay, using "intelligent agent"-software to search a range of online-auctions for bids and to present the aggregated results to its clients. Apparently this was not in the interest of eBay, although maybe in the interest of market transparency helping to lower transaction costs. First eBay tried to get rid of Bidder's Edge automated searches by a user agreement (regarding of course robots as users) forbidding monitoring and copying of WebPages; then they applied technical measures that did not work well. Negotiations with Bidder's Edge also failed. eBay then accused Bidder's Edge of five different types of infringements. Next interesting point is the reasoning of the Court in favour of eBay. Of the five counts, the Court chose the legal figure of "trespass to chattels" meaning here that the "intelligent agent" had not respected the access agreement and diminished the capacity of eBay's computer system leading to "reputational harm". Elad Harison as well as a group of professors on high technology law regard this as an outstanding, although not first case of myopic jurisdiction in matters of new technologies.

The talk by Carsten Orwat, ITAS, based on a study (by Riehm, Orwat, Wingert) on the German book selling industry was focused on (des)intermediation. He argued that while traditional booksellers are likely to lose a share to online-booksellers, the winners won't be the pure online book sellers, but the incumbent intermediaries of the branch: the wholesalers. In the field of digital content more desintermediation might take place, but Orwat held that to make this market happen, new intermediaries would be required first. In addition he claimed that at present the providers of digital content are still faced with a range of unresolved basic problems such as inefficient production environments for digital content, insufficient protection of intellectual property rights, insufficient quality of reading devices and a lack of adequate payment systems.

The contribution by Jan Wessels (VDI/VDE) dealt with the commercialisation of digital content on the Internet. His talk has to be seen in the context of the eContent-programme of DG Information Society. A scenario in which large US American companies dominate the market of paid digital content seems likely, and support for European content industries is a political issue. Three studies were commissioned to prepare the eContent-programme, one of them from VDI/VDE-IT, INBIS and PriceWaterhouseCoopers titled "Access to Capital for Content Industries". It is expected that content providers will develop strategies for the future with a mix of free and paid content. At present the major problem seems to be to change the habits of Internet users who have grown up with free content. Simple and user-friendly payment systems would play a crucial role in changing existing mind sets. Accordingly Napster was interpreted as the failure of the music industry to establish such a payment mechanism in a timely fashion.

Internet payments were also subject of a small IPTS/ITAS study "Technology assessment and electronic money – between consultancy and oversight" by Knud Böhle (IPTS/ITAS), Michael Rader, Ulrich Riehm and Arnd Weber (ITAS). Six assessment studies of e-money carried out between 1996 and 1999 were compared and lessons were drawn for future technology assessment in the field. It turned out that the typical role of technology assessment, namely to advise political decision makers on urgent technology related matters, was not paramount. Even in cases where direct policy advice was requested, it was half-hearted and the research groups were not provided with sufficient resources for fully fledged TA. But TA is changing and has already changed. A new function can be envisaged in the organisation of communication at a relatively early point in time of technology development and deployment. In a long term perspective continuous structured debate among stakeholders and interested groups about new technologies and their potential impact might become a prerequisite for informed decisions. Electronic discussion fora on the Internet can be part of this effort. In the ITAS-project on Internet-Payments (1997-1999) and in the current ePSO project this element of communication has already been built-in.

[info]

- Innovations for an e-Society. Challenges for Technology Assessment, Berlin 17-19.10.2001. Conference program and papers will be available at <http://www.itas.fzk.de/e-society/>. The above referenced papers can already be downloaded:
 - <http://www.itas.fzk.de/e-society/preprints/ecommerce/LatzerSchmitz.pdf>
 - <http://www.itas.fzk.de/e-society/preprints/ecommerce/CowanHarison.pdf>
 - <http://www.itas.fzk.de/e-society/preprints/ecommerce/Orwatetal.pdf>
 - <http://www.itas.fzk.de/e-society/preprints/ecommerce/Wessels.pdf>
 - <http://www.itas.fzk.de/e-society/preprints/ecommerce/Boehleetal.pdf>
- For the EBIP report see the OECD Information Economy web page (one of the activities of DSTI): www.oecd.org/sti/information-economy
- The eContent programme homepage is at <http://www.cordis.lu/econtent>; the report “Access to Capital for Content Industries” is available at <http://www.cordis.lu/econtent/studies.htm#access>

[11&5]

Integration of Internet Payment Systems – What's the Problem?

Knud Böhle (knud.bohle@jrc.es), IPTS, Sevilla, Spain

/electronic payment systems/electronic commerce/ePSO

Based on the ePSO workshop on the Integration of Internet payment systems into e-commerce, 9th of November, some thoughts on the “real integration problem” are presented. Attention is drawn to the difference between integration of the “payment function” and “payment systems”, the difficulties to provide for a common user experience, and the potential of integration by “disintegration”.

In November 2001 ePSO organised a workshop on payment, presenting a complex picture of the subject and a basket full of problems (see reference to minutes and other workshop details in the [info] section). But days later you sit back and wonder what the real integration problem is.

Starting point

Most will agree that also the *online* transaction process in B2C markets is about the exchange of values. Goods are delivered and payments are received. When the goods delivered are accepted and the payment is settled, it's done. While this is the essence, a whole range of communication procedures have to take place before, during and after the sale to make it work. Communication procedures such as information search, price comparison, negotiation, authentication, invoicing, scoring, authorisation, repudiation of payment, dispute resolution etc. go together with the exchange, recording and storing of data, and can be supported by information and communication technology. Integration of the different steps should lead to lower transaction costs and increased efficiency of e-commerce.

First let's ignore...

First one can try to ignore any integration problem. Do e-tailers have an integration problem? Apparently there was a problem some years ago to integrate payment functionality into online-shops and to tie up with payment processing. Obviously this problem has found a solution. Today this function is outsourced most of the time, because of complexity and costs, and because the new payment intermediaries have gained reputation. Data from the UK tell that of 10.000 e-tailers 9.950 have outsourced part or all of the payment function (the 50 companies which do everything themselves, however, are those making 90% of the turnover).

Next, there might be a special problem with digital goods: Content providers strive for digital rights management systems to shift from the “paper society” to the “pay-per society” (an expression coined by media researcher Vincent Mosco), but Digital Rights Management systems do not pose a special payment integration problem, as they will in most cases be added to subscription services, i.e. the customer registers and is thus known. When it comes to digital goods of very low value, prepaid payment instruments and (micro) billing are solutions already included in the service portfolio of Payment Service Providers (PSPs).

Do PSPs have problems? Yes, but... . Heterogeneous protocols for the communication channel, different formats and different clearing processes, varying even within one country are a major

challenge for PSP. The complexity increases with new payment systems like scratchcards, digital cash or virtual accounts – sometimes promoted by non-banks. Many technical solutions and not enough market standardisation lead to extensive investments given a low volume of traffic. These problems increase considerably for cross-border payments encountering different payment cultures. But isn't the lack of transparency and the complexity of the current situation in a certain sense the “raison d'être” of these intermediaries?

At this stage you already feel uncomfortable to simply put all blame or honour on the PSP. A closer look would be needed to better assess the issues mentioned: diversity of protocols and standards, integration of new Internet payment methods, payments for digital goods, micropayments and micro-billing, and cross-border payments. It would also be interesting to see how far outsourcing does solve all integration problem of merchants. For example it is not known to what extent PSP provide exactly the data merchants need to feed their back-office systems (e.g. ERP systems, billing systems), and this issue gets more difficult with “multi-channel-merchants”, combining e.g. call centres and WWW.

Then let's get fundamental...

To avoid the multitude of issues one can try to get more fundamental. In doing so, you'll find two crucial dimensions of the payment integration problem.

Integration of payment systems and messaging standards

Payment system integration in the transaction process is difficult, because payment systems are in a sense “black boxes” encapsulated in the communication on open networks. Each has its own procedural logic, contractual and legal basis, and each is maintained and controlled from outside.

Electronic payment systems are never only about payments. They do always go together with additional ingredients: technical security measures, legal regulations and potential law enforcement, contractual regulations of liabilities and insurance against risks, communication steps to ensure dispute resolution, steps that allow the collection of digital proofs, and communications that build trust (maybe the most efficient social mechanism to reduce complexity and transaction costs).

The Internet architectures and standardisation efforts with regard to the transaction process mostly build on XML. Payment system integration, taking the example here of IOTP (Internet Open Trading Protocol, RFC 2801), works by encapsulation. It is explicitly stated that IOTP is “payment system independent” and that it “encapsulates payment systems”. This may have advantages, as there is no interference with the procedural logic of particular payment instruments that can differ considerably, think for example how the simple distinction of “pay before”, “pay now”, “pay later” instruments changes the procedural logic. Treating them as “black boxes” may however also cause problems to relate, i.e. integrate, the “payment part” and the rest of steps in the completion phase of a transaction. In general, standard initiatives at the messaging level may have difficulties to integrate the socially complex payment systems. Looking for a metaphor, the first chapter of Saint-Exupery's “Le Petit Prince” comes to mind where one of those boas is shown who gulp their victims entirely without previous digestion. Later however the boa integrates the “foreign substances” successfully. Taking the case of IOTP it is curious to observe that despite the approach of “encapsulating”, many of its current activities are about digesting the encapsulated payment system. Take for example the IETF draft for a Payment API, or the requirements formulated for the next version 2 of IOTP, including “provisions to indicate and handle a payment protocol not tunnelled through IOTP” or the requirement to add “support for server based wallets” (see [info]).

Fundamentally there seems to be a mismatch between “payments systems” and “messaging standards” and it is an open question how to integrate them. One option would be to make these messaging standards socially more meaningful by e.g. addition of liabilities. Another option would be to extend the “payment systems” in a way that they would embrace all steps of the completion phase of a transaction.

The customers integration problem

We get another view of the integration problem, if we look at the parties involved and their local computing environment. Outsourcing was mentioned as an option for merchants. Customers are in

general not able to outsource, and face two main integration problems. First they may want to integrate data on the online-shopping process with local software already installed like homebanking software or financial management software. The second problem weighs more: As the consumer is supposed to shop at many merchants, interfaces vary a lot, passwords accumulate, shopping cart information is requested again and again, and so is financial data. E-wallets (local or server-based) are solutions discussed, and with regard to some data elements, ECML (Electronic Commerce Modelling Language) looks quite promising. At present there are however many e-wallets looking for adoption, and a common future of MS Passport and Liberty Alliance, although not to be discounted, will take some time. Another case in point are the authentication mechanisms. Cardholders of MCI and Visa credit cards would have to be prepared for both, 3D-Secure and SPA/UCAF (see ePSO-N 10&2 and 10&3]. The expected *common user experience* is, to say the least, delayed in both cases.

Or just integrate by disintegration?

Why not consider disintegration as an option? At the ePSO workshop one participant put it this way, quoting someone from Deutsche Bank “The most secure way to pay on Internet is not to pay on Internet”. There were three ways mentioned how to dissociate the purchase on the Internet and the payment: first, legally binding orders, based on digital signatures. Once the merchant has a binding order, the chance to get paid increases. Maybe it is not obvious that this is about payment integration, but in a broader view anything that supports the untroubled completion of a transaction is an integration measure – fraud prevention included. Second, special escrow services can bridge the trust gap by guarantees and risk management for consumers and merchants, and third a separate more secure channel, namely wireless mobile phones, can be added to combine Internet purchases and payment.

But disintegration is not a panacea. Legally binding orders digitally signed are proofs in court. However, in B2C e-commerce, where most transactions have relatively small value, there is often no business case to go to court. Therefore binding orders can not automatically replace a guaranteed payment. Especially in the context of online auctions escrow services are indeed offered, but in practice these services are seldom used and cause additional costs. It is revealing that another social communication mechanism was “invented”, namely mutual scoring of sellers and buyers to create trust.

Conclusion

What the “real integration problem” is depends obviously on the concept of “integration”. A broad notion would state that when everything works fine and is perceived as such, the goal of integration has been attained. This view includes all types of hard and soft, online and offline, technical and non-technical measures. A somewhat narrower view would focus on integration as the task of making unequal ends meet by linking, bridging, imbedding, encapsulating, i.e. to couple Internet technology and standards on the one side and private networks and proprietary back-office systems on the other side. The strictest concept of integration would claim that the more steps of an online transaction process are done on the Internet the higher the level of integration. E-mail money and real time accessible virtual accounts could hence be considered as more integrated than other Internet payment methods. Amazingly these concepts are not exclusive.

[info]

- Information, including extended abstracts and minutes, about the ePSO workshop "Integration of Internet payment systems into e-commerce" is available at <http://epsso.jrc.es/project/M4Agenda.html>
- A good starting point for information on the work of the IETF working group on trade (including IOTP and ECML), and for downloads of related documents is <http://www.ietf.org/html.charters/trade-charter.html>

[11&6]

The European Electronic Money Institutions Directive and the U.S. Uniform Money Services Act—Similarities and Differences

Rufus Pichler (rpichler@mofo.com), Attorney at Law, Morrison & Foerster, LLP, San Francisco, CA, USA

/EMI Directive/UMSA/electronic money/regulation/USA

The article provides a brief comparison of the main features of the European Electronic Money Institutions Directive and the United States' Uniform Money Services Act. It finds that the Act has a broader scope than the Directive and covers, e.g., non-redeemable bonus points. Unlike the Directive, the Act does not establish a "single passport" regime. Moreover, States are not required to adopt Uniform Acts at all, and they are free to amend and modify the such Acts. Thus, providing interstate money services in the U.S. may remain cumbersome even if UMSA were widely adopted.

On September 18, 2000 the European Parliament and Council adopted the Directive 2000/46/EC ("EMI Directive") and amended Directive 2000/12/EC (the "Banking Directive"). Member States must implement the EMI Directive by April 27, 2002 [cf. ePSO-N 7]. In August 2000, the National Conference of Commissioners on Uniform State Laws ("NCCUSL") approved and recommended for enactment in all States the Uniform Money Services Act ("UMSA"). To date, the UMSA has been introduced and enacted in Vermont. Other States are expected to follow (see the article by A. Ramasastry in this issue).

1. The EMI Directive in a Nutshell

The EMI Directive has three main objectives: (i) Harmonizing the Member States' laws; (ii) ensuring consumer confidence by supervision of electronic money institutions; and (iii) fostering competition in the sector of electronic money. At the core of the EMI Directive stands its definition of "electronic money" (Art. 3(b) EMI Directive) and the creation of a two-track regulatory regime between traditional credit institutions and "electronic money institutions" ("EMIs"), which are subject to a somewhat less stringent supervisory regime. Other main features of the EMI Directive include:

The country of origin principle. Under the so called "country of origin principle" (sometimes referred to as the "single passport") credit institutions only need their home Member State's authorization before commencing their activities and they are generally subject only to that Member State's supervision and control.

Redeemability. The bearer of electronic money may, at any time require the issuer to redeem it at par value.

Waiver. Member States may waive the application of the EMI and the Banking Directives to EMIs if the overall significance is negligible.

2. The EMI Directive and the UMSA Compared

The concept of federalism underlying the U.S. Constitution puts a stronger emphasis on individual States' sovereignty than is the case in most European federal countries. Therefore, in many respects the U.S. is more similar to the EU than, for example, the Federal Republic of Germany. This is also the case with respect to so called "money services businesses" ("MSBs") or "nonbank financial institutions" which have traditionally been regulated, if at all, at the State level.

Not surprisingly, the main objectives of the UMSA should sound familiar to the "EMI-Directive-savvy" reader: (i) Providing a harmonized and uniform legal framework with respect to MSBs; (ii) ensuring the safety and soundness of MSBs; and (iii) reducing barriers to competition and growth in new sectors such as emerging Internet and electronic payment mechanisms. However, one has to bear in mind that a Uniform Act operates very differently than European Directives do. While European Directives are supranational law that are binding upon, and must be implemented by, all Member States, Uniform Acts have no such binding effect. The NCCUSL is a non-governmental association, and its Uniform "laws" are but proposals that are recommended for enactment in the States. Unless adopted by a State's legislature, a Uniform Act will be of no effect in such State. States are free in their decision whether to adopt a Uniform Act at all, just as they are free to amend and modify the Act and enact such amended and modified version. Measured by its purpose – unifying and harmonizing State laws – there are successful (e.g., the Uniform Commercial Code or UCC) and less successful

examples (e.g., the Uniform Computer Information Transactions Act or UCITA) of Uniform Acts. But even State enactments of the UCC, widely held to be the most successful Uniform Act, are slightly different in certain respects. Hence, one is well advised to always refer to the relevant State's version of a Uniform Act rather than the text of the NCCUSL's proposal. To date the UMSA has been enacted only in Vermont. How many States will follow suit and what level of uniformity will actually be achieved remains to be seen.

Like the EMI Directive, the UMSA makes a distinction between traditional banks (that accept deposits or make loans) and MSBs which are not banks. Unlike under the European regulatory framework (where both are "credit institutions"), however, MSBs are not subject to banking regulations at all.

The UMSA covers persons or entities engaging in the business of money services. The relevant definitions define the scope of the UMSA, which is generally broader than the scope of the EMI Directive. "Money services" means money transmissions as well as check cashing and currency exchange. The latter two activities clearly fall outside the scope of the EMI Directive as they do not constitute the issuance of electronic money as defined in the Directive. "Money transmissions" means selling or issuing payment instruments, stored value, or receiving money or monetary value for transmission. While "payment instruments" cover traditional forms of payment not covered by the EMI Directive, the definition of "stored value" resembles the Directive's concept of "electronic money". "Stored value" means monetary value that is evidenced by an electronic record (i.e., information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form").

Thus, at the core of the UMSA stands the concept of "monetary value", defined as a medium of exchange, whether or not redeemable in money. The inclusion of value that is non-redeemable obviously differs from the EMI Directive's principle of redeemability. The UMSA was intended to cover systems such as PayPal and may also cover coupons, bonus points, gift certificates or other systems that may only be redeemed for goods and/or services. Under the Directive some of these systems would either not constitute electronic money (as they might not be issued on receipt of funds) or violate the redeemability principle.

The interpretation of "medium of exchange" is such that the value must be accepted by parties other than the issuer (open systems). This corresponds with Art. 1(3)(b)(iii) of the EMI Directive, which also excludes closed systems. The flexibility that is inherent in the UMSA's definition ("[w]ith Internet payments, the regulators will ... have to make the determination as to when a certain type of monetary value has become widely accepted as to constitute a medium of exchange") is somewhat mirrored in the EMI Directive's waiver provision, which allows for a waiver if "electronic money issued by the institution is accepted as payment only by a limited number of undertakings" (Art. 8(1)(c) EMI Directive).

Like EMIs, MSBs are subject to a license requirement (§ 201 UMSA) and a prudential supervisory regime (§ 203 – Security; § 206 – Net Worth; §§ 601 ff. – Examinations, Reports, Records; §§ 701 ff. – Permissible Investments) to safeguard funds received from consumers while the payment instrument or stored value is outstanding and to guarantee safety and soundness generally. Although the UMSA provides for a security deposit between US \$10,000 and \$250,000 (which concept is not contained in the EMI Directive), the capitalization requirement of US \$25,000 under the UMSA appears negligible (note, however, that individual States may impose higher requirements) in comparison with the EMI Directive's EUR 1 million. Note, however, that this requirement may be waived for smaller EMIs under Art. 8 of the Directive. Both instruments require the EMIs (Art. 5 EMI Directive) or MSBs (§ 701 UMSA), respectively, to maintain investments at all times at least in the amount of their outstanding liabilities arising from issued and outstanding electronic money or stored value. Further, both instruments define permissible, low-risk investments (Art. 5 EMI Directive and § 702 UMSA).

One of the most striking differences is the absence of a "State of origin principle" in the UMSA that parallels the EMI Directive's country of origin principle. MSBs in the United States (and MSBs from abroad offering services in the United States) may need to apply for a license (and its renewal, see § 205 UMSA) in, and may be subject to the supervision of, all States in which they conduct business, provided there is a sufficient jurisdictional nexus (which will more often be the case than not in the context of electronic commerce). It may come as a surprise for many Europeans that conducting interstate business within the USA may be much more cumbersome than conducting international business within the EU. Also, in this context one should remember that "Uniform" Acts may in fact

differ substantially from State to State. Nevertheless, the burden of complying with, and knowing the differences of, the laws of each State lies on each provider of electronic money or money services – unlike in the banking sector, pressure by the e-money industry to adopt a single-passport system apparently has not been strong enough to incite States to do so.

[info]

- Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions; Official Journal L 275, 27/10/2000, 39-43 http://www.europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0046.html
- Directive 2000/28/EC of the European Parliament and of the Council of 18 September 2000 amending Directive 2000/12/EC relating to the taking up and pursuit of the business of credit institutions; Official Journal L 275, 27/10/2000, 37-38 http://www.europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0028.html
- Directive 2000/12/EC of the European Parliament and of the Council of 20 March 2000 relating to the taking up and pursuit of the business of credit institutions; Official Journal L 126, 26/05/2000, 1-59 <http://www.europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0012.html>. Consolidated version at http://www.europa.eu.int/eur-lex/en/consleg/pdf/2000/en_2000L0012_do_001.pdf
- Uniform Money Services Act (Final Act, 2001) <http://www.law.upenn.edu/bll/ulc/moneyserv/UMSA2001Final.htm>. Additional information on the status of the Act can be found at <http://www.nccusl.org>

Note: Used by permission of the author, who retains copyright.

**[11&7]
E-Money Regulation in the United States**

Anita Ramasastry (arama@u.washington.edu), *University of Washington School of Law, Seattle, USA*
/UMSA/electronic money/regulation/USA

In the United States, the regulation of non-bank issuers of stored value and electronic money has been an outgrowth of existing regulatory frameworks rather than a new legislative development. State regulators have made revisions to the longstanding prudential frameworks in the non-bank financial sector. Building on existing state laws, the Uniform Money Services Act (“UMSA” or “Act”) is a new state safety and soundness law that creates licensing provisions for Money services businesses (MSBs). Among the goals of the new uniform act is the suppression of money laundering by requiring MSBs to register with state regulators and adhere to safety and soundness requirements. The UMSA also places the various forms of stored value and electronic money now emerging in the Internet economy under one law.

Prudential regulation has been left to state banking regulators

European commentators have noted that non-bank electronic money and stored value issuers and sellers have not been regulated within the United States. This view has often been formed because commentators have focused more on the federal level, where there has been an absence of prudential regulation as well as consumer protection measures for electronic money. The seeming lack of federal regulation, however, relates to the fact that there is no primary federal agency in the United States charged with supervision of non-bank providers of financial services such as money transmitters or sellers of money orders and traveler’s checks. Prudential regulation has been left to state banking regulators, who have been vested with the authority to license and regulate these industries. For some time, a majority of the 50 states have had in place regulatory statutes for non-bank providers of money services. These laws provide safety and soundness protections for consumers through prudential regulation and licensing of money services providers. It is within this legislative framework that non-bank issuers of stored value and electronic money have been placed.

Money services businesses (“MSBs”) are non-bank entities that do not accept deposits like traditional banks or financial institutions or make commercial loans. Rather, they provide alternative mechanisms for persons to make payments or to obtain currency or cash in exchange for payment instruments. MSBs engage in the following types of financial activities: money transmission (e.g., wire transfers); the sale of payment instruments (e.g., money orders, traveler's checks, and stored-value cards); check cashing; and foreign currency exchange. The so-called “core” customers of MSBs

are “unbanked” consumers or persons that do not maintain formal relationships with banks/depository institutions. State licensing, regulation and oversight of MSBs vary greatly.

In the late 1990s, several American states took the position that the transfer of money over the Internet or the use of an electronic payment instrument was the equivalent of money transmission in the brick and mortar world. In other words, Internet payment services were treated as the equivalent of money services because: (i) the business entities constituted nondepository providers of financial services and (ii) they accepted customer funds for transmission to third parties. Such Internet payment mechanisms include online bill payment services, Internet funds transfer services as well as stored-value and electronic money issuers (which can be used on line or off line). Several States have included stored value within their existing money transmission law.

The Uniform Money Services Act (UMSA)

In addition to the efforts of individual states, a new uniform law has been promulgated that provides a uniform framework for the licensing and regulation of money services throughout the 50 states. On August 3, 2000, the National Conference of Commissioners on Uniform State Laws (NCCUSL) approved the Uniform Money Services Act (“UMSA” or “Act”). It is a state safety and soundness law that connects all types of MSBs and creates licensing provisions for them. Among the goals of the new uniform act is the suppression of money laundering by requiring MSBs to register with state regulators and adhere to safety and soundness requirements. The UMSA also places the various forms of stored value and electronic money now emerging in the Internet economy under one law.

In 1994, the United States Congress enacted the Money Laundering Suppression Act. The MLSA urged States to enact uniform laws to “license and regulate” MSBs including “businesses which provide check cashing, currency exchange or money transmitting or remittance services, or issue or redeem money orders, traveler's checks and other similar instruments.” Congress specifically requested that the States develop uniform legislation under the auspices of either the NCCUSL or the American Law Institute.

NCCUSL responded to the Congressional request. In 1997, a Drafting Committee was established to prepare a uniform licensing statute for money services. In October 1999, NCCUSL commissioned a Cyberpayments Working Group to examine the issue of whether stored value, electronic money and other Internet payment mechanisms should be included within the scope of the UMSA. In March 2000, The Drafting Committee considered the recommendations of the Cyberpayments Working Group and decided that Internet-based payment mechanisms should be included within the scope of the UMSA to the extent that such services involved the sale and issuance of monetary value or the transmission of monetary value by a nonbank, if the nonbank also holds a consumer's money for its own account prior to redemption. Ultimately, the UMSA did not include new or different licensing regimes for Internet payment mechanisms, rather it applies the existing licensing frameworks to new technologies.

A nonbank entity that provides Internet funds transfer, such as PayPal, for example, would be treated the same as a company like Western Union that provides traditional non-bank funds transmission services. In the comments to the UMSA, nonbank Internet funds transfer was described as an activity that would fall within the cope of the act. PayPal, when it accepts deposits from customers, that will be ultimately transmitted to third party recipients is holding funds for consumers, thus raising safety and soundness concerns.

The Drafting Committee made the following decisions with respect to cyberpayments:

- The UMSA expands the definition of “money” to reflect the fact that certain payment service providers employ a form of value that is not directly redeemable in money, but nevertheless (1) serves as a medium of exchange and (2) places the customer at risk of the provider's insolvency while the medium is outstanding. The same safety and soundness issues pertinent to redeemable forms of value apply to these irredeemable forms of value.
- Monetary value is defined as “a medium of exchange, whether or not redeemable in money.” The term “medium of exchange” connotes that the value that is being exchanged be accepted by a community, larger than the two parties to the exchange. Hence, bilateral units of account, such as university payment cards, would not constitute “monetary value” for purposes of this Act. The

definition of monetary value, to some extent, must remain flexible to allow regulators to deal with emerging forms of monetary value and Internet “scrip” on a case-by-case basis. The term “monetary value” is defined in such a manner as to exclude pure barter or activities where the “value” that is being exchanged is used for exchange with a single issuer or merchant or within a small geographic radius.

- Under UMSA (as with existing state money transmission statutes), state regulators will also have to make the same type of determination as to when a certain type of monetary value has become widely accepted as to constitute a medium of exchange. For Internet payment systems that involve Internet scrip or points (e.g., frequent flier or bonus points), regulators will need to grapple with how widely circulating such points are, whether they are redeemable, and whether they can be used to purchase or acquire a wide range of products and services.
- In the UMSA, the definition of a stored-value removes the requirement that value is stored on an instrument, because the instrument in which the stored value is embedded is not conceptually relevant.
- Because monetary value is defined as “a medium of exchange, whether or not redeemable in money,” only stored value that consists of a medium of exchange evidenced in electronic record would qualify as stored value for purposes of regulation. A medium of exchange needs to be something that is a widely accepted. Closed-end systems, as mere bilateral units of account, therefore would be excluded from regulation.
- Internet payment services that hold customer's funds or monetary value for their own account rather than serve simply as clearing agents also fall within the definition of money transmission. By contrast, entities that simply transfer money between parties as clearing agents should clearly fall outside the scope of a safety and soundness statute. Similarly, the definition excludes entities that solely provide delivery services (e.g., courier or package delivery services) and entities that act as mere conduits for the transmission of data such as Internet service providers.

The final comments to the UMSA were promulgated in May 2001. Vermont was the first state to adopt the Act in April 2001. Several other states are meant to introduce the legislation during the 2001-002 legislative cycle. The UMSA provides a unique opportunity for States to take a consistent approach to the licensing and regulation of stored value and other forms of non-bank Internet payments. A uniform and consistent approach will provide less of a barrier to competition and growth in these new sectors. For the majority of States, the Act will provide a new approach to the treatment of stored value and electronic currency at the state level. A handful of States have begun to license and regulate such diverse entities as nonbank stored-value issuers, Internet bill payment services and Internet money transfer services. Rather than create a varied and complex regulatory system for these emerging payment service providers, the UMSA attempts to provide a simple and consistent set of licensing requirements for these new entities.

[info]

- Professor Ramasastry was the reporter and academic advisor to the Drafting Committee of the Uniform Money Service Act. Used by permission of the author
- A longer version of this article is available at <http://www.law.washington.edu/Lct/publications.html#uniform>
- Memorandum from Anita Ramasastry to Cyberpayments working Group, (January 5, 2000) located at http://www.law.upenn.edu/bll/ulc/ulc_frame.htm
- Press release concerning Uniform Money Services Act <http://www.nccusl.org/nccusl/pressreleases/pr8-3-00-4.asp>
- Table of State Money Transmitter Laws (please note this has not been updated since August 2000) <http://www.law.washington.edu/lct/publications.html#uniform>
- Final Version of Uniform Money Services Act with comments http://www.law.upenn.edu/bll/ulc/ulc_frame.htm (Select Final Acts and then Scroll down to reach Uniform Money Services Act. For earlier drafts and commentary select Draft Acts instead)

[11&8]

E-money not ECLIPsed by Regulation

Leo Van Hove (Leo.Van.Hove@vub.ac.be), Free University of Brussels, Belgium

/review/regulation/smart cards/EU

The recent ECLIP II report on smart cards collates information on the legal issues raised by the use of smartcard technology in electronic commerce, with particular reference to the potential problems to which multi-application cards may give rise. It argues that while the failure of e-money so far must be attributed primarily to commercial rather than legal barriers, there is room to improve the regulatory framework especially where consumer protection is concerned.

When I was a student in economics – *tempus fugit* – I did not particularly love the law courses that I had to take. So it was with some reluctance that I started reading the ECLIP II report on smart cards that was released in September. Fortunately, my natural apprehension proved largely unwarranted and I kept reading until the end – well, almost. ECLIP stands for Electronic Commerce Legal Issues Platform and is a research project funded by the Information Society Directorate-General of the European Commission. The ECLIP consortium is comprised of five academic research centres and one management consultancy. For the report reviewed here, the IT Law Unit of the Centre for Commercial Law Studies, Queen Mary College in London functioned as the editor and core contributor. The goal of the report – which is simply entitled “Smart Cards” – was to collate information on the legal issues raised by the use of smartcard technology in electronic commerce. The report consists of 8 papers organised in 6 chapters (not counting the introduction and the conclusion).

The paper by Sonia Gonzalo of Brussels-based consultancy Bureau van Dijk, in Chapter 2, is entitled “Business outlook on smart cards”. It discusses the advantages of smart cards and surveys the key application sectors and regions. Except for complete novices, my advice is to skip this paper as it fails to offer a vision on the future of smart cards. It simply reviews the (not so recent) technical literature and presents data on smartcard sales by sector and region. Tellingly, the list of “important players” only contains smartcard manufacturers. The paper by Simon Newman, Laura Edgar and Gavin Sutter of Queen Mary, in Chapter 3, is another introductory paper. It presents an overview of the different types of electronic payment systems. The overview is well-structured and fairly complete but it could use some updating here and there (cf. the information on Klebox, eCash and BarclayCoin).

The same three authors are also responsible for Chapter 4, the core chapter of the report that provides an overview – often from a UK perspective – of the legal issues raised by the use of electronic payment systems. Topics covered include: the transfer of personal data to countries that do not fall under the Data Protection Directive, the question of ownership of a multi-functional card, contractual relationships, etc. This chapter proved to be an interesting read, especially so because everything is set out clearly, in wording that is comprehensible for laymen. As for the content, let me stress that Newman et al. are fairly critical of the Electronic Money Directives [see also ePSO-N 7 and this issue]. For one, they argue that the requirement for issuers to maintain a certain proportion of their assets in liquid form is particularly restrictive to the profit making capacity of Electronic Money Institutions. Hence they hold that the measures “may in fact adversely affect competition and innovation”. Secondly, Newman et al. also criticise the omission of deposit-guarantee or insurance schemes as some customers will not be aware of the differences in protection offered by banks and non-banks. Other interesting sections of the Chapter are those that discuss to what extent offshore e-money issuers fall under UK laws. What was also new to me is that “with the implementation of the Distance Selling Directive a consumer will not be liable even for [the] first £50 [as is stipulated in the UK Banking Code; lvh] where his or her payment card has been fraudulently used”.

After the overview provided by Newman et al., the remaining chapters investigate selected issues in more depth. The paper by Ana Moyá Borrás of the University of the Balearic Islands focuses on the Commission Recommendation of 1997 concerning transactions by electronic payment instruments [hereinafter the Recommendation] and analyses its liability implications in the case of loss, theft or fraudulent usage of payment cards. Note that as a Recommendation it is not binding on the Member States but the Commission is currently monitoring its incorporation in national law [see info]. The Commission has stated in the past that if they found the implementation to be unsatisfactory they would propose binding legislation. The most interesting part here is the section that discusses the

burden of proof in the case of fraudulent usage of smart cards containing digital signatures and the liability of certification-service providers to third parties (including retailers).

Chapter 6 on data and consumer protection is composed of two papers by Jean-François Lerouge and one by Jean-Marc Dinant, both of the University of Namur. The first paper by Lerouge concentrates on the use of smart cards in public transport. His main point is that while the Recommendation seems to encompass reloadable single-purpose cards, in practice its scope is limited to loading operations and does not include (off-line) payment operations, so that the protection offered by the Recommendation is (too) limited. Lerouge also points out that whereas the Recommendation imposes upon e-money issuers the obligation to provide cardholders with the possibility of verifying the last five transactions and the outstanding value, the issuer is not obliged to provide a reference enabling holders to identify the transaction. Lerouge argues that in the case of road tolling, for example, it may therefore be very difficult for cardholders to verify the correctness of the amount paid especially when passing more than five toll gates. Lerouge therefore concludes that if and when the Recommendation is turned into a Directive, “it might be recommendable to apply all the provisions of the text to both functions of electronic money instruments except maybe for certain single purpose applications with a limited scope of use”. In his second paper, Lerouge deals with the question who will be liable in the case of a malfunctioning multi-application card. He points out that it appears crucial for cardholders to have only one interlocutor to deal with. His preferred solution is a scenario in which all participating companies “jointly constitute a new undertaking aimed at being considered as an 'electronic money institution' in the sense of the Directive”. This would have the added benefit of ensuring the stability and solidity of the issuers. However, Lerouge concedes that for some applications the financial protection may be disproportionate. Finally, the paper by Henning Grosse Rue of the University of Muenster, in Chapter 7, analyses intellectual property rights in smartcard technology - a topic that falls outside the scope of ePSO.

Summing up, I found the core parts of the report very interesting. It is, however, unfortunate that the Chapters are basically juxtaposed: they do not refer to nor build on each other. As a result, topics such as the Recommendation, cryptography, etc. are introduced two or three times. The Conclusion also does not really integrate the individual papers. The main message of the report seems to be that while e-money still has not achieved the mass success predicted, “this is likely to be as a result of commercial barriers rather than legal ones” – hence my title. On the other hand, the report does express concern over, for example, the lack of uniformity in the consumer protection regulations applicable to e-money issuers. It therefore suggests that after reviewing the implementation of the Recommendation “the European Commission may decide that it is necessary to introduce binding legislation in this area”.

[info]

- Newman, S. (ed.), *Smart cards – ECLIP II report*, September 2001 <http://www.eclip.org/forum/4th/reports.htm>
- Study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment instruments and in particular the relationship between holder and issuer, May 2001 http://europa.eu.int/comm/internal_market/en/finances/payment/instrument – Assesses the implementation of the Recommendation in the 15 Member States.

ePSO Newsletter – Issue 12, January 2002

Focus: Standards for Payment System Integration

[12&1]

Editorial: Elegant Standards and Everyday B2C E-Commerce

Knud Böhle (knud.bohle@jrc.es), IPTS, Seville and Simon Lelieveldt (simonl@wxs.nl), Amsterdam

/electronic commerce/standards/integration

This issue focuses on payment system integration and asks particularly for the role standards have to play. Three articles are directly related to concrete standardization efforts. IOTP, the Internet Open Trading Protocol, is dealt with in an analytical article and in an interview with Donald Eastlake, chairman of the IETF TRADE Working Group. The eWallet project established by CEN/ISSS is presented by its chairman Andrew Hinchley. Apart from this, two electronic payment systems are presented and analysed: the German micropayment system Paybest and CashCard of Singapore. In addition we include an interview with Heikki Sundquist, an insider on PKI developments in Finland, dealing among others with the FINEID card and the business case for PKI in his country. The review by Leo Van Hove of the second survey of electronic money developments, published by the Bank for International Settlements, closes this edition.

In ePSO-N 11 we started to tackle the payment integration issue by reporting about the ePSO-Workshop on this subject and trying to identify and define the problem (see [info]). In theory, the need for standardization to enable integrated and interoperable online payments in the domain of B2C e-commerce can not be denied: consumers need to go through different shopping and payment procedures on different websites, merchants wish to seamlessly integrate their e-shop and e-payment procedures with existing payment and logistic procedures, and payment service providers need to integrate heterogeneous authorisation, payment-, clearing- and settlement-protocols. But doubts were raised how important standards, developed by standardization bodies like IETF or CEN/ISSS, really are to bring about integration.

In the current issue we continue digging into the B2C e-commerce integration issue. The importance of XML-based messaging standards for payment system integration is dealt with in two contributions taking IOTP, the Internet Open Trading Protocol, as a significant example. Mike Hendry explains what the standard is about, and suggests that this standardization effort has not been extremely successful. The lack of success is however not due to short-comings of the architectural design but to practical implementation reasons, hampering its adoption in everyday B2C life. In a sense the price of the purist and generic character of a standard may be a lack of flexibility towards existing and emerging products, and new e-commerce phenomena like P2P payments. The usual strength of standards of being generic and brand independent might turn out to be a disadvantage.

In the interview with Donald Eastlake, chairman of the IETF TRADE Working Group, which takes care of IOTP, ECML and other trade relevant standards, we get further insights into standardization. Concerns about the appropriate granularity and modularity of standards like IOTP shine through. Less ambitious standards like ECML (Electronic Commerce Modeling Language) which merely standardize data fields to fill at checkout (expressed by means of XML) seem to be more successful. Donald Eastlake can imagine that just modules of the IOTP standard are taken and implemented in products.

A crucial question is what incentives there are to take the step from proposed standards to standard compliant products and their adoption. At the ePSO workshop Simon Lelieveldt argued that obviously some products and solutions regardless of CEN/ISSS or IETF standards are available in the market and being used to integrate payments. When the e-merchant asks a payment service provider to integrate e-payments in the webshop and his back office, what he requires is that his most urgent business needs are solved within a given budget and given time constraints, and that not too many changes have to be made in the back-office. He won't ask for IOTP. Payment Service Providers, in the words of Mike Hendry "tend to offer the payment methods that yield the best margin, and are less concerned about creating generic interfaces". Payment systems developers (PSP of their system) such as Paybest, which Clara Centeno analyses in this ePSO-N issue, start with a very specific solution. It is

only viable and attractive in a specific environment and for a specific customer group. They probably don't care about standards.

The contribution by Andrew Hinchley, chairman of the eWallet project established by CEN/ISSS Electronic Commerce Workshop adds further to the discussion on standards. The work started less than a year ago with e-wallets being thought of as being mainly about e-payments and with smaller companies being involved. During the course of the work heavyweights came up with their own proposals with a focus on eWallets as identity technology. This in a way will influence the standardization effort of CEN/ISSS. One is tempted to think that in the near future the heavyweights, i.e. MS Passport and Liberty Alliance, or both jointly, will set the industry standard. This would be no exception, think of the major credit card companies standardizing card payment authentication mechanisms. Later they might ask for the blessing of standards bodies – as is happening for instance with SSL proposed as the IETF standard.

The apparent difficulties typical standard setting bodies face in the ICT field should however not be exaggerated and their positive role should not be underestimated. In our view these standardization efforts are useful in many ways: they often meet the needs of smaller technology companies with less influence seeking wider market acceptance by developing common standards; standardized solutions would also help to decrease the power of the middleman specialised in dealing with the dazzling array of formats and requirements. Standardization would reduce this diversity and increase transparency. Especially small and medium sized e-tailers (SMEs) could be the beneficiaries of standards either because they could avoid lock-in situations exploited by PSP or because increased transparency would enable them to avoid out-sourcing. Further, one should not underestimate the value of public standardization efforts to structure a problem field and to present an orientation not only for developers but also for debate. If this diagnosis is not totally wrong, standardization efforts would be especially important for SMEs, as a smooth antidote against power-relations in e-commerce, and as part of a democratic culture where open and informed debate of socio-technical matters shaping the information society ranks high on the agenda.

Outside the integration focus, ePSO-N this time includes two analyses of interesting electronic payment systems. Clara Centeno has studied the business case for a new German micropayment solution called Paybest – based on information kindly provided by Jürgen Nützel, Barbi Schulz-Brünken and Rüdiger Grimm. This article contains a surprise when it comes to the status of the scheme in the light of the Electronic Money Directive. With respect to our focus theme Paybest is interesting, because it can be integrated in digital content delivery systems with a digital rights management feature. Luigi Sciusco informs about CashCard, the widely diffused e-purse in Singapore also used considerably for Internet purchases. He gives an interpretation of the system in the context of the payment culture of this particular country and compares these conditions to Europe. Information about the system was kindly provided by Mr. Quek Han Lim, Mr. Chng Kwan Koon, and Ms. Janice Khoo of NETS. Arnd Weber has interviewed Heikki Sundquist, an insider of PKI developments in Finland. The interview sheds light on the adoption of the FINEID card and analyses the business case on PKI in Finland, underlining the need for multiple cards as a success factor. Finally Leo van Hove reviews the "Survey of Electronic Money Developments" carried out by the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements (BIS). As this survey is the second of its kind by BIS and considerably enhanced he titles playfully "BIS repetita placent" – Horace, you will remember.

[info]

- Knud Böhle: Integration of Internet Payment Systems – What's the Problem? ePSO-Newsletter – No. 11– December 2001 available at <http://epso.jrc.es/newsletter/vol11/5.html>
- Information, including extended abstracts and minutes, about the ePSO workshop "Integration of Internet payment systems into e-commerce" is available at <http://epso.jrc.es/project/M4Agenda.html>

[12&2]

The Internet Open Trading Protocol: What is it and why is it needed?

Mike Hendry (mike@mikehendry.co.uk), Shepperton, England

/standard/Internet payment systems

The Internet Open Trading Protocol is an open, XML-based standard which seeks to allow website developers to develop software without knowledge of the payment methods to be used. The payment methods, and their associated brands, authentication methods etc. are provided by the payment service supplier in the form of separate modules. This paper discusses why there is a need for such a protocol, how OTP and IOTP have developed to meet this need, and some of the benefits and limitations of the approach.

Background

Internet transactions use many different forms of payment: "on account" payments, credit and debit cards, e-purses, micropayments etc. For each form of payment, there are competing suppliers.

In order to carry out the transaction, each supplier collects different data, and collects it in different ways. Often the variations are caused by their different business models, possibly including earning money from the use of the data. But more often the variations are random or are determined by aesthetic or marketing criteria.

For merchants or portals, the different interfaces required by each payment service supplier pose a problem: it is impossible to design a generic payment page to capture all the relevant information. And yet there is only a limited set of fields that can have a direct bearing on the payment function - we need "account number" but not "what magazines does your wife read?" - and these could all be encoded in XML tags.

XML was designed to handle just such structured data, but although there have been several initiatives proposing XML-based solutions (as well as IOTP we can mention ECML [Electronic Commerce Modelling Language], Visa XMLInvoice, XMLPay, ebXML, Biztalk, W3C Micropayment Initiative), none has yet achieved significant market acceptance. Some have been closed down or severely curtailed.

One of the main reasons for this is not any limitation of the technology itself, but the lack of a framework for using XML. XML requires a structured approach, whereas the Internet has grown up in an organic, deliberately unstructured way. In particular, the definition of roles is not agreed - each merchant and purchaser has its own business model. Some providers have sought to impose their solutions, but users have not found the common solutions they were seeking. In the B2B world (particularly the former EDI networks) we are closer to having such defined roles and business cases, and this is where XML is more widely used.

History

In, I think, 1998 I attended a session at a smart card conference in London at which a representative of Mondex USA presented the Open Trading Protocol (the predecessor of IOTP). It seemed an odd topic for Mondex to be promoting, but as the presentation progressed I understood its logic.

By defining the roles of the participants in a business transaction, breaking down the transaction's components and defining processes and XML tags for carrying the data, OTP would allow website developers to design pages and applications without needing to worry about the detail of the authentication or payment methods to be used - these would be handled by other more specialist applications provided by the relevant suppliers.

The Internet Open Trading Protocol grew out of OTP. The OTP consortium passed it over to a working group operating within the Internet Engineering Task Force (IETF) framework, and IOTP Version 1 was published in April 2000.

Content

The IOTP Working Group definition says: "IOTP is an interoperable framework for Internet commerce. It is optimised for the case where the buyer and the merchant do not have a prior

acquaintance and is payment system independent. It can encapsulate and support payment systems such as SET, Mondex, secure channel card payment, Geldkarte etc. " [info]

The current version of IOTP (Version 1) is published as an Internet "standard", RFC 2801 (RFC = Request for Comments). It defines the following trading roles:

- Consumer (the purchaser)
- Merchant (the vendor - or a bank in the case of a local or foreign exchange transaction)
- Payment Handler (typically the Payment Service Provider PSP)
- Delivery Handler (the delivery service or logistics company)
- Customer Care Provider (who provides dispute resolution)
- A transaction is made up of various combinations of:
 - Offer
 - Payment
 - Delivery
 - Authentication

For example, a normal purchase consists of an offer, a payment and a delivery (optional). A foreign exchange transaction includes authentication, an offer and two payments. A client "plug-in" is normally required in order to handle the session management and exchange of data between the phases of the transaction.

Already we can see that this is more flexible than a simple "A buys goods from B, which is also responsible for delivery" model, but it does not fit every common Internet purchasing scenario. For example, many players use physical agents (dealers and distributors) or logical agents (including wallets and server-based wallets). In some situations players may change roles during a transaction. Because of its origins in banks and electronic purses, IOTP version 1 focuses on the payment elements of a transaction. It includes online e-purse loading (for which there is little demand) and foreign exchange transactions, but does not consider auction payments, time-based payments or repeat transactions.

Version 2 of IOTP is designed to fill some of these gaps. It will extend the interoperable framework for Internet commerce while replacing the *ad hoc* XML messaging and digital signature part of IOTP v1 with standard XML digital signatures. Another article in this issue covers its current status and gives more detail on the Version 2 upgrades.

Most small or medium-sized e-tailers use PSPs to handle payments on their behalf, and thus do not face directly the integration problems IOTP is designed to address. The PSPs, for their part, tend to offer the payment methods that yield the best margin, and are less concerned about creating generic interfaces. This is a sub-optimal solution - neither merchants nor consumers have access to the full range of payment methods available, and there is probably a large number of missed sales as a result - but most merchants and PSPs currently see operating efficiency and customer recruitment as a bigger problem than the range of payments offered.

Status

IOTP is a truly open standard, consisting of several Internet RFCs. However, it is not widely used. Version 1 was implemented by Hitachi, Royal Bank of Canada and Brokat Technologies; version 2 is being promoted by Motorola. But no major website or e-commerce business is yet built on this technology.

Part of the problem lies in the genesis of the specification. IOPT goes into great detail on, for example, the way to ensure brands are presented correctly in a generic brand-independent environment, but the real money is chasing solutions that yield more revenue or that make the consumer experience easier.

Like many other visionary aspects of Mondex, IOTP stems from a valid insight into a significant trading issue. Developers need agreement on the roles of parties and the components of transactions. However, also like Mondex, the initial design and implementations of IOTP have put perhaps too much effort into being completely generic and brand-independent, rather than attacking directly the

areas where this capability yields immediate user benefits. They risk being seen as elegant solutions to problems that most people do not realise they face.

[info]

- Internet Open Trading Protocol (trade) Charter: <http://www.ietf.org/html.charters/trade-charter.html>
- RFC 2801: Internet Open Trading Protocol - IOTP Version 1.0 (April 2000): <http://www.faqs.org/rfcs/rfc2801.html>

[12&3]

Interview: Whether or not the Internet Open Trading Protocol (IOTP) is successful depends on the definition of success

Knud Böhle (Knud.Bohle@jrc.es), IPTS, Seville, talks to Donald E. Eastlake 3rd (Donald.Eastlake@motorola.com), chairman of the IETF TRADE working group that is developing IOTP

/E-commerce/Internet-payment systems/standards/IOTP

IOTP, the Internet Open Trading Protocol, is an XML (Extensible Markup Language) based B2C e-Commerce transaction framework. The interview with Donald Eastlake, payment system expert with long standing experience in standardization (see also [info]), is about the special features of IOTP, its current state of development and its future. Special attention is paid to the question of payment integration and authentication. Related standards under the umbrella of the IETF (Internet Engineering Task Force) TRADE working group such as ECML (Electronic Commerce Modeling Language) or 'Voucher' are also addressed.

Note on IOTP: The Internet standard (Requests for Comments: RFC 2801) defines trading roles and message exchanges between them. Roles defined are the Consumer, the Merchant, the Payment Handler, i.e. the entity that physically receives the payment from the Consumer (on behalf of the Merchant), and the Delivery Handler, the entity that physically delivers the goods or services to the Consumer (on behalf of the Merchant). Exchanges defined between these roles are related to Offer, Payment, Delivery, and Authentication. The Authentication Exchange can be used for mutual authentication between all Trading Roles. The actual shopping process can be any combination of interactions defined within IOTP. IOTP does not assume any prior relationship between the consumer and the business, and it is payment system independent.

ePSO: *Mr. Eastlake, how did you get involved in OTP, and later IOTP?*

Eastlake: I started working on OTP when I was with CyberCash, and Mondex was a primary sponsor of OTP. Already at that time when OTP was a separate consortium, I argued for *Internet* Open Trading Protocol. When control was transferred to the IETF (Internet Engineering Task Force), the acronym had to change since in the IETF 'OTP' means 'One Time Password'. So it was changed to IOTP. I continued to work on OTP/IOTP while I was with the payment architecture group in IBM. While I do other things in the IETF as well, and as people participate in the IETF as individuals and not as representatives, I continue to do some work on IOTP as chair of the IETF TRADE Working Group while being a Motorola employee. My remarks in this interview will represent my opinions only, not that of Motorola.

ePSO: *There are so many standardization efforts in the world, so what is unique about IOTP and why does B2C e-commerce on the Internet need IOTP? And let me go a step further, if the yardstick for successful standardization is its widespread use in real software products and real life, at what stage are we at present with regard to IOTP?*

Eastlake: Whether or not IOTP is successful depends on your definition of success. It is more successful than some other protocols and less than others. There has not been a lot of IOTP deployment thus far. But many merchants would like to have their payment handling (at least for some payment systems) and/or shipping and/or customer support handled by separate computers or separate organizations than the computer or organization that handled their shopping web site. IOTP is unique in standardizing the customer messages to accomplish this. While IOTP assumes no prior relationship between the customer and business, it does assume prior agreement between such parts of the merchant function. Furthermore, IOTP is independent of the payment system used.

The long-term success of IOTP is not certain. However, there has been some limited deployment. IOTP is used by InterPay (see [info]) and by Hitachi in the SMILE projects (see [info]) sponsored by the Japanese government. Earlier versions were used internally by the Royal Bank of Canada.

ePSO: *There are some points in your answer where I would like to dig a bit deeper. First, I assume that IOTP to be accepted by customers has to be convenient. What is the customer required to do to become IOTP enabled?*

Eastlake: Operation of IOTP does require code at the customer site. If the payment service is being handled by a separate service/computer, the customer will communicate with that payment service, possibly via a secure path terminating within a payment module at the customer. The choices are for the customer to communicate directly with the payment server or to communicate via a tunnel through the shopping site. Either way will require some code at the customer. For use by a browser over HTTP, a plug-in would be likely to handle the application/iotp MIME type or perhaps Java in a merchant page to support a server wallet. Since the merchant site must support and is usually the instigator of an IOTP transaction, it would be reasonable to expect such merchants to provide for downloading such code.

ePSO: *Turning to merchants, apparently many (if not most) online-merchants separate webshop and payment function and out-source these functions to web hosting services and Payment Service Providers (PSP). Especially PSP might therefore become crucial for the adoption of IOTP...*

Eastlake: IOTP can assist both server ('thin wallet') and client ('fat wallet') models of operation. But it can't be used at all unless the merchant site supports it and sets up the IOTP transaction. Support by Payment Service Providers would be nice but isn't necessary initially. The IOTP 'Payment Handler' corresponds more to a merchant cash register, not to a bank. Although, of course, a bank can certainly contract to provide cash register services for a merchant.

ePSO: *What puzzles me most is the 'payment system independence' of IOTP. Of course it is an advantage and a prerequisite for an open standard not being committed to a particular payment system. But doesn't IOTP remain totally payment system dependent in the sense that the standards bodies have always to strive for the integration of each and every Internet payment scheme? How can a working group like IETF TRADE keep track with this rapid change?*

Eastlake: The payment system independence of IOTP is not dependent on the IETF TRADE working group keeping up with every newly popular payment system. IOTP permits the customer and merchant, by mutual agreement, to tunnel arbitrary payment system dependent messages to each other wrapped in a thin IOTP wrapper. The system for registering payment system IDs is very simple and three new IOTP payment system IDs have been registered in the past couple of months: 'paybox' to paybox.net AG, 'Ezpay' to ITI Services, and 'atCredits' to @UK PLC. (<http://www.iana.org/assignments/iotp-codes>).

ePSO: *"To tunnel arbitrary payment systems" is just one method within IOTP to integrate payment systems. In the IOTP 'version 2 requirements' document (August 2001, to expire February 2002, see [info]) "provisions to indicate and handle a payment protocol not tunneled through IOTP" are foreseen. To put it more generally: What modes of payment system integration have been developed through the years or are envisaged for the future?*

Eastlake: IOTP was specified under the IETF model where protocols are primarily a definition of the bits on the wire between processes and the state of those processes. Modularization of these processes, internal divisions with the processes, and APIs are informational rather than standards track. Nevertheless, it was understood from the beginning that there exist a number of payment systems, such as SET, that have their own messages already defined and for which software is already available. So the IOTP version 1 model is that, within the Customer system and within the Merchant's Payment Handler system, 'payment bridge' software would match the existing payment system API/interface to the IOTP software so that payment messages with a thin IOTP wrapper would flow through the IOTP connection. On receipt of such a wrapped payment message, the IOTP software would take note of it, unwrap the payment message and give it to the selected payment system software. The response from the payment system software would go to the IOTP software that would

normally wrap it in an IOTP message to send to the other party. Which payment system was in use would be selected in the initial IOTP negotiation.

The interface between IOTP, this payment bridge, and the payment system is what is covered in the 'Payment API for v1.0 IOTP' (see [info]). Specific suggestions for using that interface for the particular payment system SET appear in the 'SET Supplement for the v1.0 IOTP'. Thus the general API draft builds on the IOTP protocol documents and the SET draft builds on the API draft. They are not alternatives. Someone could define a different payment bridge API, but this seems unlikely. Similarly, someone could specify how to use the API for some other existing payment scheme, such as Geldkarte. The Payment API draft also provides for the dynamic registration of new payment methods with IOTP payment bridge software. While these two drafts have technically expired, they are actually under consideration by the IETF Internet Engineering Steering Group (IESG) (see [info]), which consideration was delayed for some time due to some bureaucratic glitches. I expect them to be published eventually as Informational RFCs.

Implementation experience has indicated that wrapping the messages of existing payment systems in even a thin IOTP wrapper and sending them through IOTP components to be bridged, within the Customer and Payment Handler systems, to the payment system modules, is inefficient and inconvenient. Therefore, a possible work item for IOTP version 2 is a way in which appropriate communication protocol and rendezvous point information can be exchanged so the Customer and Payment Handler modules for the particular payment system whose use has been negotiated can exchange payment messages directly, without having to tunnel through the IOTP protocol.

ePSO: *Well, Internet standardization seems to be a continuous effort and the context is permanently changing. In this respect two other e-commerce relevant standards under the umbrella of the Trade Working Group seem especially interesting to me. The first is ECML (see [info]). It appears to be a real standard, meaning widely implemented and deployed. ECML seems to be relatively successful, because it is simple (just a set of payment related information fields in XML syntax to help automation at checkout) and because it focuses on the e-wallet. Couldn't this approach of little pieces and the e-wallet focus be extended to spread parts of IOTP such as say the 'payment receipt'?*

The second development under the umbrella of the Trade Working Group I would like you to comment on is the trading of vouchers (see [info]). Addressing vouchers like loyalty points, coupons or gift certificates shows that IOTP is reacting immediately to Internet developments like beenz or flooz (although both schemes have failed for the time being). What I find especially interesting is the fact that it addresses just one specific facet of online transactions and that it envisages a reduction of complexity in handling multiple schemes by customers and merchants - a typical function to be associated with e-wallets. Would you agree that ECML and the draft on voucher trading indicate a shift in the standardization approach in the sense of 'small is beautiful', considering the e-wallet as the kernel of e-commerce standardization? What is your opinion on the real world impact of this IETF draft?

Eastlake: Yes, ECML v1 is probably the most widely deployed technology currently in the TRADE WG. I think it was successful because there was a strongly felt need for simplification of the customer data entry experience when ECML came out, it requires few code changes at the merchant site, just changes in HTML constants, and its behavior falls back gracefully to manual entry if either the client or merchant have not implemented ECML.

I think the strategy of deploying small pieces, where possible and beneficial, is a reasonable path to e-commerce improvement. Indeed, there are pieces of IOTP that could be adopted for use within non-IOTP frameworks. A lot of thought went into the design of those IOTP pieces and I would be happy to see them benefit others.

The voucher work of the TRADE working group is intermediate in its system scope between the narrower and simpler ECML and the wider and more complex IOTP. Like all good standards, it would promote interoperability and reduce complexity. Thus far, voucher has had little real world impact, but I think it will have more impact in the future.

IOTP and related supporting documents were originally the only items on the TRADE working group agenda. First ECML and later Voucher came along and asked to be added. They were not the result of a conscious plan. There are limits to how much one working group can take on, but it is possible that additional work items will be added.

All of the work of this working group is closely related and, I hope, synergistic.

ePSO: *To conclude the interview I would like to ask you, what type of standards is really required for integrated online transactions - including payments of course. During a workshop organized by ePSO (see ePSO-N 11&5), IOTP was regarded a good starting point, but it was stated that this type of standard would not be enough. People pondered if it would be feasible to make messaging standards like IOTP socially more meaningful by e.g. addition of liabilities and by providing for authentication.*

Eastlake: IOTP demonstrated the need for standard messaging and authentication in XML. These did not exist, so IOTP had to make up its own. I believe it was one reason, among many, for the formation of the ebXML (electronic business Extensible Markup Language) group to produce a standard for business messaging and the joint IETF/W3C XML Digital Signature working group to produce a standard foundation for authentication. ETSI (European Telecommunications Standards Institute) is working on a higher level signature system based on XMLDSIG. So, the IOTP version 2 requirements make it clear that IOTP v2 is to adopt such standard message and authentication systems that others are developing and stick to the trading aspects. Signatures and authentication are optional in IOTP because it was felt that for very low value transactions in benign environments, some merchants might not want to use them. If a merchant requires some sort of authentication, the customer can choose whether or not to proceed with the transaction.

I do not know how things will ultimately evolve. But I think that IOTP, ECML, Voucher, XML Digital Signature, and XML Messaging, can all be important ingredients in a successful mix to integrate online e-commerce transactions.

ePSO: *Thank you very much for so kindly making yourself available and sharing with us your knowledge on IOTP standard matters.*

[info]

- Donald Eastlake 3rd is a Distinguished Technical Staff Member at Motorola. He previously worked at IBM in their Internet payment architecture group. Before that he was with CyberCash where he implemented their cross platform secure payment messaging library and designed their SET implementation. He is chairman of the IETF TRADE working group that is developing IOTP, co-chairman of the joint IETF/W3C XML Digital Signature Working Group and co-editor of the W3C XML Encryption draft.
- The InterPay presentation on IOTP at the fifty-first Internet Engineering Task Force Meeting, London, August 5 - 10, 2001: <http://www.ietf.org/proceedings/01aug/slides/trade-1/index.html>
- For information on SMILE (Standard SMART Card Integrated SettLEment System Project - SMILE Project -) see <http://www.ietf.org/proceedings/99jul/slides/trade-smile-99jul/index.html>
- Documents related to the IETF Working Group on Trade mentioned in this interview can be accessed via <http://www.ietf.org/html.charters/trade-charter.html>
- The IETF Internet Engineering Steering Group (IESG) website is at <http://www.ietf.org/iesg.html>; Documents under IESG Review can be found at <http://www.ietf.org/IESG/status.html>.

[12&4]

The CEN/ISSS eWallet project presents its work

Andrew Hinchley (andrew.hinchley@futuretv.com), FutureTV, chairman of the eWallet project group of CEN ISSS /standard/interoperability

CEN/ISSS Electronic Commerce Workshop initiated the eWallet project in mid-2001 assuming a need for standardization in this field. eWallets are presented as a crucial component building trust and convenience in e-commerce transactions. To achieve interoperability both common technical standards and a shared trust model seem to be requested. With respect to the dynamics of eWallet developments the shift of focus from a payment tool to an authentication/identity tool, and the recent interest of heavyweights like Microsoft in the field are of great interest. In July 2002 a CEN Workshop Agreement (CWA) will be delivered containing recommendations. ePSO-N readers are invited to comment on early versions.

Drivers for eWallet development

In general terms the WorldWideWeb remains for the time being the main driver for eWallet developments, but both mobile commerce and TV commerce should not be ignored as these areas are

expected to be larger in B2C than the web in the mid-term. In particular there are a number of different drivers which are likely to contribute to the widespread use of eWallets.

- **E-payment:** E-Wallets can generally ease payments and this is attractive to banks and major payment service providers. Additionally, any micropayment system (other than those based on holding value on a smart card), is likely to benefit from an eWallet approach as a component in delivering a micro-payment system
- **E-commerce:** The growth of e-commerce relies on making authentication, payment authorisation and billing details secure and easy to use. In some countries, concerns on security, which could be addressed by eWallets, is holding back e-commerce.
- **Identity and single sign-in (SSI):** Irrespective of the nature of any subsequent transaction, there is considerable benefit in linking the eWallet solution to authentication for web services, making personal/business information available in an appropriate way once mutual authentication has taken place.

eWallets therefore address much more than only payments. The operation of eWallets needs to provide workable solutions to a number of trust issues with identification and authentication issues being crucial. For example, whoever manages eWallet information on behalf of its owner has a duty of trust in relation to its storage and use, and most eWallets only release information to merchants when explicitly authorised by the eWallet owner.

Accordingly CEN/ISSS has chosen a flexible working definition for an eWallet that is not limited neither to the type of wallet (client, server-based), not to the channel used (web, iTV, mobile) and relatively open regarding the type of information contained: *"An eWallet is a collection of confidential data of a personal nature or relating to a role carried out by an individual, managed so as to facilitate completion of electronic transactions"*.

Rationale for an eWallet project

To date, despite the large numbers of eWallet developed, market penetration and usage has been low. A proliferation of eWallet solutions will involve personal or corporate role information being held in many different places, subject to many different conventions on how it is managed and released. For merchants, each eWallet will require unique interfacing resources, a problem particularly for the smaller merchant. For the payments industry, there is little incentive to invest in electronic payments or micropayment systems without a stronger business case that there will be consumer confidence and a stable infrastructure – including eWallets as a component – attractive to merchants. Against this background it was assumed that standardisation efforts are needed.

The CEN/ISSS eWallet Project

CEN/ISSS Electronic Commerce Workshop initiated the eWallet project in mid-2001. Key companies involved in the eWallet group include the payment processor euroConex (Bank of Ireland), a number of start-up companies in the payments area including Cyscom and NewGenPay as well as e-commerce software suppliers Commerceworks, Choreology and Intellect. Also represented are the ECBS (European Committee for Banking Standards) and the telecom operator organisation ETIS (e-and Telecommunications Information Services).

The main objective of the CEN/ISSS group in its 12 month lifetime is to develop proposals for eWallet interoperability, which given sufficient interest and momentum could then be carried forward in a European context. In the initial phase of course a lot of work of the eWallet project has been devoted to look at how eWallets have been used to date and to scope the overall area. The group has looked in detail at Microsoft Passport, the Liberty Alliance, JAVAwallet, IPIN/BT, Micropay and Payware.

The CEN/ISSS group is reviewing both harmonisation and interoperability issues. Harmonisation initiatives would relate more to business issues. Two example areas for harmonisation are eWallet content profiles and minimum levels of protection for the consumer to meet the concerns by the consumer on the management of personal information.

Regarding eWallet content profiles: Given that eWallet suppliers and services may propose different eWallet contents, understanding of what information is being used would be helped by

common profiles of eWallet contents. A further benefit of this approach is that harmonisation of eWallet contents assists in moving towards use of common registries, or exchange of information between eWallets (with eWallet owner's permission of course).

Regarding consumer protection: Minimum standards could be promoted to address:

- Management of information by the eWallet management authority
- Validation of merchant sites
- Release of information to merchants
- Authentication of the eWallet owner to authorise release of eWallet information
- Single Sign-In (SSI)

Looking back and looking forward

Since CEN/ISSS Electronic Commerce Workshop initiated its eWallet project in mid-2001 this area has been of an increasing interest to a wide audience, partly because of its relevance to web services and the single sign-in requirement often quoted as a necessary element for web services.

During this period the initial rationale for eWallets – as a critical component of e-commerce payments – has also risen in prominence as many of the small start-up eWallet solutions are replaced by more heavyweight proposals from major banks and service companies. While most eWallets to date have emerged from the payments area, more recently solutions of the heavyweights, such as Microsoft Passport, are intended as a major plank of web services products such as Microsoft's .net.

The eWallet Project will publish its final deliverables as a CEN Workshop Agreement (CWA) in July 2002. It is too early to predict recommendations at this stage, but it is clear that this area of considerable interest in Europe and the challenge as ever, is to chart a way forward indicating how and where a standards process can help meet both commercial goals and the public interest. Achieving interoperability presents much more of a challenge since both common technical standards and a shared trust model may be needed to achieve any convergence.

[info]

- All the documents produced by the eWallet group are available at the CEN/ISSS web site(ftp://ftp.cenorm.be/PUBLIC/ws-ec/Projects/ewallet/ewallet_Documents.doc).
- More information can be obtained from the Chair: Andrew Hinchley (andrew.hinchley@futuretv.com) or from the ISSS/EC Workshops Manager: Barbara Gatti (barbara.gatti@cenorm.be). The project will be publishing the first part of the CWA at the end of February and would be particularly interested in comments on this document.

[12&5]

Paybest, an emerging micropayment solution for digital goods and services

Clara Centeno (clara.centeno@jrc.es) IPTS, Seville, Spain

/micro-payment/digital goods/digital content/e-publishing/e-learning/pre-payment

Paybest is a pre-paid on-line micropayment solution developed recently by a small start-up company. At present it has been introduced in the German market at a small scale. It addresses in particular payments for spontaneous purchases of small value digital goods/services in the Internet. This article brings the micropayment problem to mind, presents the solution proposed by Paybest and assesses its strengths and potential weaknesses.

Introduction

Jupiter Research projects annual revenues for all pre-paid content categories of \$1.7 billion for 2002 and \$5.7 billion for 2005 (Content Revenue Model, Oct 2000), and estimates that the items most likely to be purchased will be, in order of importance, general content, music, on-line games, e-books and e-learning (Consumer Survey, Aug 2000). It is expected that an important part of the digital content market will be low value, and that this segment will be attractive for "unbanked" youngsters. Content industries promote a pay-per-feature model and hope to sell digital goods and services in slices. Fragmentation of content is however not only due to a strategy to increase income for businesses, it is

also due to the reduced distribution costs that internet offers. Some markets such as on-line games and e-learning seem particularly appropriate for content fragmentation as, for example, users play at increasing game levels or learn through a step-by-step approach.

This in mind, an appropriate payment method for pay-per-feature digital content should allow to pay spontaneously for small amounts and support both banked and un-banked customers, with and without credit cards. In addition, one could add generic requirements for any payment instrument to be adopted, such as user friendliness, familiarity to the consumer, wide acceptance, and acceptable costs. It is common sense that cost effective micropayment services require aggregation of transactions. Pre-payment and bill payment (micro-billing) are the two basic models where subscriptions are not viable.

Paybest, introduced in the German market by 4Friendsonly.com AG, addresses the whole range of low value digital goods/services and pays special attention to spontaneous purchases. It is based on a server-based pre-paid solution. Paybest has currently sold more than 2000 coupons, which can be used to pay the single merchant that accepts it (www.knowone.de).

Paybest can also be combined with digital content distribution systems with digital rights management features. One example is its integration with the Game Feature Platform (GFP), a pay-per-feature client-server system for games and other digital content like audio, video or multimedia content. GFP will start operations in March 2002 with the independent Game SpinOff (www.spinoff.4fo.de).

How does Paybest work and what is new about it?

Pre-payment: The buyer needs to have a billing relationship with a fixed or mobile telecommunication service provider, or have a pre-paid mobile phone card (although not all cards support it). The buyer calls a premium number and obtains a coupon number of eight characters of a fixed purchasing value of 2,50 Euro. The buyer pays a variable amount for the 2,5 Euro coupon (through the call charge) depending on the telco service provider (2,50 Euro or higher for mobile operators). The buyer is billed for this amount, at the end of the month. During the call, which can last up to 82 seconds, music is played and information is provided.

Purchasing: The buyer can immediately use his coupon number by entering it at the content provider's web site to pay for amounts of up to 2,50 Euro. When payment takes place, the value remaining on the coupon is displayed. For higher amounts, multiple coupon numbers can be used. For smaller amounts, the coupon number can be re-used until completely spent or until it expires, after 30 days.

Clearing: Paybest is credited by the telco service provider for the coupons bought to a bank account once a month, six weeks after the end of the month during which coupons were bought. Then merchants are paid from this account for the consumers' purchases, receiving money two days later. The money on the bank account provides float earning. Accounting details of valid coupons and the available amount to be spent per coupon are kept at a Paybest server, thus providing anonymity.

The business model: Of the money paid by the buyer for the purchase of a 2,5 Euro coupon (2,5 Euro or higher), Paybest receives only between 65 and 90% from the telco service provider (depending on the provider). Paybest pays merchants under two models: either 50 % of the sales value or 65% if a monthly fee of 40 Euro is paid by the merchant. The total sale is therefore split among the telco service provider (10-35%), Paybest (15-40%) and the merchant (50%). One could say that the cost of the payment instrument in this case would be around 50%. Additional income streams for Paybest will come from the non-used amounts of expired coupons and the interest generated by the float amount.

What's new or particularly interesting: Probably the most innovative feature is the way the coupons are bought via the charged telephone calls from home. This feature supports spontaneous payments. In terms of user friendliness the fact that there is no need for registration is worth mention, as well as consumers' familiarity with the Euro currency and charged calls. In addition, the anonymity provided by Paybest has to be highlighted, achieved by removing the link between the payment of a coupon and the purchase events.

Integration with the Game Feature Platform (GFP): In the GFP, content is available online from the GFP server and the client part is installed on the PC. Assuming that the basic version of the game is distributed for free, payment gets relevant when further information, or new game levels in our example, are purchased. First time visitors of the server who want to purchase content, have to enter a user name and an e-mail address. A password will be sent to this address. During this registration procedure an RSA key pair is generated. The public key is stored at the server and the private key is

stored at the user's PC, encrypted using several of the PC's installation parameters. The user can not transfer content downloaded to another person and here Digital Rights Management comes in, as all downloaded units of content are differently encrypted for each user.

The user will not pay directly with Paybest for the new content. He will 'pre-pay' on his GFP virtual account using Paybest and the GFP server will decrease this account after electronic delivery of the content. The GFP account can also be linked to a bonus point system where bonus points are increasing the account if users, for instance, stimulate purchases of other users.

In this integration example, however, Paybest would not be used for spontaneous payment, but as a means to 'pre-pay' a virtual GFP account.

Open questions and some doubts

Taking a closer look we see a number of questions arising that may influence the wider adoption of Paybest :

User friendly? Yes, but ...

... If I do not have a coupon (I am a spontaneous buyer!) and I am using an analogue dial-up line, I need to disconnect my phone line to buy it, or use my mobile phone, which is more expensive.

... If I use a telco service provider to buy a coupon which charges a fee per minute (i.e. the 0190-8-number charging 1,86 Euro per minute), I would need to stay a long time on the phone to reach the coupon value of 2,5 Euro.

... If I am an occasional shopper, and want to buy for a smaller amount than 2,50 Euro, and do not expect to come back to the site in a month's time, I will lose the remaining amount on the coupon.

Is Paybest cheap or expensive?

... Consumers will normally pay 2,5 Euro for a coupon worth 2,5 Euro. However, in some cases, Paybest consumers will have to pay more than 2,5 Euro, particularly when buying the coupon through a mobile phone. In such cases, Paybest may loose some attractiveness.

Paybest's costs for the merchant can be estimated at 50% of the goods sold, let's say 1,25 Euro for a 2,5 Euro transaction, with revenues paid 6 to 10 weeks after the goods/services have been delivered. Taking into account the fixed costs of the on-line distribution of low value digital goods (i.e., IPR, server and communication infrastructure, software, etc), would this 50% cost and late payment be affordable for merchants, or would the 50% income be an opportunity to sell goods at marginal costs that would otherwise be given for free or not distributed in this form?

Will Paybest become an Electronic Money Institution?

... Although Paybest coupons could be considered a sort of e-money, there are some elements that could, in principle, exclude them from the electronic money definition provided within the Directive 2000/46/EC on Electronic Money Institutions (EMI). The first element is that coupons are not redeemable. The second is the fact that, since Paybest is designed for spontaneous purchases, one could expect consumers to buy coupons and use them immediately or rather quickly, also due the fact that coupons expire after 30 days. One could therefore also expect that, in most of the cases, the coupons would have been spent when the telco bill is paid for at the end of the month. If this is true, Paybest would not really be a pre-paid payment instrument, from the consumer perspective. On the contrary, it would rather have the characteristics of a billing relationship, granting a line of credit. The third element is more subtle as it is related to the timing aspects of the money flow and the float amount. Consumers pay for the coupons at the end of the month and may use them during 30 days. Paybest receives payment six weeks after the end of the month during which the coupons were bought, that is 15-75 days after they have been spent, if not unused and expired. This means that when Paybest is paid by the telco service provider, it will pay the merchants for the purchases made by the consumers with all coupons purchased (if not unused). The remaining net amount, without considering commissions, will be related to the non-used and expired coupons. Therefore, in this model, one could question if Paybest would just be a money transmitter, being the telco service provider the organisation holding the float, for a fixed six weeks period, and under the Directive's potential consideration.

[info]

- Paybest, a concept initially created at Ilmenau Technical University, has been brought to the German market by a small spin-off company 4friendsOnly.com Internet Technologies AG (4fo AG) founded by Jürgen Nützel.
- Micro Payment System Paybest: <http://www.paybest.de>
- 4FriendsOnly.com AG: <http://www.4fo.de>
- Functional description of the Game Feature Platform at "Selling Games stepwise via the Internet", http://www.4fo.de/download/iic_flyer.pdf
- e-Learning project DaMiT: <http://DaMiT.dfki.de>
- Paybest is part of the Project Fairpay: <http://fairpay.dfki.de>, <http://www.dfki.de/~jantke/papers/JantkeLange-NetSiKom2002-preprint.pdf>

We would like to thank Rüdiger Grimm, Jürgen Nützel and Barbi Schulz-Brünken (Technical University of Ilmenau), for their kind contribution to the elaboration of this article.
ruediger@rgrimm.de; juergen.nuetzel@tu-ilmenau.de; barbi.brueken@tu-ilmenau.de

[12&6]

The CashCard: Lessons from Singapore

Luigi Sciusco (sciusco@tiscalinet.it), Rome, Italy – Knud Böhle (knud.bohle@jrc.es) IPTS, Seville, Spain
/electronic money/Singapore

Singapore is taking the concept of representative money to its extreme by promoting electronic legal tender. To understand the circumstances that led to this decision, this article analyses the CashCard e-money scheme and the critical success factor that could be exported to Europe.

Singapore with a population of about 4 million without doubt represents an interesting payment culture, as a BIS report on Singapore reveals (see [info]). Cash as everywhere is still the most accepted payment medium for small-value transactions. The amount of cash in circulation is however relatively high with 1,719 USD per capita. Although this ratio is lower than the one of the US and Japan, it is definitely higher than in EU countries. At the same time Singapore is a dedicated card country. All major credit cards are offered in Singapore. With almost 3 debit/credit cards per inhabitant Singapore surpasses the US, the UK and of course the rest of EU countries. The number of cards is reflected in a percentage of 38% of total volume of cashless payments made by these cards. Again, this percentage is higher than the respective share in the US, the UK and the rest of EU countries. These basic findings may explain that cash reduction would be welcome, and that new card payment products may find it easy to be accepted as payment habits are already shaped by experience with payment cards.

The CashCard e-purse is a smart card application that was launched in 1996 in Singapore by Network for Electronic Transfers (S) Pte Ltd (NETS), whose shareholders comprise local banks and a telecommunications company. The banks involved are Development Bank of Singapore, Oversea-Chinese Banking Corporation and United Overseas Bank. Singapore Telecommunications Limited was appointed as a shareholder of NETS last year. NETS supports CEPS (Common Electronic Purse Specifications) and operates beyond Singapore too. CEPS-enabled CashCards will be on trial in Singapore next year. NETS would then work with the CashCard systems in other countries (South Korea and the Philippines), where CashCard has been implemented, to enable interoperability. The CashCard is co-branded with the Visa Cash trademark when CashCard technology is exported.

CashCard in Operation

Since its launch, nearly 6 million CashCards have been issued, yielding over 100 million transactions annually via more than 22,000 usage points. When the value in the CashCard has been depleted, it can be reloaded with funds from the cardholder's bank account, via ATMs, re-loading terminals and over the Internet. The maximum value for reloading is S\$500 (about EUR 310). The consumer can get a refund via ATM/POS if he wishes to return the CashCard or if the CashCard has expired. The remaining value in the card plus the deposit value of S\$2 are credited into the consumer's bank account immediately. In the year 2000, more than S\$340 million (about EUR 210 million) worth of CashCard transactions were made. This figure comprises payments and reloads. Taking only payments into account, the figure stands at ca. 50% (S\$174 million).

The CashCard is the only means of payment for road tolls on the island. The same card is used to pay parking fees as well as for payments made in the real world and at virtual retail outlets. With the aid of a smart card reader and NETS' proprietary E-Wallet software, consumers are able to pay online for their Internet purchases at about 70 Internet merchants. 500,000 transactions per month (loading included) indicate that this payment method is in fairly common use. Nevertheless the bulk of payments, about 60% of the total CashCard transactions, comes from the Electronic Road Pricing system with the remaining 40% from retail outlets, department stores, payphones, car parks, libraries, cabs and for purchases made over the Internet. NETS has also developed a loyalty programme application – whereby card holders, who use the card for payments at participating merchant outlets, are rewarded with loyalty points – for the CashCard. Points can be redeemed for discounts and gifts. More than 8,000 transactions are made each month with loyalty points awarded to these card users.

The retailer at a retail outlet activates the CashCard POS terminal with a specific card. During logon, terminal parameters such as the transaction type allowed, CashCard keys, loyalty parameters and the black list files are downloaded onto the terminal for authentication. The retailer connects online for settlement at least once a day. The terminal parameter file contains the time parameter for automatic daily settlement and the maximum number of transactions per batch. If one of the two conditions is met, the terminal automatically initiates a connection to the CashCard Host for a settlement.

A model for Europe?

The success of the CashCard is strictly related to the peculiar cultural and geographical situation in Singapore. An e-money scheme, to be successful, should be usable in the real and, possibly, in the virtual world. The usability in the real world strongly depends on network effects and in this respect Singapore is in an ideal condition. It is an island, geographically well confined, although very open from a cultural and economical perspective, hence a framework can be defined that could not be easily implemented in bigger or more heterogeneous countries.

Some years ago the Italians tried to introduce a fully automated system to pay tolls on highways but the company that manages highways was forced to have at least one terminal for cash payments, and most people use it. Also in some European countries (e.g. Belgium, the Netherlands) it looked as if the development of e-money could be very successful, due to the restricted geographical dimension and to the open-minded attitude towards markets and innovations. In these countries public phones were thought of as "killer application", but e-money was never the exclusive payment instrument: citizens could still use other payment instruments for public phones. Besides, mobile devices rapidly rendered public phones as non-essential.

If we could define this approach as "payment democracy", probably e-money would need a "dictatorial" approach forcing people to use it. E-money would have to be the only instrument to pay for an essential service (like Electronic Road Pricing system in Singapore). This would force citizens to have e-money in their (real) wallets. In the short-medium term, citizens would have great benefits from this implementation, but it might not fit into the European payment culture (assuming that a more or less homogeneous European payment culture really exists, and this is not obvious at all). In Europe, not everybody agrees on the fact that improved efficiency is an adequate motivation to impose a payment instrument. In many countries authorities believe that market operators should be free to find the right time and solution and if they are not able to do it, probably citizens don't feel the need for e-money. Singapore acts as a laboratory for innovation in payment systems and their trial for legal tender – if it does take place – will be a great experience. Europeans can learn much about innovative technology, but my feeling is that their cultural model is very distant from the European one: it is Far, very Far, East.

[info]

- CashCard® is a registered trademark of Network for Electronic Transfers (S) Pte Ltd. See <http://www.nets.com.sg>
- Committee on Payment and Settlement Systems: Payment systems in Singapore. Prepared by the Monetary Authority of Singapore and the Committee on Payment and Settlement Systems of the central banks of the Group of Ten countries. BIS November 2001; available online at <http://www.bis.org/publ/cpss47.pdf>

Special credits to Mr Quek Han Lim, Senior Manager - Technology Projects, Mr Chng Kwan Koon, Deputy Manager - CashCard Technical, Ms Janice Khoo, Account Manager, of NETS, for time, effort and information.

[12&7]

How can PKI-services Take Off in Finland? From One ID-card to Multiple Company and Customer Cards

Arnd Weber (arnd.weber@itas.fzk.de), ITAS, Karlsruhe, Germany, talks to Heikki Sundquist (heikki.sundquist@sundcon.com), Sundcon, Espoo, Finland

/digital signatures/law/Finland

This interview highlights the business need for using different physical cards for different purposes, like signing digital business documents, making payment orders, or using loyalty points. Heikki Sundquist explains why Finnish businesses don't use the government's ID card for signing. Yet he believes that business-to-government use will be the key for creating the market for signatures.

Dr. Sundquist is a former Managing Director of Novotrust Oy, which hoped to become a major provider of company ID cards and certification services in Finland. Novotrust ceased to be an independent company, but its business is continued by one of its owner companies.

ePSO-N: *Mr. Sundquist, electronic commerce has been growing, yet we have seen little use of digital signatures for business use. Finland aims at replacing paper documents by issuing a smartcard as a national ID card, which is capable of creating digital signatures. Has the market for digital signatures taken off in Finland?*

Sundquist: Novotrust has been selling ID cards to companies, to be used as a company card, with the capability to sign documents. The cards have been approved by the Finnish government for use in transactions with the government. Novotrust has been selling these ID cards since the autumn of 1999. The card uses two key pairs, one for authentication, one for signing. If a company also wants to use the identities for official use, not only between companies, for example in taxation, then the card has to have the status of an identity card for government use. Novotrust has been listed in the official list of CA providers by the Finnish Ministry of Finance.

In the whole period, less than 1,000 cards were sold. These two years were very difficult.

ePSO-N: *Can you give us an overview of the whole Finnish market for ID cards and signatures?*

Sundquist: About 13,000 citizen cards have been issued by the Finnish Population Register Centre. 5,000-10,000 cards have been sold for Virtual Private Networks, these cards are used for authentication of a user to the network. There is a total of about 20,000 cards in Finland.

Everything that has been done in Finland up to now are trials. In the trials, we really replaced the paper documents. But it's only been trials, that's why the number of cards is so low.

ePSO-N: *One might think that Finnish companies make use of their employees having government-issued smartcards capable of digitally signing, to save the costs for issuing smartcards. Of course, companies would have to handle who is allowed to sign what. One could use so-called attribute certificates indicating whether somebody is an employee, allowed to sign, etc. Companies could outsource this handling to a certification service provider. The attribute certificates would have to be revoked when somebody leaves a company. Certification Authorities (CAs) would handle revocation, time-stamps etc. One can imagine that thus a country can run a very cheap PKI-infrastructure. Has this approach been considered in Finland?*

Sundquist: This was exactly the reasoning of the Finnish Population Register Centre two years ago. It does not work because the citizen card is possessed by the citizen. If there is a change you cannot take the card from the employee because it is a private card. But if it is a company, the card is the property of the organisation, then the person has to give the card back.

The model of attribute certificates does not work. What is important is the physical nature of the card. Digital strings don't have physical nature.

ePSO-N: *Well, one could design software in a way that a signature is only valid if an on-line revocation check has been made.*

Sundquist: If you think you can put attributes to the card and just revoke them, it doesn't work because revocation lists are not used often. That means that the card has to be taken away. That's the only way to guarantee that the person doesn't have those attributes anymore. We cannot control the

implementations, so an application needs not make a revocation check. We could make the check of revocation a rule, but a relying party may not know about our rules. And off-line usability is, of course, beneficial to the users. Therefore the only way is to issue a card.

Two years ago, we argued against the model of the Finnish Population Register Centre. Now it has been shown it doesn't work. Now even civil servants don't use their private ID cards for their employers. The revocation system is mainly for a short term protection of the card holder, as for credit cards today.

ePSO-N: *So how could the market for digital signatures in business take off in the future? Is there any interest of businesses to use digital signatures?*

Sundquist: First one must see that big companies use EDI very widely. EDI is a closed system, so companies don't need PKI-signatures. Secondly, for other B2B electronic commerce, there is little demand for signatures, because companies use faxes.

ePSO-N: *But don't Finnish managers and purchasing people still have lots of paper documents to be signed on their desks?*

Sundquist: This is true. I am just signing a contract with the European Commission. This will be sent both ways with an express courier. That costs more than the whole signature implementation would have cost.

ePSO-N: *So why are businesses not interested?*

Sundquist: Nobody wants to be the first. Only wide scale use can bring general trust in the system. The question is: Who is the first to buy a phone? You cannot call anybody. That's why we need critical mass.

ePSO-N: *Do you see any way to achieve critical mass?*

Sundquist: Yes, businesses will use smartcards for digitally signing documents in business-to-government communication. But currently nobody in Finland is buying anything because the digital signature law will be changed. In Jan. 1, 2000, a law was passed on the use of PKI for government use. Now, according to the EU Directive, there should be a new law. The deadline was July 1, 2001. Finland is late, it is a banana republic of PKI. The law will be likely be passed in Spring. The original law has to be changed. All text concerning PKI-technology had to be removed [because the Directive is relatively open regarding what an electronic signature could be, see info].

Right now I am working on founding a new company, together with some other experienced player's in the field in Finland. We have to start all over again. The delay on the market as the new law was late is one of the reasons why Novotrust could not meet its targets and had to go out of business.

The law will change the business situation. But at the moment, nobody really knows what will be the details of the law. So nobody buys anything.

ePSO-N: *Why are you optimistic that the market will change through using signatures in B2G-communication? In companies, typically only few persons sign documents to be sent to the government.*

Sundquist: What we need is a multifunctional card that can be used for three things: (1) as a company card, (2) as an official card for transactions in official use, and (3) for single sign-on to your system. Then also use in B2B can develop.

ePSO-N: *Let's imagine this has taken place. Would you then expect that an employee will sign a payment order to the bank using the company card or using a bank card?*

Sundquist: Employees who are entitled to sign something on behalf of the company, will then use their card in several occasions. Money transfer is only one type of transaction. Presently companies very often give to their employees a bank credit card. This is because banks have been effective in sensing their market position.

I think this will be different in public data networks, i.e. the Internet. Why do the banks historically have such a strong position in delivering ID credentials to people? This is because in the early days of clumsy computer systems the only thing simple enough to be digitised was money transfer. Now it is

becoming possible to transfer other commitments and items through the network than just money. Banks have realised this and are putting a lot of effort to remain in their strong position. However, their position will dramatically change as the whole society is moving from physical logistics to digital logistics.

Other players will be penetrating the market. Think for example of a debt collection company that could support its business also as a CA service provider, such as Baycorp, New Zealand. They can then issue cards for people registering their name and other details to ensure debt collection, but the cardholder name may be "Donald Duck". Now the company informs all sellers in the e-business sector that whoever buys from their web site with an identity certified by this CA can be considered as a trustworthy client and may buy on bill. In this way public e-commerce products paid by anonymous customers become possible and banks are needed only once a month for settling bills, or maybe not at all. Here the real issue is evident. It is the question of trust, in this case the trust of a seller to Donald Duck to pay his bills. If a debt collecting company guarantees it then it will be ok. Consumers will want to buy on bill, they want to have the same benefits as companies in the B2B environment, and want to get rid of bank "services".

ePSO-N: *Do you also see a chance that the consumer market for digital signatures will develop?*

Sundquist: Consumers can do electronic commerce with electronic banking. Within a second the money transaction can be made (see ePSO-N 5&3). This is the case when anonymity in the transaction is not needed.

ePSO-N: *Sometimes it is argued that the average citizen makes only few transactions with the government, which need to be signed, per year, for instance, a tax declaration. Similarly, the citizen as a bank customer may be asked to sign, but will perhaps also only sign a few documents per year. Wouldn't it make sense for banks and governments to join forces and jointly provide a public key infrastructure?*

Sundquist: The idea of our new company is that there are several areas: one is government, another one are money transactions, and then there are company cards, loyalty cards, and things like that. The idea that people have only one card in their wallet will never come true. You have your citizen card, your money card, and other cards, for example your employer's card. This is more flexible. You can change cards. Of course, citizen cards or bank cards can be used for such purposes too, but because of a market economy, it will never become true. Because you want to own your customers. You cannot own your customer if the only contact is an attribute in somebody else's card.

A single card with attributes is not attractive for a consumer or an employee, because of the physical nature of the card. Let's look at mobile phones. Mobile operators often sell their agreements with handsets. For people the handset is a very physical thing, a subscriber agreement is very difficult to sell, as a piece of paper or a SIM card. Of course, people may change, but this will take 2 or 3 generations.

ePSO-N: *What if you put IDs and bonus points, etc., in the handset, here they can easily handled, viewed, spent or be left.*

Sundquist: It is important that you can revoke your card, or your handset, if it is missing. If we think of the credit cards, they are quite seldom lost. People understand the value of their card, they keep it in a good place. They know when it is stolen. That is the same with all these cards. When they have a value, people keep them in a safe place.

If you have everything on your PC at home, and a connection to the Internet, then you have to rely on your firewall. But if you take your card out, people can rely on that if they take it out, it cannot be abused. So people rely more on physical things, which is quite understandable.

There is another thing. People are afraid that their information on networks is used and their privacy lost. If I have one card for adult entertainment services, and another for my employer's use, I know that these identities will never be revealed to each other because I have the IDs from different trusted third parties. This protects my privacy. If you have a single identity card and attributes on that, you are not sure if somebody in Pentagon collects all your information.

ePSO-N: *Thank you very much, Mr. Sundquist.*

[info]

- Baycorp, New Zealand: <http://www.baycorp.co.nz/index.asp>
- 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. Official Journal L 013 , 19/01/2000 p. 0012 – 0020. http://europa.eu.int/eur-lex/en/lif/dat/1999/en_399L0093.html.
The Directive defines an “electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”.
- Finnish Population Register Centre (Väestörekisterikeskus): <http://www.fineid.fi>

[12&8]

“Survey of Electronic Money Developments”: BIS repetita placent

Leo Van Hove (Leo.Van.Hove@vub.ac.be), Free University of Brussels, Belgium

/review/survey/electronic money/international developments/regulation/policy

In November last year, the Committee on Payment and Settlement Systems (CPSS) released an update of its May 2000 "Survey of Electronic Money Developments". The report provides information on both card-based and software-based electronic money products in no less than 82 countries, as well as on the policy responses formulated by the respective central banks. The survey itself is an improvement upon the previous one in several respects. The subject of the survey, however, seems to have made little progress.

In the very first issue of ePSO-N, that of July 2000, I reviewed the first publicly available *Survey of Electronic Money Developments* compiled by the Committee on Payment and Settlement Systems (CPSS) of the G10, and published under the auspices of the Bank for International Settlements (BIS). Back then, the Editor of ePSO-N summarised my comments by means of the phrase “impressive, but far from perfect”. In November 2001, the CPSS released an update of its survey. Compared to the May 2000 report, the current survey is an improvement in several respects.

A first improvement relates to the fact that the number of participating central banks was expanded. In all, 82 countries from around the world are now covered. The basic structure of the report has not changed. The country reports are divided into three sections. Section 1 provides a description of the current state of 'card-based products', Section 2 does the same for 'network/software-based products' and the final section describes the policy stance adopted by the various authorities concerned. Just as in the first version, there are two comparative tables at the back – one that compares system design features, and a second table containing data on actual usage in selected countries. There is, however, one novelty. In my review of the May 2000 version, I deplored the absence of comparative analysis and argued “some sort of synthesis report – drafted by the CPSS itself – painting the overall picture would have given real value added to the document”. The present version contains just that, albeit in perhaps too limited a way. The Introduction is a 5-page summary, but much of the analytical work is left to the reader. For example, no mention is made of the shake-out in the e-purse market: Chipper is dead, Mondex is not in good health, ... Also, Simon Lelieveldt has pointed out to me a case of what he calls “institutional drift”: the Eurosystem mentions technical standards as a part of its oversight role, whereas the Electronic Money Directives assign this role to the competent national authority – which is not necessarily the central bank. A positive point of the new survey is that the statistics – which relate to late 2000 or early 2001 – appear more reliable (see ePSO 1&8). This said, the lack of uniformity in the definition of the number of terminals does not seem to have been solved. Also, I would have preferred to see data on the number of active and/or activated cards rather than just the total number of cards issued, as the latter figure is not very informative.

Now what are the main developments since the release of the previous version? First, concerning card-based products, the summary states that “in a sizeable number of the countries surveyed, card-based e-money schemes ... are operating relatively successfully. [...] Card-based products are gradually gaining acceptance” (p. 2). A quick comparison of the situation at end-1999 with that at end-2000 shows that this picture is too upbeat. True, some European schemes did register fair to sizeable growth rates. For example, the number of terminals increased by 49% in Austria (Quick) and by 17% in Germany (Geldkarte). In these two countries, transaction volume also increased by 45% and 30% respectively. On the other hand, the growth rates for the Belgian Proton scheme – often considered to be the most successful so far (Van Hove, 2000) – slowed in 2000 (+9% and +5% in 2000, compared to

+41% and +35% in 1999). Also, the transaction *levels* provide a sobering note: the frequencies of use for the Austrian and German schemes, measured as the number of transactions per card per month, are a mere 0.07 (in April 2001) and 0.04 (in February 2001) respectively. [Proton scores significantly better here with a figure of 0.55 (in February 2001).] In addition, Geldkarte turnover was even somewhat lower in February 2001 compared to February 1999. It is also worth pointing out that while the Octopus scheme in Hong Kong currently registers 7 million transactions per day (or a staggering 26 transactions per card per month), only some 3% are nontransit-related – so that its usage in the retail environment is comparable to European levels. Finally, in large parts of the world – let me just mention Australia, Canada, the UK, and the US – no nation-wide roll-out of e-purses appears to be within sight.

Turning to network-based schemes, a comparison of the two reports indicates that their number is increasing. At the same time, an increasing number of card-based products have been adapted for network payment. In short, the attraction of the Internet is on the rise. Unsurprisingly, however, the survey points out that network-based schemes “remain limited in their usage, scope and application” (p. 2). And several of the schemes mentioned in the first report have all but disappeared in the meantime (Kleline, BarclayCoin, eCash). It should also be stressed that the definition of e-money used in this part of the report is a broad one: schemes that rely on one-time-use credit card numbers are also included. Token-based schemes *à la* eCash do not seem to be *en vogue*; the newly mentioned schemes are mainly prepaid accounts (loaded from credit cards or scratch cards).

Finally, where Section 3 on policy issues is concerned, it is worth noting that so far no central bank has indicated an adverse impact on the size of its balance sheet. All central banks therefore are confident that they will be able to retain the reins of monetary policy. The Section also documents the way in which EU central banks envisage making changes to existing legislation to bring it in line with the two E-Money Directives. The overview also makes clear that many other central banks around the world are adopting a ‘banks only’ approach when it comes to e-money issuance. Interestingly, central banks also seem to have been asked whether they envisage issuing electronic money themselves. All 15 central banks that mention it state that they have no intention of doing so. However, 10 out of these 15 qualify their statement in order to keep the option open for the future. Most do this by including terms such as “at present”, “for now”, etc. Others do it more explicitly. The Bank of Greece, for example, states that its stance “will depend upon the long-term effects of e-money on seigniorage revenues” (p. 36-37). The five central banks that do not qualify their position are those of Latvia, Mexico, the Netherlands, Sweden, and Thailand.

In conclusion, e-money seems to have been making little progress since the previous CPSS survey. At least where the euro-zone is concerned, e-purse operators are hoping that this will change in 2002. Indeed, the change-over to the euro improves the competitive position of e-purses. For one, the number of euro denominations – 15 in total – is significantly higher than for most disappearing national currencies. This makes it harder for the public to recognise the different coins and notes, and to find the specific denominations needed to make more or less efficient payments (in order to avoid getting to many coins back). Also, in Belgium the largest euro coin has a significantly higher nominal value (2 euro) than the largest BEF coin (1.24 euro) and will in effect replace to a large extent the much-used BEF 100 banknote (2.18 euro). As a result, Belgians will have to get used to carrying around a far heavier and bulkier traditional purse – or will have to start using its electronic equivalent. The next CPSS survey thus promises to be a crucial one. If European e-purses cannot make a definitive breakthrough now, then when?

[info]

- **Card Technology**, Octopus cards failing to deliver expected retail sales, *Card Technology News Bulletin*, January 18, 2002 <http://www.ct-ctst.com>.
- **Committee on Payment and Settlement Systems (CPSS)**, *Survey of Electronic Money Developments*, Bank for International Settlements, Basel, Switzerland, November 2001 <http://www.bis.org/publ/cpss48.htm>.
- **Van Hove, L.**, Electronic purses: (which) way to go?, *First Monday*, Vol. 5, No. 7, July 2000 http://www.firstmonday.org/issues/issue5_7/hove/index.html.

With thanks to Knud Böhle, Simon Lelieveldt, Michael Walters, and Arnd Weber for comments on a draft version.

ePSO Newsletter – Issue 13, April 2002

Focus: ePayments in Transport

[13&1]

Editorial: ePayments in Transport – High Speed Systems or Customer Monitoring?

Arnd Weber (arnd.weber@itas.fzk.de), ITAS, Karlsruhe, Germany

/public transport/contactless smartcard/telematics/positioning

This issue focuses on payments in transport. Contactless payment systems are emerging in European public transport, in particular in cities where stations have gates. Transport operators also plan to use contactless cards in gateless systems. In these systems, an issue is whether checking-in and out will be accepted by the users. Another issue is whether inter-operability between systems will become available for the European citizen. Physical gates could be avoided by using technologies for monitoring customers over a distance. Such technologies can not only be used in public transport, but also for road pricing. Future cars may be on-line for "buying" services anyway. Distant monitoring reduces speed requirements for systems, but raises privacy issues. Other articles in this issue address third party billing, smartcard security, and the ePSO-conference on consumer online payments.

Convenience, Speed and Inter-operability

Public transport is currently introducing contactless fare collection systems. Thanks to built-in payment mechanisms, customers need no longer worry about the proper ticket, and charges can even be automatically "capped" so as not to exceed the equivalent of a day or season ticket. Road toll systems are increasingly being introduced all over Europe, to pay for roads or to reduce congestion and pollution. For electronic payments in transport a high transaction speed is desirable. Gates of public transport systems should let people through at walking speed, which leaves about 300 ms to finalise a transaction. Motorway gates should even work if a car passes at 200 km per hour or more. Given trans-border traffic in Europe, it makes sense to think about whether such systems should also work across borders, for the sake of convenience and to achieve economies of scale.

Contactless Systems

In ePSO-N [5&6] we analysed some of the critical conditions for the functioning of the Hong Kong Octopus public transport system, such as lack of convenient transport alternatives, and lack of season tickets. In several countries large local transport operators are aiming to repeat the Hong Kong success. Operators of systems using gates plan to convert towards using contactless cards. For example Transport for London and partners have started the Prestige project. They have already ordered 4 million smartcards and plan to launch the system in August 2002. Partners are Cubic, Schlumberger and others (Card Technology). Paris RATP has already equipped more than 1,000 fare gates to accept contactless chip cards, and intends to replace all annual passes with chip cards during this year. Here, the partners are Schlumberger and ASK. Later, RATP plans to use disposable chip cards for single rides.

Even in countries in which season tickets play a significant role, such as Germany, operators aim at repeating the success of Hong Kong. But will holders of season tickets check-in or even out every time they enter a train or bus? This question is raised in my article on the ERG-Proton deal. ERG was the principal contractor for the Octopus system. In today's European public transport, no inter-operable systems exist. Will the ERG-Proton deal change this situation?

Gateless Systems

Gates in public transport stations and in road-pricing have in common that some electronic communication takes place to trigger the payment, and some physical control is exercised, for instance through a barrier which closes if no payment is made, or through a video camera which takes pictures of the number plate if the owner doesn't pay. Instead of building even more gates at rail and bus

stations, or on roads, wouldn't it be easier to permanently monitor individuals or cars and have them pay when moving?

That principle becomes visible in public transport, e.g. in the Easyride project, which is being supported by many Swiss public transport operators. In their trial, a smartcard with battery and radio interface has been used to communicate with on-board units and their antennas in carriages. On the one hand, this approach has clear advantages:

- Customers can simply walk in and out, without a ticket.
- No physical gates need to be built.
- It is impossible to forget to check out.
- On the other hand, a number of issues emerged (see [info] on Electroline), such as:
- Lack of control of costs by the users.
- Customers need to be credit-worthy, or have to deposit funds in the first place.
- Battery power in the cards is needed for radio communication.
- Privacy.

There are ongoing attempts at moving in the direction of fare collection while walking in or out of trains and buses in Germany (Intermobil), while the Easyride partners are also developing an electronic equivalent of the paper ticket, to be put onto a smartcard (Easyticket).

GPS in Cars

Systems without physical gates are also emerging in road user charging, as can be seen in the article by Ian Catling and David Crawford. They propose to have GPS systems in cars and have the car trigger a payment when moving on a toll road. While today the road-pricing systems in EU member states are all incompatible, using GPS and radio communication could become a technical standard to make borderless fee collection possible. Payment would no longer be time-critical, therefore customers could in principle use their preferred payment instrument. Recently, Transport for London published the results of a study which suggests that all UK cars could be equipped with a link to a satellite navigation system for paying for roads and city access. The mayor of London, Ken Livingstone, reportedly is expected to announce that a pilot scheme will go ahead in the British capital next spring (SCN Daily News).

Talking Cars

You think it will take a long time until cars can communicate all the time? Well, maybe, but see Erik Dahlström's article about automotive telematics discussing how many things a car driver may wish to buy in the future using the car's wireless connection.

Beyond the focus theme, we first have an article by Thorsten Wichmann who discusses what third party billing means when using a phone to pay for different goods and services with different means of payment. Thereafter, Laurent Beslay discusses how smartcard systems can even be attacked by non-specialists using publicly available knowledge and tools. His example is the "Yescard" which emulates French CB-cards. Subsequently, Luigi Sciusco discusses the Security Guidelines which the Monetary Authority of Singapore recently put on the Web. Finally, Leo van Hove this time does not review a publication, but the ePSO conference on consumer payments.

[info]

- Card Technology: London Orders 4 Million Transit Smart Cards. January 2002. <http://www.ct-ctst.com/CT>
- Card Technology: Paris Transit Operator Begins Smart Card Rollout. October 2001. <http://www.ct-ctst.com/CT>
- Easyride: Swiss Project by the Public Transport Association, the Swiss Federal Railways (SBB AG), the Postal Vehicle Service and the Federal Department of Transport. Cf. <http://www.easyride.ch> (<http://s26282.sbb.ch:80/easyride/e/index.htm>)
- Electroline: All Aboard - So Long As You Have a Card. http://www.electroline.com.au/elc/feature_story/102001.asp
- Interomobil (in German): <http://www.intermobil-dresden.de>
- SCN Daily News, 25 February 2002: Smart Cards To Be Used in UK GPS Transport System
- Transport for London: The Prestige Project. Progress report February 2001. http://www.londontransport.co.uk/abt_prest_rep.shtml/

[13&2]

Payment Solutions for Automotive Telematics

Erik Dahlström (erik.dahlstrom@ausys.se), AU-System AB, Gothenburg, Sweden

/mobile services/telematics/pay-on-demand/positioning

Automotive telematics is an emerging and growing market. Advanced payment solutions will be required once the telematics infrastructure is in place in vehicles. The payment model likely to fit telematics-based services in cars is a pay-on-demand model. Once established, the GPRS and 3G infrastructure allows the provision of more data to and from cars, many new opportunities appear for vehicle manufacturers, mobile operators and service providers.

Introduction to Automotive Telematics

One increasingly greater area of attention within telecommunications and the automotive industry is automotive telematics. Automotive telematics is about providing mobile services to cars. A suitable definition of automotive telematics is presented by Telematics Valley, a Swedish telematics industry organisation:

"Telematics refers to any kind of vehicle service intended to promote safety, productivity, mobility and convenience, which relies on a wireless communication link and often includes a positioning system."

Telematics-based services range from accident notifications to ordering music to the car. In short, a division can be made primarily between two types of services:

- Services of more general character such as communication services (telephony, e-mail, chat, Internet access), infotainment services and mobile commerce. These services are "generally available" and provided to many different devices where the car is just another access platform.
- Specific services related to the ownership and driving of a car such as route guidance, vehicle diagnostics, road toll payments and airbag deployment notification. These services are unique for the car environment and more closely linked to the vehicle manufacturer and the vehicle itself.
- Some of the most common telematics-based services today include:
 - Emergency notifications – when the airbag inflates, an SMS with the position of the car is sent to an emergency call centre. Simultaneously, a voice call is initiated from the car.
 - Dynamic traffic information – based on the car position, traffic information is sent to the car enabling the driver to reroute from accidents, roadwork and congestions.
 - Points-of-Information (POI). Again, based on the current position of the car the nearest restaurant, hotel or gas station can be found. Directions could be sent to the car either through a call centre or as text.
 - Information and concierge services – drivers are able to get information, make reservations and bookings.

Here in Europe, BMW, Mercedes, Audi, Fiat, Citroen, Volvo, and Ford to name a few brands, offer services based on GSM infrastructure. Most schemes run with a business model where customers pay a fixed annual or monthly fee for unlimited usage of the telematics-based services. Added to that come telephony costs. The reason that these business models have emerged is partly that vehicle manufacturers are used to the charging models for products, rather than services, and partly that there are no off-the-shelf payment solutions available. At present, it is a problem for telematics service providers to provide advanced payment options.

Outlook

Whether the world will enjoy a vast flora of in-car services in the coming years or not remains to be seen. It is however likely that the telematics marketplace will evolve in parallel with the telecom industry.

The potential of automotive telematics is promising. In just a few years time, the majority of new cars will have integrated telephony, enabling the vehicle manufacturer, mobile operators and other service providers to provide customers with services as they drive their car.

Equipping the car with an integrated phone is the main pre-requisite for telematics. European drivers spend over two hours on average in the car every day. According to some telecom industry analysts, more than half of all mobile calls are made from cars. Here is another interesting fact: The profit made on telephony in the car exceeds the profit vehicle manufacturers make on new-car sales, parts, service and accessories combined. For the vehicle manufacturer, the profit margin on new-car sales is about 4-6%. For mobile operators the profit margin ranges from 25-50%.

Even though most vehicle manufacturers feel it is out of the range of their core business to make money on telephony, they are eager to realise the potentials of surrounding services enabled by equipping the car with a mobile phone, a GPS and a navigation system in the car.

When considering automotive telematics from an "electronic payments point-of-view" some observations can be made. The growing possibilities of telematics-based services will put increasingly higher requirements on how drivers pay for these services. The 3G-development will have major effect on telematics-based services. In the automotive industry however, this development is not referred to as 3G, but as *off-board*. 3G will namely enable the delivery of both content and applications to the car. Hence, drivers can seamlessly download information such as e-mail, news and music to the car. They can also purchase new applications they feel they need in the car. This is the concept of off-board services.

So how does this affect payment systems? Take conventional, on-board navigation as an example: Today, drivers spend about €1,000 on a CD with maps of Europe. Once every second month the CD needs to be updated and the old one thrown away. With an off-board (3G) infrastructure drivers only need to download those maps of relevance for a specific trip. A suitable payment model for such a service would be to pay-on-demand!

Pay-on-demand – payment model for telematics-based services

Even though not all telematics-based services will be chargeable, some services of the future will require a *pay-on-demand* model: pay-per-use for applications and pay-per-view for content.

There are several benefits with pay-on-demand payment models. First, on most emerging markets new innovations are pushed onto the market often requiring a change in behaviour of the users. This is certainly the case for in-vehicle services. The business or pricing model of new services not created from a user-driven demand is more likely to succeed as a pay-on-demand model. Drivers unable to directly see the benefits of a new service are more likely to accept it if they are charged only if they themselves decide at some point that the need is there.

Second, to enable a pay-on-demand model, the "payment provider" (which could be the vehicle manufacturer, a mobile operator or a telematics service provider) needs specific information on service usage (unlike pay once, use freely). When more advanced payment methods such as pay-on-demand gain ground, the *service of payment* itself will receive increasingly more attention. It becomes more than ever the key component of the customer relationship. The keeper of what is usually referred to as the *point-of-billing* becomes the keeper of the customer information and is consequently best positioned to profit from the customer relationship.

Third, pay-on-demand payments within the automotive world will interestingly enough give birth to many new services. One example is *dynamic road tolls*, a good example of how the access to more detailed information, such as type of driver (private; commercial), type of vehicle (weight; environmental class), vehicle position (expensive street; cheaper tunnel) and number of passengers, will enable new types of payment service models. Dynamic road tolls will enable operators to charge dynamically based on a number of parameters. Or better, the driver *pays exactly for what he uses, exactly when he uses it*. Another good example of a new service based on new payment technology is *Pay-as-you-drive insurance*. Car owners pay their premiums based on how much they actually drive, a model favoured by many insurance companies.

In conclusion, these are the reasons why clever payment solutions play a pivotal role in a telematics service offering:

- They are needed when more advanced services arrive.

- They are needed so that a multi-market provision of services is possible.
- They are needed for competitive reasons, enabling the vehicle manufacturer to maintain control of billing and the customer relationship.
- The right payment model is required to attract new customers on this emerging market, and not to scare them away.
- To a greater extent the service of payment itself will become a differentiator.

[info]

- BMW: http://www.bmw.de/de/produkte/index_telematik.html
- Mercedes: <http://www.mercedes-benz.de/mbd/t46/0,1506,C21SD,00.html>
- Audi: http://www.audi.com/de/de/kundenservice/audi_telematics/produktbeschreibung/produktbeschreibung.jsp
- WirelessCar: <http://www.wirelesscar.com>

[13&3]

New Technology for Mobile Electronic Fee Collection

Ian Catling (ic@catling.com), David Crawford (itseditor@ropl.com), Ian Catling Consultancy, Chipstead, United Kingdom

/Intelligent Transport Systems/Vehicle Positioning Systems

Proposed Electronic Fee Collection schemes now have the option of Vehicle Positioning Systems (VPS) as well as of Dedicated Short-Range Communication (DSRC) as a technical base. VPS transactions are not time-critical and so offer greater flexibility, as well as scope for value-added services using a mobile communication link. VPS can thus operate with any payment means. Switzerland has introduced a system that uses GPS for her heavy goods vehicle charging system, and other European countries are moving towards VPS implementations, e.g. the Netherlands. The EU INITIATIVE project will assess both VPS and DSRC systems.

Electronic Fee Collection (EFC) is an important application of Intelligent Transport Systems (ITS) and provides the capability for Electronic Toll Collection and Road User Charging, both of which are increasingly used around the world.

Until recently, most technical approaches to EFC have been based on Dedicated Short-Range Communication (DSRC) between in-vehicle units and roadside equipment. An alternative that is fast gaining credibility and interest, under the generic heading of Vehicle Positioning Systems (VPS), uses in-vehicle locational capability and replaces infrastructural support with "virtual gantries". The basic technology dates from the early 1990s.

While it is possible with both types of system to accept payment by a range of methods, including smartcards and pre- or post-payment via a central accounting system, there have in the past been problems with some smartcards in DSRC trials. This is because of the real-time nature of the DSRC transaction which must be capable of completion as a vehicle passes a roadside installation, potentially at high speed. Because of the time taken to communicate with a smartcard which might have been designed for non-time-critical usage, such as an ATM machine, it is often not possible to complete authentication routines. VPS transactions are not time-critical and so can operate with *any* payment means.

With VPS, the in-vehicle unit locates itself within the charging area – typically using GPS, although future systems could use UMTS or 3G mobile telephony. It also stores charging structures and determine when these should be applied.

When a charge is generated, it can either be deducted directly from a smartcard inserted into the in-vehicle unit, or stored for later transmission and debiting to a back office.

VPS can also include a mobile communication link, offering such benefits as:

- Automatic updating of stored charging data, e.g. to introduce incentives for off-peak use;
- Transmission of digital "certificates" to enforcement systems;
- Continuous system diagnostics; and
- A continuous communication medium for integration with other ITS applications and services -

to give "value-added" attractions to motorists.

As with virtually all EFC systems, enforcement is based on capturing images of violating vehicles. Since VPS does not have fixed roadside charge points, the successful approach developed in the recent Hong Kong trials involved a small number of fixed enforcement sites, typically at points of high traffic flow, supported by mobile sites for random enforcement.

A well-trodden route

VPS dates from EU-funded projects in the early 1990s. In 1995 the German motorway tolling trials included two VPS systems. The following year, the ISO/CEN standardisation committee on road transport telematics set up a sub-group to propose standards for such systems.

In 1997 the Hong Kong Government initiated a "Feasibility Study on Electronic Road Pricing" which included field evaluation of DSRC-based and VPS-based options. The study concluded that VPS technology offers the best-balanced choice for electronic road pricing in the longer term.

In 1998, the European Commission issued a communication on interoperable EFC systems, including recommendations for actions on interoperability. This recognised both the technological approaches.

In January 2001 Switzerland introduced a system for charging heavy goods vehicles for road usage, based on distance travelled. This includes a GPS-based positioning system, which has a number of functions. It provides internal monitoring of distance readings; ensures that vehicles' on-board units (OBUs) keep exact time; double checks whether vehicles are inside or outside Switzerland; and records border crossings by vehicles being transported by rail.

In mid-2001, the UK Government contracted the Fareway consortium to implement its €30m DIRECTS project, with on-street trials in Leeds planned during 2002. Although the main focus is on DSRC, it is planned also to demonstrate VPS.

In his pre-budget statement in November 2001, the British Chancellor announced the Government's intention to introduce distance-based charging for lorries. The technological approach has yet to be determined but VPS is a strong contender. The likelihood of it eventually being adopted has been increased by the recent publication, by the Government-established Commission for Integrated Transport (CfIT) of a nationwide proposal very similar to the current Dutch initiative (see below).

After several years of follow-up work from its 1995 trials, the German Government is planning a charging system for heavy goods vehicles (HGVs) to be operational on the national autobahn network during 2003. At the time of writing, two consortia – AGES and Toll Collect – are in the final stages of bidding and both teams are understood to have based their bids on VPS approaches. The anticipated attractiveness of VPS reflects the high cost of DSRC infrastructure.

Meanwhile, the Austrian Government announced its revised programme for heavy goods vehicles charging in 2001. The new programme follows the German model in specifying functionality rather than technology, and implementation is scheduled during 2003.

The current focus of attention is the Netherlands, where the Government has undergone a major policy shift, after years of trialling DSRC for its heavily-congested Randstad conurbation. It has now opted for the use of VPS in its "Mobimeter" kilometre-levy scheme for charging all vehicles on all roads – the most ambitious initiative in the world to date. At an open meeting on 20 March 2002 to initiate a "market dialogue" with potential suppliers of the eight million OBUs that would need to be installed by 2006, Transport Minister Tineke Netelenbos envisaged the Netherlands laying down a marker for the rest of Europe, if not the wider world.

The prospects are, therefore, that Germany, Austria and the Netherlands could all introduce VPS-based charging systems for heavy goods vehicles during the next few years to replace the current paper-based Eurovignette system, with a similar system operational in the UK.

Two European cities, Copenhagen (Denmark) and Gothenburg (Sweden) are implementing VPS trials under the European PRoGRESS project, which started in May 2000. These are behavioural trials led by the city authorities to investigate the potential for urban charging schemes. Finally, the first European city outside Norway to introduce urban Road User Charging is likely to be London, where a licence-based system is scheduled to be operational during 2003. VPS could prove the most acceptable means of achieving an eventual upgrade to EFC.

INITIATIVE

INITIATIVE (INdustry Initiative To Introduce Automatic Tolling In Vehicles in Europe) is an EU-funded research project aimed at validating aspects of interoperability between EFC systems based on both DSRC and VPS. It recognises that, although DSRC might be seen as nearing maturity for Road User Charging applications, the "virtual gantry" might offer a more attractive alternative in the medium term. The main players are three equipment suppliers – Q-Free, Vodafone and Fela – who will demonstrate DSRC and GNSS/CN (Global Navigation Satellite System with Cellular Networks) systems.

The main issue being validated is the use of common, integrated on-board equipment including a dual interface. Test sites are being implemented in Germany, Switzerland and the UK in Summer 2002.

Pros and cons

A main attraction of VPS is that it does not need roadside infrastructure at charge points – a major bonus for urban environments, especially historic ones. This makes it easy and inexpensive to redefine charging areas, to reflect changes in road networks or land use. The main disadvantage is the higher cost of the in-vehicle units. Even as component costs fall this is likely to continue, although full system costs may be comparable with those of DSRC-based installations with their extensive infrastructures.

VPS offers scope for integrating a range of ITS applications in a single in-vehicle platform. As the demand for integration increases, driven by innovative transport policies based on road user charging, VPS is likely to become the accepted approach to EFC for the 21st century.

Current developments in Australia, Austria, Germany and New Zealand all focus on charges for heavy vehicles, and these could encourage early availability of low-cost VPS units – making it more attractive to apply to all vehicles.

A key consideration will be comparability of overall system costs with DSRC, coupled with the ability of VPS to respect the environment, reflect changing traffic patterns cost-effectively, and offer drivers incentives – so keeping fees low and balancing them with benefits.

[info]

- Ian Catling Consultancy: <http://www.catling.com>
- INITIATIVE project: http://www.cordis.lu/telematics/tap_transport/research/projects/initiative.html
- PRoGRESS: <http://www.progress-project.org>

[13&4]

ERG Buys Proton

Arnd Weber (arnd.weber@itas.fzk.de), ITAS, Karlsruhe, Germany

/electronic purse/public transport/contactless smartcard

The Australian ERG Group, which provides automated fare collection systems for public transport systems (e.g. Hong Kong Octopus), has acquired Belgium's Proton World, traditionally renowned for its electronic purse and more recently for its Global Platform-based smart card components. This article reviews some of the plans ERG has with its partners in the transport, telecommunications and banking industries, and asks what this acquisition means for inter-operable payment and transport applications in Europe.

ERG's main business is to build, own or operate card-based, automated fare collection systems for public transport system world-wide. In ePSO-N 5&6 we reported on Hong Kong's contactless smart card based Octopus fare collection system, which appears to be one of the few broadly successful electronic purse schemes operational today. The ERG Group was the primary contractor to the Hong Kong operators. As we wrote, the closed nature of the Hong Kong public transport systems, using gates, the lack of alternative means of payments, and the inconvenience of alternative means of transport (traffic congestion, etc.), lead to high acceptance by commuters, and thus also high transaction numbers. Thus, the operators achieve significant cost reductions compared to cash.

Some telling ERG activities in Europe

In Europe, similar success stories involving electronic purses are rare. In October 2001, ERG bought out Banksys, InterPay, Visa and AmEx to acquire loss-making Proton World, known for their purse, EMV and PKI solutions, as well as their Global Platform based Prisma cards. One immediately wonders whether ERG and their customers and partners will aim at repeating the success from Hong Kong elsewhere, using Proton technology.

In 1999, ERG had already bought rights to the Proton technology for the United Kingdom, Italy and other countries. In the UK, they founded Prepayment Cards Limited (PCL), together with major transport operators including Stagecoach, FirstGroup and National Express. PCL will provide a smart card issuing and ticket clearing system. Their partners aim at offering an integrated system, allowing for use of the same ticket for journeys throughout the country. The UK Post Office will provide a card issuing and recharging service for Prepayment Cards. The cards are already in use in South Wales (South Wales Integrated Fast Transit - SWIFT), but the first major test of the new system will be in Manchester where 650,000 cards are to be issued during 2002. A National Express spokesman said: "We will be able to see where and how people travel at what times. It will be a bit like a supermarket club card, which tells the supermarkets what sort of people are buying each product" (cf. Murray-West 2000).

ERG is also active in Germany. In public transport in Berlin and the state of Brandenburg the "tick.et" trial took place in which a card was loaded with value and then the fare was deducted depending on the distance travelled (with the help of check-in and check-out terminals). Users were offered small smart card readers to check their balance ("tick.et checks"). The intention is to rollout such a system in the Berlin/Brandenburg area, with the involvement of Deutsche Bahn. ERG also partners with Card.etc, with the support of VDV (Verband Deutscher Verkehrsbetriebe), the Association of German Transport Companies. Card.etc will use PayCard technology, which was formerly owned by Deutsche Telekom. Card.etc announced that two regional transport operators, Verkehrsverbund Rhein-Ruhr and the one from the Rhein-Sieg area, would deploy 1.6 million smart cards. As season tickets, their area and time range of validity will be printed onto them. The cards will contain a purse, which can be reloaded at Deutsche Telekom phone booths. They will have a dual interface (contact and contactless). Card.etc has applied for a bank license.

ERG is also active in Rome, where stations, buses and trams are already being equipped, and cards are being issued, as well as in Gothenburg and elsewhere outside Europe.

Making sense of the Proton deal

With the acquisition of Proton World, ERG intends to acquire more expertise in financial areas. They say: "The acquisition positions ERG as a "one stop shop" for all smart card systems and application requirements for the combined groups' collective customers. The transaction significantly expands our customer base throughout the banking and financial services sectors and gives us access to the fast growing security and identity markets. We welcome more than 500 banking customers that have deployed the Proton technology to add to our world-wide transit client base." Their objectives also become visible in ERG's plans to continue the Proton business with American Express, Banksys and InterPay Nederland, each of whom have service contracts with Proton.

In this context it should be noted that ERG, in their home country, partners with the telecommunication carrier Telstra and with ANZ Bank in the "Ecard" venture for processing multi-application smart card transactions.

As an observer, I wonder about two things:

1. Will the transition to regular check-ins and check-outs be accepted by customers?

In several schemes in which the contactless cards are to be deployed, there are no barriers today. Requesting customers to check in, or even to check out, may have several advantages: "Slippage", i.e. the user not paying, can be reduced. Prices can precisely reflect the distance travelled. Even "best-price" fares can be offered, meaning that a customer paying for single trips will not pay more than a season ticket would have cost. However, it may be difficult to teach customers to change rules. In the "get-in" trial by Rhein-Main Verkehrsverbund, operating in the area of Frankfurt, Germany, the

problem will be addressed by encouraging the use of the new check-in and –out terminals by providing bonus-points. Here it is envisaged that people will even check in and out when changing trains. But will holders of season tickets be prepared to do it? In schemes with flat fees, the problem will be smaller, as a check-in will be sufficient.

2. *Will the ERG-Proton deal bring about the cross-border electronic Euro and door-to-door usable transport tickets?*

Peter Fogarty, CEO of ERG, said: "With the majority of major transport operators in the UK adopting ERG's technology, and now adoption of the technology in Germany, ERG is increasing the likelihood of its technology becoming a standard across Europe." At present, there is little interoperability between the various electronic ticketing schemes being deployed in Europe, although initiatives such as "Fastest" or "kontiki" are discussing interoperable tickets [info]. Will interoperability be increased in the future, thanks to ERG obtaining a strong position in Europe? And will transport companies issue an electronic Euro which can be used all over Europe?

Furthermore, while the regional operators may consider inter-operability with selected other local operators, what does this mean for door-to-door ticketing? Will the long-distance train operators put their ticket on the same card? Or would we no longer really need the door-to-door ticket anyway when local trips can be handled more conveniently?

[info]

- Berliner Verkehrsbetriebe (Transport Authority of Berlin): <http://www.bvg.de/>
- Card.etc: <http://www.cardetc.de/>
- CEN Workshop Fastest, led by Berliner Verkehrsbetriebe: <http://www.cenorm.be/iss/Workshop/fastest/default.htm>
- ERG Group Media Releases: <http://www.erggroup.com/news/media/index.cfm>
- Global Platform: <http://www.globalplatform.org>
- Kontiki: http://www.contactless-club.com/pages/whats_other.htm ; <http://www.kontiki.net>
- Murray-West, Rosie: National Express invests in smartcards. 10 Feb. 2000
<http://www.telegraph.co.uk/et?ac=004395484117162&rtmo=QwxQxH9R&atmo=rrrrrrq&pg=/et/00/2/10/cne xp10.html>
- Octopus Cards (formerly "Creative Star"): <http://www.octopuscard.com/>
- Proton World: <http://www.protonworld.com/press/index.htm>
- Rhein-Main-Verkehrsverbund (in German): http://www.rmv-get-in.de/fs_02.html

[13&5]

Billing Woes

Thorsten Wichmann (tw@berlecon.de), Berlecon Research, Berlin, Germany

/billing/telecoms

Telecommunication operators are supposedly in a good position to offer billing services for content providers. However, as a closer look at the requirements for modern billing systems shows, the traditional telco billing infrastructure is not sufficient for offering modern billing services. Only recently have the telcos started to introduce new billing systems that are specially designed for handling the complexity of billing for voice, data, content and products using a variety of payment instruments and pricing schemes.

It is often said that telecommunication operators (telcos) are in a good position to become billing providers for third parties. As they already have a billing relationship with households or individuals, so the argument, they could easily put charges for content or services consumed on the Internet or via mobile phone onto the bill, collect the proceeds and redistribute a fair share to the content or service providers.

This seems to be easier said than done: E.g., the lack of billing systems for content was seen during 2000 and 2001 as one of the major obstacles to the development of the mobile Internet. As mobile content providers had no possibility to charge for their offerings, they had no incentive to create truly valuable services. Only recently have the mobile operators started to offer billing-services for third-party content, most prominently KPN mobile and e-plus with the European introduction of i-mode this spring. While these services are a start, they are restricted to the users of the networks and to services and goods provided by the official partners of these networks.

This article discusses the challenges facing modern billing services in general. Its purpose is to show – in a rather simplified way – why billing (the consolidation of charging records on a per-user basis and the presentation of this information to the customer) becomes non-trivial as soon as many different parties, many different pricing schemes and many different payment schemes come together. These complexities explain to a certain extent why telcos are much slower in introducing third-party payment solutions than expected by many.

Traditionally, billing for voice telephony was rather simple. The cost depended on the duration of a call, the distance between the parties involved and the time when the call took place. This information was generated for each call and compiled in a dataset called CDR (Call Detail Record) by switches, the technical equipment routing each call. Billing in these early days basically consisted of attaching a price to each event according to given rules (called rating), aggregating the information for each telephone line, maybe applying a discount scheme and eventually sending out the bill. This was typically done way after the event (the call) had taken place and in batch mode, e.g. by processing all records at the end of the month.

Over time, the CDR has become larger by including more information. Also aggregation of CDRs has become more complicated, e.g. due to roaming. If mobile phone users roam on any other than their home network, the CDR produced by these switches somehow has to find its way to the home operator for billing in some way. Nevertheless, even in these more complicated settings the operator's main currency remains the CDR.

So far the simple story of the old world. In the new – convergent – world, things are much more complicated: not only telephone minutes are supposed to be billed, but also totally different entities like data packets, digital goods or subscriptions to digital services. To complicate matters, these are not necessarily post-paid, but often pre-paid. In addition rebates might apply and the proceeds might have to be shared between telephone operator and content provider. What is needed for this new world is a convergent billing system. The CDR-based legacy billing system employed by most incumbent telcos is ill-suited for these requirements. The following scenarios show why.

Assume that young Swedish teenager Knud has a prepaid card for his mobile phone. Each time he wants to make a call, the system has to check his account and make sure that sufficient funds are available to conduct the call. Even more – the system has to deduct the amounts due continuously from his account to make sure that the total cost of the call at the end is not more than the funds available. It is obvious that the traditional batch-processed CDR-based system is not sufficient for this purpose. The operator needs a real-time billing system or at least a very fast batch system that works almost in real-time.

Only so-called next-generation billing systems provide this functionality. They enable transactional real-time billing, meaning that the system can decide before an event takes place whether this event is allowed to take place. This is not only important with pre-paid cards: Imagine Arnd, Knud's father, wanting to buy a Bahamas trip for his family and using his mobile phone as payment device. Although Arnd has a post-paid account with his mobile operator, the system would typically check whether Arnd is really good for the unusually high amount. To do this, the system might have to connect to Arnd's bank. Needless to say, interfaces enabling this will have to be provided.

Also rating becomes more complicated as new strategies for customer relationship management make prices more variable: Maybe the Bahamas flights are the first ones booked with the respective carrier and Arnd is entitled to a 10 percent discount. Or he receives an hour of free airtime on his mobile phone. The billing system must be able to handle such extremely flexible pricing schemes.

Next is revenue sharing. As the operator receives a share of the revenue from the Bahamas tickets, this must be accounted somehow by keeping special partner accounts. A related issue are tax rates: In many countries the VAT-rates differ depending on the nature of the good or service. While there might be no VAT on Arnd's plane tickets, the full rate might apply to Knud's telephone charges, and a reduced rate to a theatre ticket.

And the correct aggregation of information is only the beginning, as the internal billing engine has to be connected to all different sorts of (external) payment systems. Some customers might use a credit card, others direct debit, invoice, pre-paid cards or a mixture of these. As things are getting obscure, the system has to provide the telco with the necessary means to manage the risks associated with these payments and to assess the current exposure at each point in time.

As these examples show, billing in a convergent world is not an easy task. And these are only some of the issues a complete convergent billing system has to tackle. Currently, many telcos are in the

process of installing such systems, which are provided by specialised companies like Amdocs, Portal Software, SchlumbergerSema, Convergys and several others. In particular incumbent operators have to solve the additional problem of connecting these new systems with their legacy systems or the problem of designing a seamless migration towards a new billing system. This, like all large IT projects, is also a challenge.

[info]

- <http://www.billingforbusiness.com/>
- <http://www.globalbilling.org/>

[13&6]

Success factors for credit card fraud? An illustrative example: the Yescard

Laurent Beslay (laurent.beslay@jrc.es), IPTS, Seville

/security/smartcards/usability

Cyber-fraud, as fraud in general, is made possible by the confluence of three factors: motive, opportunity and vulnerability. When the value is sufficient to incite motive, the influence of the two other factors depends specifically on the available technologies - in the case of cyber-fraud - on the availability of new information and communications technologies. The Yescard case is an interesting illustration of this concept. It shows that the opportunity for fraud increases considerably due to publicly available "encapsulated skills". As this illegal technology also fulfils the main criterions necessary for widespread acceptance of a technology, developers of legal security technology can draw some lessons from this case.

In Spring 2001, a new type of credit card fraud, employing the so-called Yescard, appeared in France, the native country of the smartcards, which also goes for banking smartcards for internet and mobile payments (e.g. C-SET, CyberComm, Paiement CB sur mobile). It is a credit card emulator based on virgin smartcards, which are freely available and can be programmed for numerous functions. With the proper tools that can be found on the Internet and at an electronic components basic retailer, it is possible to build three types of Yescard. The first type can be a clone with the data of a real bank card. The second type is a card in which the authentication value is generated by cryptographic computation, in this case the credit card number can be logical but unreal or it can coincidentally correspond to an existing one which constitutes the third type of Yescard. The name comes from the fact that whatever PIN code is given, the smartcard is always recognised positively and accepted by point of sales terminals or vending machines, which deliver goods, services, transport tickets, gasoline, etc.

The development of the Yescard must be seen more as the ultimate step in a linear process than an accident or a non-linear "discovery". Indeed, the first step of this kind of fraud was made with the old decoder box of well-known European pay-channels; the first swindler used to weld a couple of electronic components with a flash-EEPROM, which was able to unscramble these pay-channels. Then, following the growth of satellite receivers, smartcards were forged for satellite decoders in order to have free access to the satellite package, and this has led finally to the Yescard. Even if there are a couple of innovations around the Yescard, which permitted to go a step further in fraud, the various technological tools were already in use and the initial technologies were already well known. The novelty lies in the distribution of encapsulated skills via Internet and the user friendliness of the tool.

Yescard – easy distribution of encapsulated skills

Using the potential of an Internet forum to share information, a group of "users" enhanced the capabilities of the Yescard. One of them developed and diffused the "geZeroLee" software, which facilitates the production of Yescards by integrating several steps of the fraud "procedure". This software became a very useful fraud tool, mainly for non face-to-face transactions. Indeed, the card is a blank smartcard with no bank name or hologram. Nevertheless, according to the latest news, some Yescards counterfeiting real credit cards are already in circulation. The user only has to carefully

exchange the chip of the cards. This news would mean that Yescards can now be used at real points of sale in any shop.

Yescard first targeted pay-TV channels to "buy" movies on demand. The latest official victim of the Yescard in France according to the media, are the automatic DVD renting machines. Targets of fraud change rapidly. Thus it would come as no surprise if fraudsters would pay a return visit to pay-TV, which today not only offers movies on demand, but also goods, devices and web-services.

The geZeroLee software built with the Delphi programming tool (Delphi is essentially object Pascal with similar programming tools found in Microsoft Visual Basic 3.0) has an extremely user-friendly interface, which is accessible to any fraud rookie. It seems that the fraud tool designers consider a top priority that their creations are easy to use and understandable for every trainee. Its latest version permits the production of Yescards, which are accepted by any point-of-sale terminal. It must be underlined that its growing use is catalysed specifically by this user-friendly nature, which is not the strength of most security or protection software.

This friendly tool also underlines the specific dimension of cyber-fraud in relying on encapsulated skills. This availability to a broad audience has a direct impact on the level of opportunity and vulnerability for cyber-fraud. To counterfeit a bank note, a lot of important skills are needed like drawing, colour, design, paper engineering, etc..., and therefore a lot of training time to acquire these very specific skills. With the Yescard fraud, an Internet connection and a couple of cheap electronic tools are enough to "make money". The clever part of the process (key generator, crack and deciphering software) can be more or less freely downloaded and used without reinventing the wheel. This new dimension effectively boosts the level of fraud opportunity. Indeed, with encapsulated skills, the cyber-fraud "market" is now accessible to new players who could never before commit this kind of fraud because of the skills bottleneck.

Yescard – an example of user friendliness

Even if it is unusual to apply the Technology Acceptance Model of Davis (see [info]) to illegal technology, it is really interesting to notice the very attractive rank, which could be achieved by the Yescard applying this model. TAM was developed to predict and explain the voluntary use of any type of end user computing system. It takes into account a) the perception of usefulness, b) actual use, and c) ease of use.

In France use is made of smartcards in numerous non-face-to-face commercial applications which represent hundreds of potential targets (Public parking, food distributors, transport ticket, post services, gasoline station, etc.). Therefore this new device offers a lot of new fraud opportunities, which strengthen its *perception of usefulness*. Similarly, the linear progression of fraud innovation around the card encourages the *actual use*. Indeed, the technology for this new kind of fraud was already well diffused and used for legal and sometimes even illegal applications. And finally, the user-friendly interface and the encapsulated skills of this computing system boost the perceived *ease of use*. It appears clearly that the Yescard presents a winner business case as a new computing system. More seriously it underlines the necessity for new computing systems in general and for security tools in particular to enhance their user-friendly interface and their usefulness in order to have a chance to be adopted by the end user.

The objective is not to applaud the Yescard phenomenon but rather to describe the success factors of this magic card and compare its great "market acceptability" to the one of tools delivered by cybersecurity industry, if this exists.

[info]

- Davis, F.D.: A technology acceptance model for empirically testing new end-user information systems: theory and results. MIT Sloan School of Management, Cambridge, MA, 1986.
- A well documented web-site on French credit card fraud: <http://parodie.com/monetique/>
- A positive and diplomatic article, which forgets to underline the flaw of the new authentication method which use a 768 bits RSA key. It progressively replaces the previous 320 bits key (this "old" key will be available until 2004) in order to stop Yescard fraud. Science & Avenir janvier 2002 numero: 659, <http://www.sciencesetavenir.com/tempsfort/p659/a8942.html>

[13&7]

Internet and Mobile security in Singapore

Luigi Sciusco (sciusco@tiscalinet.it), Rome, Italy

/review/security/mobile payment systems/Singapore

February 2002 the Monetary Authority of Singapore (MAS) issued a consultative paper on "Security guidelines for mobile banking & payments" ("Mobile report" for short). This paper followed another publication by MAS (July 2001, version 1.1) about "Internet banking, technology risk management guidelines" ("Internet report" for short). The reports provide guidelines to help banks identifying area of risks and to put in place the best organisational, legal and technical tools to monitor such risks. These reports do not go into details of specific attacks or tools. In this article both reports are reviewed.

The Internet Report

The Internet report is a valuable job especially because it explicitly defines a methodology. After a short introduction (chapter 1), the report summarises the main points of a risk management framework (chapter 2). These concepts may look trivial to self-confident readers but I completely share with the authors the opinion that it is necessary to stress their importance: quite often they do not receive the proper consideration and this "arrogance" leads to poor risk management. Chapter 3 outlines the types of Internet financial services and chapter 4 describes the security and control objectives. These two chapters (3 and 4) are the core of the report. Here MAS tries to answer two key questions of any risk analysis: "is there a need for security above a 'baseline' level?" and "what and where are the security risks?". The authors provide the right basis to help banks to give the more appropriate answers and to create an effective asset model. In the following chapters the report focuses on some fundamental security principles (human resource management, firewall infrastructure) and practices. Special attention is given to recovery and business continuity (chapter 6) and outsourcing management (chapter 7) and, after 11 September, this highlights the great attention and expertise of MAS in the field of security. Afterwards, the report correctly deals with bank disclosure (chapter 8) and customer education (chapter 9), that both play a key role in achieving a high level of security for Internet banking platforms.

Everything is perfect in this paper? Not perfect, but very good. However it should be clear to readers that this document is not a security elixir: it is just a document about best practice. Any bank has to identify its own security requirements assessing risks and analysing the legal requirements that they have to satisfy.

The Mobile Report

When I started to read the Mobile report, I expected the same clean approach to the problem. I read the report assuming that its scope is not limited to mobile phones but to mobile computing facilities (e.g. notebooks, palmtops, laptops, mobile phones).

I agree on the fact that a repetition of the risk management framework is not necessary and a simple cross reference to the Internet report is enough. However, in the introduction there is a description of authentication methods, PIN security, transaction logs, fraud detection. I think that this creates confusion: the paper starts with security practices instead of giving guidelines to build the proper asset model.

After this introduction the authors analyse bank accounts and stored value accounts (the assets) and then they deal with technology risk management and security practices. I cannot understand why the Mobile report does not have the same clear conceptual framework of the Internet report. I would suggest to use, *mutatis mutandis*, the same chapters of the Internet report, thus creating coherence between the two reports. In this way the reader would be invited to have a clear scheme in his mind and apply it to every risk analysis activity.

The Mobile report does not address security of pseudo-random numbers used to charge mobile phones or electronic money products. This issue is not strictly related to wireless communication but it

is visible to end users. Citizens don't know anything about security benchmarks for algorithms used to generate such numbers and for methods used to print and distribute them.

The report focuses on technological security that, of course, is of primary importance while it does not deal enough with human factors. If we have a perfect wireless network but people forget their mobile devices on tables, security is weak. In my opinion it should be stressed that when mobile devices are used in public places, care should be taken to avoid the risk of prying by unauthorised people. Mobile devices should be physically protected against theft, especially if they store critical information. Finally, training should be arranged for staff using such devices to raise their awareness on the additional risks resulting from this way of working and the controls that should be implemented.

I am not sure that a specific report for mobile computing facilities was necessary. I think that the main point is not whether the device communicates via radio or not: the strength of an architecture critically depends on effective information security management systems. I expected to read something more about personal security management (see [info]) but with current operating systems there probably is no effective solution to protect against a large scale attack on personal devices.

[info]

- The reports can be downloaded, free of charge, at <http://www.mas.gov.sg>
- Useful information about best practices in information security can be found in the following standards: ISO 17799 and ISO 13335. For more information about them, please contact your national ISO member or <http://www.iso.ch>
- About personal security management see Birgit Pfitzmann, James Riordan, Christian Stübke, Michael Waidner, Arnd Weber: "The Perseus system architecture"; IBM Research Report RZ 3335 (#93381) 04/09/01, IBM Research Division, Zurich, Apr. 2001. <http://www-krypt.cs.uni-sb.de/~perseus>

[13&8]

The ePSO Final Conference: hopefully not the end

Leo Van Hove (Leo.Van.Hove@vub.ac.be), *Free University of Brussels, Belgium*

/pay-per-view/smartcards/regulation

On February 19, Brussels was the scene for the ePSO Final Conference. This review proffers some personal impressions about the conference in general, as well as a number of reflections about issues that were (or were not) discussed. Topics tackled include micro-payments and the pay-per-view business model, the role of non-banks, and the future of smart cards.

As most readers will know, on February 19 the ePSO Final Conference on "Consumer Online Payments: Trends and Challenges for Europe" took place in Brussels. Since the minutes are available on the ePSO website, I will not try to present a complete overview of the conference (which would be impossible anyhow) nor will I try to summarise the presentations that I attended. Rather I would like to bring forward some personal impressions and raise a number of additional points – some of which were mentioned at the conference but did not make it into the minutes, some of which were not addressed at all.

One such point relates to a remark made by Peter Seipp, Chief Operating Officer of Germany-based paybox, who pointed out – and coming as it did from a mobile payment service provider this surprised me somewhat at first – that he does not believe in micro-payments. Mr Seipp argued that consumers are simply not interested in paying 5 cents here and 5 cents there. Also, and perhaps more importantly, micro-payments would be – in his words – "the death of content providers". Later on Mr Seipp clarified his stance by pointing out that perhaps content providers might resort to a pay-per-view business model and thus to *prices* at the euro cents level, but that he did not believe that this would also result in *payments* at the euro cents level. The solution, in his view, would be aggregation of some sort.

This is a question that has been bothering me for some time: to what extent will the pay-per-use model really catch on? The answer to this question has important implications because it will determine to a large extent the importance of small-value and micro-payments, and therefore the need for payment schemes that can handle such payments. Ultimately it might determine the future of electronic money – in the stored-value sense – on the Internet. This is why I would have liked to see a presentation by a content provider at the ePSO conference. A particularly interesting candidate would

have been The Economist. Some months ago they introduced a pay-per-view service. This gives non-subscribers the possibility to buy one-time access – with a money-back-guarantee – to premium-content articles from the Economist.com archives, and this at USD 2.95 apiece. Delivering the article and charging the user is done by Northern Light. Their payment mechanism relies not on any novel scheme developed specifically for the Internet but – yes, Mr Seipp – on aggregation and ultimately on credit cards. That is, the credit card of a Northern Light account holder is charged for purchases on the 28th of each month or when the document purchases have reached USD 20, whichever comes first. Also, when looking at the way in which The Economist has set its prices, one gets the impression that they have embraced the pay-per-view model only half-heartedly. If you expect to read more than three articles in a given month, then a monthly subscription which gives you unlimited access for USD 9.95 is a better option. And if you expect to have this level of monthly consumption throughout the year, then a yearly subscription (at USD 59) is available at half the price of 12 monthly subscriptions. Clearly the Pay Per View Service aims only at the (very) occasional reader. So perhaps publishers do indeed fear, as was predicted by Shapiro and Varian (1999, p. 77), that if they had to sell each article on a pay-per-read basis (at a reasonable flat price) they would get significantly less revenue compared to a situation in which they can resort to bundling.

My biggest frustration concerning the ePSO Conference, however, was of a positive nature: I would have liked to be able to attend all three parallel sessions. Given that I was the rapporteur for the Session on "Innovation & Regulation", I was not even in a position to sneak in and out of sessions. For example, a recurring theme in "my" session was the continued reliance on bank schemes and their infrastructure. Mike Hendry pointed out that "non-bank systems always sit on top of bank systems". Both Peter Seipp of paybox and Alberto Sanz of Mobipay International emphasised that they see themselves primarily as "activators" that leverage existing bank payment systems. The two speakers also took pains to emphasise that their m-payment solutions are not – for now at least – substitutes for bank cards but that they rather create new business. Mobipay is backed by the bulk of Spanish financial institutions, for that matter. And Mr Seipp indicated that paybox is now open for participation by banks. While to date paybox has been an independent player, the company is moving to an indirect sale solution with partners. In this scenario, the product will be co-branded: it will carry the paybox logo, but – and this may well be crucial for banks – the partner company gets to keep its relationship with its customers. This is one reason why I would have liked to also attend the presentations by the people from PayPal and eBay in order to see to what extent they actually plan to take the place of banks and credit card companies instead of making the line of intermediaries even longer.

At the same time I regret having missed the presentations by Hervé Kergoat of Europay International and by Dave Birch of Consult Hyperion because a crucial question for the future is indeed which role smart cards will play (and within what time frame). If e-purses cannot justify a card reader infrastructure, then perhaps credit card fraud can, or the need for digital identities in general? From the minutes I learn that Mr Kergoat is convinced that it will take multiple applications to warrant investment in card readers, and that Dave Birch at least is still "optimistic that the technological future of security will be based on smart cards". In this respect, the Finnish case presented by Sakari Myllymäki was probably also interesting because for some time now the OKO Bank has been commercially exploiting the FINEID government ID-card for authenticating customers and obtaining their digital signatures. Reading all this, I could not help thinking about Malaysia, for example, where the Government Multipurpose Card was launched in April 2001. The card combines national ID with driver's license, passport and health applications. In addition, cardholders can load an optional electronic purse. Plans were to cover the nation of 22 million within three to six years.

If anything, I hope my long lament about missed sessions demonstrates that the future outlook of online consumer payments, in Europe and elsewhere, will be the result of the interaction of multiple requirements and multiple players. The latter do not only include the usual suspects, and the recent additions to that list (banks, consumers, telecom providers and other non-banks, e-tailers), but also e-content providers and lest not forget copyright holders (cf. the presentation by Anthony Belpaire of Info2Clear on Digital Rights Management). And then I almost overlooked regulators. During the discussion at the end of my session the "innovators" indicated that they primarily expect regulators to create stability. Although they agreed that regulators can sometimes play a positive role (as in Spain where the antitrust regulator forced Movilpago to open up), they complained that the legal environment can be a "jungle". A point well understood by Mr Thébault, Director Financial

Institutions of DG Internal Market, who in his presentation earlier that day had already pointed out that EU regulation of the payments industry is too scattered. Let us hope that this will guide future regulatory initiatives.

Summing up, the ePSO Conference clearly addressed a complex, multi-faceted issue and demonstrated that it is far from solved. Given that all reactions that I heard concerning both ePSO and the event were most positive, let us hope ePSO will continue in some form after the 15 months for which it was originally scheduled. The need for a neutral observatory has not lessened.

[info]

- Conference website <http://eps0.jrc.es/conference>
- Shapiro, Carl and Hal R. Varian, *Information rules: a strategic guide to the network economy*, Harvard Business School Press, 1999 <http://www.inforules.com>

ePSO Newsletter – Issue 14, May 2002

Focus: Small Value Cross-Border Payments

[14&1]

Editorial: Cross with Old Banking Boys' Cross-border Retail Payment Networks

Knud Böhle (knud.boehle@itas.fzk.de), ITAS, Karlsruhe, Germany

/cross-border payments/European Commission/European Central Bank//P2P/Internet/e-commerce

To overcome the unsatisfactory situation of cross-border retail payments in Europe, not only co-operation of the banking industry is required. In addition the joint forces of regulation, competition and technological innovation are necessary to speed up change. The potential of converging B2C e-commerce payments and P2P credit transfers is often not taken properly into account. In addition to the editorial, four articles deal with the cross-border issue: an interview with Harry Leinonen, adviser of the Bank of Finland, a thorough analysis by Mike Hendry of status and options in the cross-border area; an assessment by Malte Krueger of the problem solving potential of m-payment systems in this respect, and by Michael Rader a look back at the good old times of the Eurocheque and International Money Orders. Further articles present findings of a consumer online-payment survey, information about a workshop on the future of online-banking, and Leo Van Hove's review of a study on "Recommendation 97/489/EC" concerning electronic payments.

The current ePSO-N issue is focussed on cross-border retail payments. Defining the problem, we first have to keep in mind that the concept of "retail payments" covers a wide range from micropayments up to € 50,000. Second it is worth to distinguish the B2C e-commerce payment part from the P2P credit transfer part. The two parts are interrelated, and, as a consequence of e-commerce and European integration, growth is expected in both of them. Exact data are hard to find, however some indications are given in [14&2] and [14&6].

For all we know, the payment instrument of choice for cross-border e-commerce is the credit card, due in part to a lack of viable alternatives such as cross-border e-money or electronic giro payments (see Böhle 2002 for more details). While for cross-border e-commerce payments at least one strong, although not all embracing solution is available, in the field of low value cross-border credit transfers it looks as if there were no efficient solutions at all. The current infrastructure is still based on old technology, is inconvenient, and expensive for customers.

The status quo is not only a problem in the light of the predicted demand, it is a tremendous political problem as cheap cross-border payments within the European Union would be one of the most concrete benefits for EU citizens and thus a success story for European policy. In the past however, despite a series of EC efforts to put pressure on banks (detailed in Jones 2002 and STOA 2001), the banking industry has been moving slow to change. ECB states "the banking sector has failed to address in a serious manner the issue of cross-border retail payments in euro and the situation remains highly unsatisfactory" (ECB 2001, p. 4). The question therefore is: What impact will the forces of regulation, competition, and technological innovation have to change the current state of things?

Regulation

In December 2001 the EC imposed a new regulation on cross-border payments in euro (EC 2001) mandating the principle of indifference between national charges and charges within the Euro zone. Charles Goldfinger has underlined the "unprecedented character of this procedure" (Goldfinger 2002). At first glance this act of political interventionism might look strange in the context of a liberal market economy. How can reductions of charges be imposed by law, as long as the volume of cross-border transactions is quite small and not an incentive big enough to encourage modernisation of the cross-border retail payment infrastructure? It looks like a vicious circle as with high charges also the demand remains low. Harry Leinonen (see interview) talks of a "negative incentive situation" for banks, and the STOA report already referred to, explains in terms of network theory the inertia of banks and the present deadlock situation with its huge potential switching costs.

Discussing the unsatisfactory situation has two aspects: one is about the level of charges, the other about infrastructure. Actually the average charges for cross-border credit transfers of 100 ECU or 100 € within EU-Europe have not come down considerably since 1993 (the data of the European Commission quoted in Goldfinger 2001 are for 1993: € 23.93; 1994: € 25.41; 1999: € 17.10; and 2001: 24.09 €). As long as the real costs of the correspondent banking system are not transparent, one is allowed to assume that the cross-border segment could be profitable and inefficient at the same time due to a lack of competition.

Given the network effects mentioned above, reducing profits by law however does not automatically result in investments by banks in the cross-border sector. The standard strategy proposed, how to break the vicious circle is to strengthen co-operation within the banking industry. Charles Goldfinger proposes a "Working Party on European payment systems architecture" and Harry Leinonen (see interview) recognises the need for a Masterplan. Indeed there are different paths to interoperable lower cost retail payment systems under construction (see [14&3]), the impression however is that the proposals of the banking sector are rather mid-term than short-term. That is reason enough to consider the potential of alternative players using new technologies.

Competition and technological innovation

Phenomena like PayPal demonstrate how a convenient, reasonable cheap cross-border payment system based on Internet technology combining "virtual accounts" and e-mail messages might look like. The PayPal type of system gives an idea of both the next generation of P2P credit transfers and B2C e-commerce payments. It remains however the solution of a single (non-bank) player with an international network. Big banks like Citibank or Deutsche Bank are also able to bring charges down within their cross-border inhouse networks (e.g. Deutsche Bank charges 1.50 € and the same does Paybox using the network of Deutsche Bank). However these particular developments do not yet establish a new infrastructure.

The next alternative is presented by credit card companies with international credit card networks. Pressed by the success of e-mail-money schemes, credit card companies have started to add P2P payment facilities to their services. This move, stimulated by events in the Internet domain, turns out to hold a promise also for small value credit transfers in general. The STOA study of 2001 makes reference to Europay announcing a new service called "Mastercard Payment/Deposit Transaction Service" that "allows credit cardholders to make P2P-payments via e-mail, even cross-border" (p. 49), and epaynews titles "Visa, Mastercard Ramping P2P Efforts in EU" (epaynews 2002), telling that both card firms aim to have P2P payment services operative in EU by end-2002.

Bottom line: Firstly regulators and moderators like EC and ECB should not only focus on banks, when they develop ideas and strategies how to build the European payment area. The potential of non-banks with new technological solutions should be included systematically. Secondly, restructuring the European payment area, there is a need to take into account both, the requirements of the e-commerce payment part and the credit transfer part in a comprehensive approach. Why not think of an integrated European giro payment system suitable for both parts? Last remark, as systems like PayPal and credit cards schemes appear less suited for payments above €1,000, the mid-term efforts by banks are not threatened. An interoperable and less-fragmented cross-border payment infrastructure is required in any case in the Euro-zone. Given the low pace of banking innovation one might even speculate that banks would prefer to concentrate on higher payments and credit business, leaving the bulk-type payment services to other players.

Many facets of the cross-border problem outlined here, are analysed in more depth in the following articles. The interview with Harry Leinonen deals with the required change of the current cross-border payment system. His rather optimistic vision is based on the increasing demand and the ability of banks to co-operate. As cheapest payment instrument for cross-border payments he suggests customer initiated credit transfers; Mike Hendry provides us with an analysis of the correspondent banking systems and develops several options to overcome the old structure. In the long term he expects convergence of non-bank schemes and banking schemes. In the following Malte Krueger reasons about the potential of mobile payment solutions to fill the cross-border gap, and Michael Rader muses about the little progress made since the days of the Eurocheque.

In the general section we present findings of a German online-survey, the results of which among others hint to the increasing importance of cross border payments. In the section about ePSO activities, Clara Centeno sketches the main points of a workshop on the future of on-line banking held in January 2000 in Barcelona, organised together with University of Girona. Finally, in Leo's corner we come back to the impact of EU regulations on the financial industries. Leo Van Hove reviews a complex evaluation-study about the impact of Recommendation 97/489/EC of 30 July 1997 concerning transactions carried out by electronic payment instruments. This review is just in time as the European Commission plans to turn the Recommendation into a Directive with a working document already on the web about "a possible legal framework for the Single Payment Area in the Internal Market" (see [14&8]) inviting comments.

[info]

- Böhle, Knud: The Innovation Dynamics of Internet Payment Systems Development. IPTS Report, April (2002); <http://www.jrc.es/pages/iptsreport/vol63/english/ICT4E636.html>
- (EC) Regulation No 2560/2001 of the European Parliament and of the Council of 19 December 2001 on cross-border payments in euro. Official Journal of the European Communities 28.12.2001 L 344/13-16; http://europa.eu.int/comm/internal_market/en/finances/payment/area/ec01-2560_en.pdf
- ECB 2001 (European Central Bank): Towards an Integrated Infrastructure for Credit Transfers in Euro. European Central Bank, Frankfurt am Main, November 2001; <http://www.ecb.int>
- epaynews 2002: Visa, Mastercard Ramping P2P Efforts in EU. Lafferty Publications. Retrieved at <http://www.epaynews.com> 16.4.2002
- Goldfinger, Charles (2001 revised version): Institutional Payment Systems and the Internet; http://www.fininter.net/payments/issuepaper_rev.htm
- Goldfinger, Charles (2002): Cross-border payments in euro: Glass half-full or half-empty? <http://www.fininter.net/payments/Euro%20crossborder%20payments%20regulation.htm>
- Jones, Peter: Cross Border Tangle. European Card Review, January/February 2002, p. 30-36
- STOA 2001, Technological Feasibility of Reducing the Costs of Small Cross-Border Transfers (CBCTs) Within the Euro-Zone. Options Brief and Executive Summary, July 2001; available at http://www.europarl.eu.int/stoa/publi/pdf/summaries/00-05-01sum_en.pdf; for the complete report see: European International University Brussels for STOA 2001: Technological Feasibility of Reducing the Costs of Small Cross-Border Transfers (CBCTs) Within the Euro-Zone. European Parliament, Brussels July 2001 (PE 297.569/Fin.St.); to be obtained via STOA in printed form.

[14&2]

Interview: The Road to Efficient Cross-border Retail Payment Systems in Europe: Long and Winding or Straight Through?

Knud Böhle (knud.boehle@itas.fzk.de), ITAS, Karlsruhe, talks to Harry Leinonen (Harry.Leinonen@bof.fi), Bank of Finland, Helsinki

/cross-border/banking/standards/European Union/Finland

Harry Leinonen is Adviser to the Board of the Bank of Finland, particularly on payment system policy issues. Currently he is also the Finnish representative on the Payment and Settlement System Committee (PSSC) within the Eurosystem. For more than 20 years he has actively participated in developing Finnish and international payment systems and standards. Mr Leinonen has also published articles and books on payment system issues. The talk highlights the increasing importance of cross-border payments, shortcomings of the present correspondent bank system, and the need for international standards and co-operation to overcome them.

ePSO: *Mr. Leinonen, what are the most important types of cross-border retail payments?*

Leinonen: Studying, working and vacationing abroad are constantly on the increase and so people are frequently sending money to children and other relatives as well as for their own purposes. Internet has increased the interest and possibilities for buying different kind of goods and services directly from the source in other countries. This kind of trade is bound to increase in the future. Especially as regards Europe, a common currency is likely to lead to increases in cross-border mail-order and e-commerce activities.

ePSO: *Nevertheless, the share of cross-border payments will probably remain quite low...*

Leinonen: You are right in that cross-border payment traffic is generally low compared to domestic traffic. For instance, in the Finnish case the number of cross-border payments is clearly below 1% of domestic payments – in fact only about 0.3-0.5%. However, in value terms, cross-border payments amount to as much as 8-9% (in 2000) of domestic payments. This clearly suggests that the wholesale market is more international than the retail market (which includes a lot of small B2B payments). Some caution is needed here because cross-border payment statistics are generally not as accurate as domestic statistics. There is no clear definition of retail payments to apply in the statistical reports. Looking at credit card statistics, we see a clearly higher growth rate for international transfers (about 15%) than for domestic transfers (about 8%). In Finland the value shares of cross-border payments are 10% for outward bound and 17% for inward bound, both of which clearly exceed corresponding figures for traditional bank-provided foreign payments.

Although Finns are generally active Internet users, e-commerce is only starting to grow. There are no good statistics in this area. Younger consumers, in particular, do order various goods via the Internet, but the volumes are not very large. Credit cards are the main payment instrument for these kinds of purchases and, according to the rough statistics that are available, the share of Internet-type purchases with credit cards rose in 2001 from about 1% to 2%. While the growth has been significant, the total volumes remain low. The volume of online-purchases is still not significant. Domestically you can also use debit cards in Finland in the same way as credit cards. We have also electronic giro and mobile payment systems applicable to e-commerce, but unfortunately we don't have statistics to compare their market share.

ePSO: *Do you expect a considerably increasing demand for cross-border payments?*

Leinonen: The demand for cross-border payments depends on the costs. The introduction of euro cash and payment regulation by the EU Commission (see [info]) will substantially reduce the costs of cross-border payments within the EU area. It will be interesting to see what impact this has on demand over the next few years. My guess is that we will see a very significant increase, especially in Western Europe (e.g. Benelux and neighbouring regions where distances to the borders are often very short). But because customers' payment and purchasing behaviour generally changes slowly, it will probably take some time before the full impact can be observed.

ePSO: *Do you think that the demand, expected to increase slowly, is sufficient to bring about more efficient cross-border retail payment systems?*

Leinonen: The processes and conventions for cross-border payments are clearly less efficient than those of domestic payments. The main reasons seem to be a lack of volume and competition. The present low volumes have not created a business case for banks to invest in cross-border payment systems. Competition in cross-border payment services is also low-keyed, because the service depends on a small number of large correspondent/settlement banks in each country and because no bank, by itself, can improve the system. Wide interbank cooperation is needed. Banks are also caught in a negative incentive situation. Presently, customers must pay bank fees based on current cost levels. In order to improve the cross-border payment systems, banks would have to invest in changes that would cut into their incomes and total margins - seldom a profitable prospect. Because payments derive from commerce and are limited by budget constraints, the overall demand for payments is probably not increasing rapidly. Some part of domestic payments will shift into cross-border payments and some larger payments can be divided into smaller payments, but all in all the total volume will not change drastically in response to fee reductions.

ePSO: *How do the two parts of your answer fit together, i.e. the expectation of a considerable growth of demand by cost reduction and the opposite that the volume won't change drastically by reduction of fees?*

Leinonen: The answers may seem inconsistent and in need of elaboration. Firstly, making a payment is not pleasant, so nobody does it for fun. Secondly, we usually shop close to our own neighbourhoods. Although Internet and the single European currency expand the convenient shopping and low-cost payment area, consumers will still use mainly their local shops. However, we will experience a gradually increasing move from local payments to cross-border payments. The consolidation that we see in progress in all industries will also lead to a gradual shift to cross-border payment patterns. Because current cross-border payment flows are so small, even a slight increase in

volumes will result in considerable growth in cross-border flows. My feeling is that after some years the 20-80% rule will also apply in this case, i.e. 20% of all payments will be cross-border payments in Europe. However, this will depend somewhat on country size and distances. For instance, in the Benelux area the cross-border share will probably be higher than in Finland.

ePSO: *Assuming a co-evolution of demand and more efficient cross-border retail payment systems, what would be the steps required to make it happen?*

Leinonen: Hopefully payment regulation and increased competition via euro-cash have removed the negative incentive situation. This would help in starting up the process of creating a new efficient cross-border payment infrastructure. This is a logistical challenge that should be solved today by an electronic payment network. How should payments be routed quickly and efficiently from payer's to beneficiary's account? For this, we need standardised customer payment interfaces (for both paper-based and electronic payment instructions), interbank payment standards and rules, as well as a payment network to connect banks and payment centres and a common interbank settlement process. An overall decision-making body (managing organization) is needed to control the common infrastructure. Payment processing is a bulk-type service that would benefit greatly from global standards. Domestic payment systems vary a great deal, for historic reasons, but basic payments (credit transfers) require only simple and basic data elements and processes, which are easy to standardize. Good standards have been designed but not implemented. One example is the IBAN (International Bank Account Number), which will finally be implemented in Europe in 2002, following many years of discussion. To get all the different pieces into place so as to create a good infrastructure will require effective cooperation between a large number of parties (banks, clearing centres, central banks, software providers etc). Currently there seems to be good momentum for creating an efficient cross-border infrastructure for Europe, and hopefully this will be a successful process that can be copied in other parts of the world.

ePSO: *Are there current initiatives indicating that the financial sector is moving to comply with the recent EU directive?*

Leinonen: This is somewhat early to answer on. The prices should change by July 1st only. The IBANs and BICs (Bank Identification Codes) have been distributed partly already earlier. The regulation is not asking for other types of compliance. Due to the incentive construction in the regulation the banks are starting to develop the infrastructure but it is still too early to assess what will be the result of this.

ePSO: *In any case, it looks as if a masterplan would be required to bring about the change. Surprisingly you don't mention the Internet or Internet payment instruments as part of the new infrastructure. What role can the Internet play to increase efficiency of cross-border retail payments (P2P, B2C, C2B, SME B2B)?*

Leinonen: You are right in that a masterplan is needed and Internet should be part of it – to enable increased electrification and automation of payments. Payments are bulk services that can easily be automated according to global standards, just as there are international standards for email, phone calls and even word processing. The wall between domestic and cross-border payments should be removed and an international infrastructure implemented. Internet can be used similarly for both domestic and cross-border payments so as to increase payments efficiency. For instance, most Finns, i.e. more than 2.6 million bank customers, already use Internet-based e-banking solutions for making payments. The simplest format is to send an electronic giro to your bank via Internet; the bank then debits your account, credits the receiver's account, and sends an electronic notification to the receiver. Everything is done electronically. Finland nicely illustrates the possibilities of e-banking and e-payments. According to recent year-2001 statistics, 91% of all payment instructions received by Finnish banks are delivered by customers in an electronic format. Only 6% of payments are presented over the counter in Finland (see [info]). What we need in order to achieve this easily and in more countries are international standards.

ePSO: *Talking about B2C e-commerce payment standards one might hold that credit card payments are the de facto standard, and that there is no need for further standards. I remember well your statement at the ePSO-Final Conference in February, where you argued in favour of a credit-push*

that could be effective in real time. In what situations and under which circumstances could a giro payment be more efficient than a credit card payment?

Leinonen: We need different means of payment for different purposes and situations. Card payments are convenient in shops and in other point-of-sale environments. Cards will probably soon be integrated into mobile phones, which will be used as payment terminals. Credit transfers and direct debits, for example, are convenient for making payments effective at specified future dates and recurrent payments.

ePSO: *How would you compare credit transfers and direct debits? In your conference statement you hold that a debit-pull would require too many processing steps. Applying this statement also to B2C e-commerce payments, would this mean that you don't believe in European wide electronic direct debits for e-commerce?*

Leinonen: Credit-push or debit-pull relates to the technical payment process and the order of the debit and credit bookings. In a credit-push process, the paying customer's account is debited prior to payment, i.e. the credit transfer is sent to the receiving bank for crediting. In a debit-pull process, the receiving customer - often a merchant in the case of a card payment - receives the credit booking before the payer's account is debited. This creates a credit risk for the receiving bank or merchant if the transaction is not pre-authorized. However, pre-authorization requires additional transactions. In a real-time environment, card payments can be changed from the current debit-pull to a credit-push process. The authorization request is changed to a real-time credit transfer instruction, so that the paying customer's bank can identify the paying customer with a greater degree of certainty. If the payment instruction is accepted, the merchant's account is credited with immediate finality. This is a more efficient solution in a real-time network environment, and so the international CEPS chip card standard seems to be moving in this direction.

ePSO: *I am a bit surprised that you mention CEPS, the Common Electronic Purse Specifications. Naturally "prepayment" solves the merchant's credit risk, but at the same time the risk of the customer increases that merchants do not fulfil their delivery obligations appropriately – especially in the cross-border area. Do you expect that prepaid schemes will become more important for cross-border payments in the foreseeable future?*

Leinonen: This question relates basically to trust between the buyer and seller. Should the seller trust the buyer to pay after delivery or should the buyer trust the seller to provide the product or service after payment? If there is no trust between these parties a third party, which is very often a bank, can provide the required certainty of delivery and/or payment. Banks have different means to provide trust e.g. DVP (delivery versus payment) procedures, security settlement, revocation possibilities etc. However, to provide trust increases the cost of the transaction due to more complicated processing and/or higher credit risks. It would therefore be important that direct and low cost payments methods would be used whenever the parties have sufficient trust in each other. The term "prepaid" is most often used in connection with chip cards. However, all debit cards could also be seen as prepaid cards, because the funds must be available on the accounts. The same is true also for most of the other bank account dependent transactions. The main obstacle to overcome for chip card based solutions is the required investment in reader equipment. Chip card devices are not common enough. This will probably be solved by mobile phones with integrated payment capabilities becoming generally available. My expectation is therefore that banks and telephone companies will cooperate and provide payment schemes from bank accounts that could be either prepaid or credit based according to needs of the paying customer. For the merchant or the payee there is no technical difference between these alternatives, but the rules of different payment schemes vary.

ePSO: *Well, let's get back to the role of direct debits on the Internet...*

Leinonen: As with card transactions, the direct debits can be used in either a credit-push or debit-pull process. My impression is that the trend in direct debits is toward greater control, i.e. credit-push, and away from less secure debit-pull solutions. With a credit-push solution, the debtor sends a direct debit request to the payer's bank, which debits the payer's account on the due date and returns a credit transfer to the debtor's bank for crediting. Otherwise, the banks would encounter credit risk. However, there is a payer/consumer aspect involved here, due to the possibility of unwanted debits. There is also a remaining credit risk for the banks if direct debit transactions can be revoked. This has led to

different kinds of controls in new and more secure direct debit schemes. The payer can name or pre-authorize the debtors they will accept, and the bank then checks each transaction against the list of accepted debtors. There can also be a limit placed on the frequency and value of debits per debtor. These kinds of automated controls effectively reduce the risks of unwanted debits. The banks must also assess the debtors in order to reduce the risk of fraudulent debtors. The risk of fraudulent transactions would be very high if all that was needed to make a debit was an existing customer account number.

ePSO: *Regarding the state of standardization, would you hold that standardization of cross-border credit transfers will be easier to achieve and to implement than of direct debits?*

Leinonen: Credit transfers are easier to implement because the payment flow is straightforward, credit risks are low, and customer identification is done by the payer's bank. Credit transfers will become highly user friendly when payment and billing information can be sent email-style via the Internet and, upon inspection, forwarded to the bank for payment on the due date.

A low risk direct debit scheme would require – in addition to credit transfer standards – standardization of direct debit requests, pre-authorization, limitation registers, and a European debtor codification system. Today the domestic direct debit conventions and processes, as well as the rules and regulations, are different. We would need a common starting point before drawing up detailed standards. However, this does not mean that such a good payment instrument as the direct debit should be discarded in respect of cross-border payments. The direct debit has its place among the means of payments, especially for recurrent payments such as for electricity, telephone, tax, credit card invoices etc. My feeling is that it will take some time yet before a European consensus is reached on this more complicated payment instrument than on the more basic credit transfer instrument.

ePSO: *Having considered credit transfers, credit card payments, and direct debits, where do you see the niche or role for schemes like PayPal in the field of cross-border payments? Would you regard PayPal as a model for future international online-banking and e-commerce payments?*

Leinonen: It is difficult to answer in respect of specific private schemes and brands, but I will try to answer the question in broader terms. The traditional banking sector has not thus far been able to deliver an efficient international routing code for transfers, i.e. an international account number. The IBAN represents a good attempt, but it is still in the implementation phase. New systems have solved this problem via innovative solutions incorporating email addresses and phone numbers. Many banks are still using batch systems, and interbank transfers are also slow due to batch processing and inefficient transportation networks. New entrants are using real-time and end-to-end solutions based on efficient networks. Customers are interested in e-services based on the Internet, but banks have generally been slow to provide such services, thus enabling new entrants to secure a market advantage. Some of these new entrants, together with modern banks, are developing a model for future e-banking and e-payments that differs very much from the current banking and payment environment. My impression is that the outline of this new model has emerged during the last couple of years, but it needs to be refined in detail in order to serve as a guide for an efficient overall infrastructure on the global level.

ePSO: *Given the constraints of ePSO-N interviews, there's just room for a final question about the future payment infrastructure. I wonder how far the payment infrastructure has to be an integral part of the e-commerce infrastructure. Would you say that a new type of integrated standards is needed and that closer co-operation of standardisation bodies is required to bring them about, e.g. co-operation of standardization bodies dealing with e-commerce standards like CEN/ISSS or IETF and payment and e-banking standards bodies like ECBS? Are payment standards underway to fulfil the needs of e-tailers in a real-time environment?*

Leinonen: There are two important factors in electronic integration: the record/data standards of payments and the reference/remittance information for identifying specific transactions. Interface standards are needed for all parties to process the payment data. The creation of national Finnish payment standards has been the basis for the high electronification level. But as you point out merchants and other payees need to be able to identify the payer and which invoice has been paid. The Finnish payment standards therefore contain a reference number, which is stated on the invoices and giro forms, and which will be transported along with the other payment data throughout the payment

process. The recipient/payee will thereby be able to automatically update the receivables file upon receipt of the payment. An evidence for the importance of the reference code is that more than two thirds of the Finnish credit transfers contain a reference number. This kind of payment reference/identification code can be found in Scandinavian giro systems and also in some other countries. Unfortunately it is not a general international feature and there are no global standards. Implementation of standards requires cooperation and conflicting standards should be avoided. The advantages of global payment standards are obvious, both for real-time and slower payments. Banks and standardisation bodies should be actively remedying this shortcoming.

ePSO: *Thank you very much for this talk.*

[info]

- Leinonen, Harry: Towards the Future of E-payments. Available from the ePSO Final Conference Webpage at <http://epso.jrc.es/conference/> or directly at <http://epso.jrc.es/conference/presentations/leinonen.ppt>
- Regulation (EC) No 2560/2001 of the European Parliament and of the Council of 19 December 2001 on cross-border payments in euro. Official Journal of the European Communities 28.12.2001 L 344/13 - L344/16; online available at http://europa.eu.int/comm/internal_market/en/finances/payment/area/
- Data on the Finnish payment system are provided by the Finnish Bankers Association at <http://www.pankkiyhdistys.fi/english/index.html>; see especially: Statistical data on banks' payment systems in Finland 1991 - 2000; http://www.pankkiyhdistys.fi/sisalto_eng/upload/pdf/statistics.pdf

[14&3]

Cross-border Low-value Payments. What is Likely to Emerge from the EC Legislation?

Mike Hendry (mike@mikehendry.co.uk), Payment Systems Consultant, England

/regulation/cross-border/banking/Internet/business case

In December 2001 the European Parliament published a Regulation requiring banks to charge no more for retail cross-border euro transactions than for domestic transactions. This poses a challenge to banks and payment schemes, whose current structures impose high costs. This article considers the technical and commercial issues, and what schemes might emerge to meet the requirements.

The Regulation

Following more than ten years of reports and discussions with the banking industry, the EC lost patience in December 2001 and issued a Regulation (EC 2001) requiring banks to reduce the charges made on cross-border low-value payments to the same as those for domestic transactions.

The Regulation applies to cash and card transactions below €12,500 from July 2002, to credit transfers from July 2003 and to transactions below €50,000 from July 2006 (although the change in amount is subject to review). Although it applies to all 15 member states, it only applies to euro transactions (but, for example, UK customers can be expected to make their transfers in euros rather than in sterling if that involves much lower charges – their suppliers and relatives will appreciate it). It is intended to capture most retail payments made by private individuals and small businesses – groups which have been shown to lose out badly from the current charging structure.

According to a report for the European Commission by the Institut Européen Interrégional de la Consommation in April 2000 (IEIC 2000), typical costs for cross-border transfers of €100 range from under €10 for transactions originating in Luxembourg, the Netherlands and Austria, up to over €25 in Ireland & Portugal.

The Technology Assessment unit of the European Parliament, STOA (Scientific and Technological Options Assessment), points out that since 1993 the average cost of cross-border transfers has only dropped from €24 to €17, whereas comparable costs for domestic transfers are under €1 (STOA 2001).

There are also problems with transparency of pricing (ensuring that the consumer knows in advance the cost of the transaction), with double-charging (where both the sender and the receiver are charged for the transaction) and with the length of time the transaction takes to reach the recipient's account. In all these areas there have been some improvements since 1993, but the gap between cross-border and domestic payments remains glaringly wide.

The scope and wording of the Regulation focuses on the cost and transparency of payments, but it also specifically encourages the use of the International Bank Account Number (IBAN) and Bank Identifier Code (BIC) to promote ease of use and to facilitate entry to the new systems.

Current systems

Currently, most retail cross-border payments pass through an antiquated system of correspondent banking, in which amounts are placed in *nostro* accounts with a foreign bank together with an instruction to pay a third party. The system is slow, prone to errors, requires significant manual intervention and hence generates high costs. Double-charging is almost universal.

Increasingly, banks are finding that for common destinations the costs of using the networks designed for higher-value transfers – in particular the SWIFT network – are lower than the costs of correspondent transfers. However, SWIFT is very secure; it has relatively high infrastructure costs and transaction costs are still quite high (following Eurogiro News, 3 August 1999, average is €3.8 per transaction to the bank). In addition, banks carry high costs checking and converting customers' paper instructions into electronic form, resolving errors and incomplete forms etc.

By comparison, typical domestic Automated Clearing House (ACH) schemes have unit transaction costs of less than €0.01 and very low error rates. This is as much because everyone understands how the systems work, how account numbers are structured etc. and because of the absolute number of transactions: the total volume of cross-border retail transactions in Europe is probably around 500 million a year (precise figures are almost impossible to come by), comparable to the domestic volume of, say, Belgium.

The Euro Banking Association, EBA (see [info]) has set up a system called STEP-1 which seeks to address the retail cross-border payment issue. STEP-1 uses the SWIFT network and charges €0.48 per message, although a message can cover multiple payment instructions. However, participating banks still have the manual costs referred to above. An evolution of STEP-1, called STEP-2, is proposed specifically for low-value transactions.

Eurogiro A/S (see [info]), based in Copenhagen, is an association of post/giro banks (in most cases, the main postal savings bank in each country). It has set up a system which permits transfers either into a postal savings account or for cash withdrawal. The average charge for this service to the consumer is €6.22 (STOA 2001) – well under half that of the banks' services – but the drawback is that there is generally only one correspondent in each country and so the service is not convenient to consumers and businesses which want to make transfers to and from their "normal" accounts.

The charge to the partner bank for eurogiro transactions is, however, only €0.01 – 0.02. This draws attention to the fact that most of the cost in a cross-border transaction is not the a network or transaction cost, but rather relates to the manual elements of the transaction: capturing the data, checking account numbers, recovering from errors etc. We can summarise the costs mentioned above as follows:

Table 1: Transaction costs cross-border

	Transaction / network cost to institution	Average charge to customer
Standard bank transfers	€3.80	€17.10
STEP-1	€0.48	~€15
Eurogiro	€0.02	€6.22

Any system which aims to reduce costs down to the level of domestic transactions must address head-on these manual operations and the scope for errors and incomplete information submitted by the user.

Why is cross-border different?

Cross-border transactions generate a disproportionate number of errors and manual operations. However, this is also true of some other types of transaction: one-off payments between individuals for cars, for example. Generally all infrequent transactions are error-prone. Cross-border payments are made worse by language issues, and by lack of familiarity with other countries' banking systems and account number structures.

Differing legal and banking regulatory environments mean that any cross-border system must meet all the different national requirements. Some requirements, (for example money-laundering) are actually more difficult to meet in an international environment, because the databases used to check a person's identity are not homogeneous. This tends to push up the cost of compliance.

Banks have long supported unprofitable activities (which includes most current accounts) on the back of other more profitable activities carried out for the same customer groups. In many cases the charges for domestic transfers are included in the account-holding charge. However, the discussion of cross-border charges comes at a time when market-structure, business and regulatory pressures are driving banks to analyse the unit costs of each operation, to make the costs of each activity transparent and to eliminate cross-subsidies. It would be perverse if as a result of the Regulation, the Parliament effectively required banks to reintroduce a cross-subsidy.

There is a valid argument (Schwan 2002) that implementing the Regulation will cause banks to lose money on cross-border transactions, and that they will therefore discourage rather than encourage the free flow of funds within the euro area. Many banks argue that the Regulation will simply entrench differences between national implementations and charging structures and will do nothing to encourage cross-border flows.

Networks and clearing infrastructures

In a recent paper, the European Central Bank (ECB 2001) reviewed some of the alternative solutions which could provide the network and clearing structures required for cross-border retail payments.

It concluded that a single European ACH for all euro transactions would take too long to set up and would reduce competition. The second option, a pan-European ACH for cross-border transactions only, is very close to the EBA Step-1 model. However, it still restricts competition and the EBA version is based on a relatively high-cost infrastructure.

National ACHs could be linked using the ECB's Target system (which also runs over the SWIFT network). This would cover a much higher proportion of the market, but there are four countries, including Germany, where there is no single national ACH. The ECB is also concerned that linkages of this sort would slow the migration towards a lower-cost infrastructure.

The ECB believes that many large banks will opt for the simpler solution of bilateral links. These would be cheap and easy to set up. However, adoption of this solution would result in fragmentation of the market and a lack of standards; it would also make it very difficult for smaller banks to participate.

None of the ECB's options, however, addresses the manual costs referred to above. Peter Jones (2002) points out that there are two further options:

- Person-to-Person (P2P) payments solutions using the Internet (PayPal model); the marginal cost of such payments can be reduced to the risk only, but the current commercial models adopted by most providers would not allow the kind of universal system sought by the EU.
- Use the Visa and Mastercard networks to enable transfers between card accounts (and potentially pseudo-card accounts for non-cardholders). In fact, both schemes have already been working on such proposals for some time. They would be able to offer the service through any member bank.

Both of these options offer some scope for reducing the manual costs, and hence the price charged to the customer.

The European Payments Group (a group of some 65 banks within the European Banking Federation) has proposed to the ECB a Blueprint for a Single European Payments Area (Simon 2001). At the heart of this Blueprint is a proposal for a standardised consumer-initiated credit transfer, known as the "Eurocred" Eurocred messages could in principle be passed across any network, including secure subnets on the Internet. Detailed standardisation of the Eurocred has been passed to the European Committee for Banking Standards (ECBS), which has a reputation for thoroughness rather than speed.

Requirements for a retail credit transfer scheme

The underlying requirements which must be met by any proposal are fairly simple:

- Wide availability – not restricted to one service provider or group of service providers. Ideally,

all credit institutions should be able to make use of the scheme without major capital cost or subscriptions.

- Low risk, particularly clearing and fraud risk. Money laundering is not generally such an issue, as transfers are being made between established accounts, but the system should also include neural money-laundering checks. Clearing risk is minimised by adopting Straight-Through Processing (STP) wherever possible; fraud risk is minimised by good customer registration procedures and secure logon and password systems.
- Low overheads within the network and clearing system.
- In order to reduce the manual costs for the sending bank, data capture should be automated (preferably fully account-holder-initiated) and there should be some form of automated feedback so that errors can be corrected at data capture time. This is almost certain to require a single standardised form of account number or user ID.

Any system which meets these requirements should be able to provide cross-border transfers at a cost well under €1.

Likely evolution

The requirements listed above can easily be met by an Internet-based solution, and with little difficulty by the card schemes. In each case, however, we need to consider how to cater for the excluded groups: those who do not have Internet access, or who do not have a credit or debit card. Both can be dealt with fairly easily by having an extra step at the front of the process, although this raises again the question: is it better to have uniformity of charging or to avoid cross-subsidies?

A critical issue is the checking of recipients' account numbers; in an Internet solution this is dealt with by using email for notification; the transfer is not initiated until the recipient confirms the details. For users who do not have email, some other form of check is required; an IVR (Interactive Voice Response) or text messaging system could be used.

For the time being, the card schemes and P2P providers are well ahead in the race to provide such a scheme. In the case of the card schemes, transfers are between card accounts, and with the P2P schemes between accounts held on the P2P system. There is, however, no reason why a similar scheme could not be offered by the banking industry itself, using either an existing network or a peer-to-peer solution with suitable authentication; such a scheme could offer transfers between current accounts.

In practice, given most banks' hostility to the Regulation and the lack of enthusiasm with which they have promoted the IBAN, progress towards the Eurocred solution is likely to be slow. However, the P2P providers could greatly enhance their credibility with the banks (and probably their political capital) by adopting any Eurocred standards and offering them as interfaces to the P2P systems, for bank use. This allows the P2P providers to benefit from bank customer registration, while the banks are able to offer a service at very low cost.

This suggests a long-term solution in which the non-bank schemes converge with bank proposals, using a common account structure and messaging system, but with front-end and notification systems similar to those currently used by the P2P providers. Under such a scheme, suppliers could compete to provide wholesale services to banks, or could offer services directly to end users. The ECB should actively encourage the development of such a market and ensure that non-bank providers are represented in the formulation of the Eurocred standard.

[info]

- EC 2001: Regulation (EC) no /2001 of the European Parliament and of the Council on cross-border payments in euro. Consilium PE-Cons 3669/01
- IEIC 2000: Institut Européen Interrégional de la Consommation: "Bank charges in Europe" A report for the European Commission, Directorate-General Sanco
http://europa.eu.int/comm/dgs/health_consumer/library/surveys/sur14_en.pdf
- STOA 2001: "Technological feasibility of reducing the costs of small cross-border credit transfers (CBCTs) within the Euro-zone", STOA, May 2001. Consilium PE 297.569
- Schwan 2002: "European Payment Traffic – a Monetary Policy Undergoing Change". Ingeborg Schwan, UBS AG, Clear-it (Payserv house magazine), Feb 2002 http://www.telekurs-sic.ch/pdf/de/clearit/clearit_12.pdf
- ECB 2001: "Towards an Integrated Infrastructure for Credit Transfers in Euro", European Central Bank, November 2001
- Jones 2001: "Cross-border tangle" Peter Jones, European Card Review, Jan/Feb 2002

- Simon 2001: "Towards the Creation of a Single Euro Payment Area" Pierre Simon, AFECEI, Payments in Euro in the Internal Market conference, September 2001. http://www.afecei.asso.fr/fr/m_paiement/dossier/010924-ps.htm
- Euro Banking Association <http://www.abe.org>
- Eurogiro A/S <http://www.eurogiro.com>

[14&4]

The Cross-border Payments Malaise: M-payments to the Rescue?

Malte Krueger (mkrueger@paysys.de), Frankfurt/M., Germany

/m-payments/cross-border payments/e-commerce

There are hopes that m-payments might improve the current retail payment landscape. Thus, m-payments are seen as a step towards the EU Commission's goal to make cross-border payments cheaper and more convenient and they are assumed to provide a convenient means for micropayments. However, such hopes may be premature. For the moment, m-payments have to rely on the existing payment infrastructure to settle payments.

Cross-border payments have been an issue for a long time. Both the high price and the long duration of such payments have infuriated consumers, small businesses and policy-makers alike. After a long time of investigating the matter and negotiating with banks the European Commission finally took action and mandated that from July 2002 onwards cross-border card payments below € 12,500 may not cost more than national payments. From July 2003 onwards a similar rule applies to cross-border credit transfers. This surely does make cross-border payments cheaper. Whether such a move will encourage the creation of a more efficient cross-border payment system remains to be seen. Doubts have been expressed that mandating low prices will encourage investment in this area (Jones 2002, Schwan 2002). Without further investments, cross-border credit transfers will remain slow and cumbersome and cross-border debits or standing orders will remain impossible.

This has not only implications for households but also for businesses. To be sure, at the real POS, payments by customers from foreign countries are not a big issue. Credit cards and increasingly debit cards can be used internationally – not to mention cash (at least in Europe the Euro has extended the reach of cash impressively – moreover, international ATM networks make it easy to obtain local cash in a foreign country). In e-commerce, things are different. Credit cards can be used internationally and are widely used, however, in many countries other payment systems are dominating on the Internet and these payment systems are usually national in character.

In principle, this would leave the possibility to rely exclusively on credit cards when it comes to international e-commerce. However, such a solution has a number of draw-backs:

- not everyone has a card,
- credit cards are not suitable for micropayments,
- so far, P2P payments are usually not possible,
- credit card payments usually involve a number of risks,
- customers have to pass on personal data to merchants,
- merchants run the risk of charge backs.

There are a number of attempts to make credit card payments on the Internet more secure. However, past attempts have not been successful and the lack of agreement between Visa and Mastercard is slowing down the spread of the new schemes.

Therefore, it is often suggested that m-payments might be used to fill the gap. After all, mobile operators are used to billing of small amounts ("micro billing" as opposed to "micro settlement") and they operate internationally, tracking and billing calls that go through local and foreign networks. Both roaming and international call termination make it necessary to have some kind of clearing and settlement mechanism. It may seem, that this puts mobile operators into an ideal position to offer international payments including micropayments.

The mobile phone can be a useful tool in the payment chain in many ways. First of all, as a communication instrument, it can be used to transmit payment information - providing another communication channel for the use of traditional payment systems. Second, the fact that the user of a

mobile phone can be identified by the SIM can be used for payment authentication purposes. Third, the SIM can be tied to a user account (prepaid or post-paid) that is secured by an extra payment PIN. Or, fourth, it can be tied to a bank account or credit card account. Again, authorisation would be via an additional PIN.

Thus, there is plenty of scope for involving mobile phones in the payment process. But many of these possibilities do not really create any new means of payment. They basically rely on the existing payment infrastructure. Thus, in these cases, m-payments cannot be expected to provide cross-border solutions that are any better than those solutions that already exist. They may, however, make existing services more widely available and more convenient to use.

Thus, improved solutions for cross-border payments can only be expected where mobile operators provide entirely new payment systems or - more importantly - where they use their existing billing infrastructure for voice services to provide a wider array of payment services to third parties. Basically, the latter option consists of putting third party services on the phone bill or of charging third party services to a prepaid account. Since already today any mobile operator charges customers for services provided by other mobile operators - both nationally and internationally - one should think that the move to providing payment services for third parties is not a big issue. However, such a conclusion would be premature because

- there is no common standard for mobile payments,
- third party payment systems would require elaborate risk management,
- payment services would require highly sophisticated billing machines that are able to manage the additional payment information in a reliable way,
- there may be regulatory hurdles.

Voice roaming has been made possible by agreements on a common standard (GSM). In the area of m-payments there is no such standard. At the moment, there only exists a large amount of mutually incompatible payment systems (Krueger 2002). To be sure, there are attempts to solve this problem. There are a large number of industry-fora dedicated to standardisation of m-payments (see Centeno 2001) and there are initiatives of large players such as Mobipay International or the recently announced joint effort of Vodafone and T-Mobile. However, the outcome of these ventures is still uncertain.

Equally, it is not clear whether current risk management techniques and technical billing capabilities would be sufficient for an interoperable payment scheme provided by many operators on an international scale. The technical challenge alone would be large (Wichmann 2002). In addition, operators would have to switch to an almost bank-like risk management approach. For instance, a successful payment scheme with fairly high volumes would necessitate daily settlement or even real-time settlement.

Some of the risk-issues could be circumvented if prepaid payment systems were to be used. However, such systems would involve regulatory problems - such accounts could either be interpreted as e-money or deposits requiring the status of an E-Money Institute or a bank.

In practice, cross-border m-payment solutions involve some type of traditional payment system. For instance, Mobipay International plans to provide credit card payments facilitated by the mobile phone. Paybox offers different kind of cross-border payment possibilities including P2P payments. But all of these are also tied to traditional payment systems. The concrete plans of the Vodafone - T-Mobile joint venture are not yet known.

To sum up: at the moment there is no m-payment system that provides a genuine international payment solution. Whether or not such a system will be developed in the future depends on demand (Is there a business case?), on progress in standardisation and on regulation.

[info]

- Centeno, Clara, Mobile Payment Industry Fora – Consolidation of Initiatives Expected. ePSO-Newsletter – No. 8 – July 2001; <http://epso.jrc.es/newsletter/vol08/3.html>
- Jones, Peter, Cross-border tangle, European Card Review, January/February, 2002
- Krueger, Malte, Mobile payments: a challenge for banks and regulators, IPTS Report, April (2002), 5-11, <http://www.jrc.es/pages/iptsreport/vol63/english/ICT1E636.html>
- Schwan, Ingeborg, Europäischer Zahlungsverkehr: Preispolitik im Umbruch, ClearIT (Swiss Interbank Clearing AG), No. 12, February, http://telekurs-sic.ch/pdf/de/clearit/clearit_12.pdf

- Wichmann, Thorsten, Billing Woes, ePSO Newsletter – No. 13 - 2002, <http://epso.jrc.es/newsletter/vol13/5.html>

[14&5]

Back to Tin Foil and Banknotes? – The Trials and Tribulations of Petty Cross Border Trading

Michael Rader (Michael.Rader@itas.fzk.de), ITAS, Karlsruhe

/low-value payments/cross-border/postal service/Eurocheque/money order

The demise of the Eurocheque has created a gap for low-value cross-border payment systems, even in the bricks and mortar world. There is also a need for the competitively-priced electronic equivalent of postal orders and international money orders. The author's reasoning is based on his hands-on-experiences.

A case of cross-border payments

David has recently embarked on his most ambitious project yet: 8 CDs containing the complete recorded works of Bessie Smith, newly transferred by the best sound restorer in the business. For most people, this is not very exciting news, but for a small band of collectors scattered all over the globe, it is positively mouth-watering. David is a CD producer and owns a typical small business catering for a committed minority market. Such businesses frequently suffer from poor distribution due to lack of interest from the major local wholesalers, and thus resort to selling their product direct to customers, which also has the advantage for the producer that a greater share of the revenue stays in his own hands and can hence be invested for new projects. The sums involved in transactions can be as low as €10 for the single customer, who frequently only wishes a single item.

For domestic customers, buying direct has always been fairly easy since they can use the payment systems in general use in their own country. For very small payments, there were always postage stamps, but these might be falling out of favour in these days of e-mails. For international customers, making cross-border payments of modest size was always something of an adventure. I well remember my own first experience of this, making the pilgrimage to a bank, filling in most intimidating forms in several copies and paying what was then for me an enormous sum, but it was either that or not having the product I wanted.

IMO and Eurogiro

Then I discovered the post office. When post offices were nationally owned and provided what was then regarded as essential services, there used to be a payment instrument called the postal order, and its cross-border counterpart, the international money order (IMO). In both cases, the principle was very simple: the customer filled in a small oblong form containing the details of the sender, the recipient and the amount to be paid, and paid cash in at the post-office counter. The order was duly processed and several weeks or months later, the recipient was paid the money in cash by the local mailman in national currency at his or her own doorstep. The fee for this service was low enough to permit the transfer of fairly modest sums. For people holding an account at the post office savings bank, it was possible to do the paper work at home and to send the form to the postal savings bank by letter. If the recipient also had a postal account with his or her national postal savings bank, it was possible to make a direct transfer from one account to another, even across borders!

For a time, the German post office offered an alternative solution known as the postal cheque. For the customer, the procedure was much the same. The difference was that it took much less time for the process to be completed and that the recipient was delivered a cheque rather than cash. The main disadvantage of this form of cross-border payment was that it was so little known and publicised that someone wishing to make use of it first had to convince the post office counter clerk that it actually existed.

This all came to an end when the post office was deregulated. While post office banks do still offer international money orders, the fees have been "harmonised" with those of international bank transfers. In Germany the cost of the successor of the old IMO is €15 while a TIPANET bank transfer

costs a mere €7.50. Together with Western Union, most major European post banks have set up a system called Eurogiro, which enables fairly cheap transfers from accounts at the post banks to accounts at other post banks, but customers not holding accounts and paying cash are charged the commission of €15. Only the very desperate will use these methods for low value payments of the kind mentioned above. Apart from lack of attractiveness for low-value payments, a major drawback is a complicated fee structure, which means that commissions on transfers vary a great deal, depending on country of destination and the method of payment selected.

The Eurocheque

Until very recently there was an instrument called the Eurocheque which could be used very conveniently for cross-border payments throughout countries participating in the scheme (mainly in Europe). Although they were basically conceived for face-to-face situations, you could simply slip one in an envelope and send it in payment – although I was never sure myself if you could enter your own location or needed to fill in the place where the recipient lived, or how to date the cheque.

Strangely, the Eurocheque originated in Germany, a country where cheques do not traditionally play a major role in the country's payment culture. It took several years for the Eurocheque to achieve widespread acknowledgement – despite the great use made of cheques domestically in the UK, UK banks were among the last in Europe to accept Eurocheques. Once this payment scheme had attained almost universal status in Europe, the cheques were gradually phased out, due largely to the spread of technology like cash dispensers or POS terminals. Eurocheques were no longer accepted in the Nordic countries, France, the UK and Ireland after 2000, the guarantee was dropped (in Germany) at the end of 2001, and the cheque forms lose their validity at the end of 2003. It looks as though the only goal was to demonstrate that you could produce a Europe-wide payment system, and hard luck if you actually got used to it.

Conclusion: Technological progress has actually had the effect of worsening the situation, at least for the time being. As a last resort, people wishing to make cross-border payments once had the option of sending cash or international reply coupons (the international counterpart of postage stamps). The internationally accepted standard was to slip a few dollar bills in the protective wrapping from a bar of chocolate into an envelope mailed to the recipient. The ECB might therefore consider the introduction of one Euro banknotes – maybe those and tin foil will prove an unbeatable combination for cross-border payments.

[info]

- On the situation regarding phasing out of Eurocheques, a newspaper article from a Berlin daily: <http://www2.tagesspiegel.de/archiv/2001/06/22/ak-wi-4410431.html>
- On the German post bank's options for cross-border transactions and their costs: <http://www.postbank.de>

[14&6]

Expanding Niches. Some Results of an Online-survey about Online shopping and Paying

Knud Böhle (knud.boehle@itas.fzk.de), ITAS, Karlsruhe Germany

/survey/payment systems/consumer perceptions/cross-border/Germany

Selected results of the fifth online-survey on "Internet Payment Systems from a Consumer Perspective" are presented. The survey carried out by University Karlsruhe, Germany, shows that even in 2002 the role of traditional payment systems to pay for online-orders has not decreased. At the same time experience with new payment systems also grows, but curiosity seems often to be the main motivation. Interestingly online-shopping cross-border seems already to be of relevance especially with respect to the digital goods market. Furthermore with increasing Internet experience of users the willingness to purchase cross-border apparently grows.

In May 2001 the fourth online-survey called "Internet Payment Systems from a Consumer Perspective" (IZV 4) was already subject of an ePSO-N article (see [info]). This month the results of the fifth survey carried out between December 2001 and February 2002 have been published (see [info]). This time more than 11.000 Internet users participated, and more than 9000 questionnaires were completed. Compared with the 2001 survey the design of the questionnaire has been modified

addressing more the digital goods segment, and the distribution of the questionnaire was changed as it was also available from the web-pages of some specific payment service providers. In this article we don't go into depth and concentrate on some general results. The survey also takes into account a lot of social variables we don't consider here. What has to be kept in mind however with respect to the sample is that participants selected themselves and therefore the results of the survey are in no way representative. To characterise the participants as group, most of them are experienced Internet users with considerable shopping experience (80,6 % have already ordered online at least physical goods), and they are well equipped with basic payment tools: 95,2% have a current account, 64,1% own a credit card and almost all, 98,1%, have a mobile phone.

How do German online-shoppers pay?

The research team of Karl-Heinz Ketterer does not ask for quantifications or explicit preferences in this respect, addresses however the users' experience with different payment methods as can be seen in Table 1 next page.

At first glance it might look surprising that even the conventional methods have increased their percentage between 2001 and 2002 considerably. But as the question addresses just experience in general without a time reference it is quite clear that all values should increase as Internet and shopping experiences develop over the years. Nevertheless the increase of "payments in advance" is especially striking. The plausible explanation of the research team is the popularity of online-auctions often requiring payments in advance. The table also shows the increasing experience with new methods. An optimist will see growth rates of more than 100%, while a sceptic will see that none of the new methods reaches 10 per cent.

Table 1: Experience with different payment methods in percentage of respondents

<i>Which payment methods have you already used for Internet ordering or purchasing over the Internet?</i>		
	IZV 2002	IZV 2001
Payment after receiving a bill	83.1	72.3
Direct Debit	63.1	47.6
Cash on Delivery	63.6	46.6
Payments in advance by cheque or credit transfer	30.9	11.7
Credit card SSL	36.9	32.6
Credit card unsecured	11.0	5.2
Credit card SET	8.2	3.2
Micro-billing	7.5	3.1
Mobile phone	6.8	3.4
Prepaid systems (e-purses, scratchcards etc.)	1.9	1.5

Legend: Adapted from Chakam et al 2002, p 22.

The question why the new methods have been used is interesting. The survey reveals that just testing and curiosity on the one hand, and the use of a special payment method as precondition to obtain a desired good (no alternative) are of great importance here. Comparing just the two motivations out of a broader spectrum used in the survey leads to the following table 2.

Table 2: Motivations to use a new and special payment method

Payment method	Curiosity and testing has been a reason to use a method say in %	No alternative to get the good has been a reason to use a method say in %
Mobile payments	72.9	14.6
Microbilling (special biller)	32.9	75.6
Microbilling (telco as biller)	41.7	64.5
E-purse	57.3	21.7
Scratch cards	65.4	14.1

Legend: Selected and adapted from Chakam et al 2002 p. 34, 41, 49, 56, 65.

First the question arises if raising of "curiosity" is the first step to establish a business case or an indicator of just a momentary interest; second we may ask if the choice of microbilling systems based on the lack of alternatives is an appropriate indication of acceptance, and – as goods paid for in this segment are often of the digital kind – also a sign that the market for paid digital content is beginning to develop.

Do German online-shoppers buy abroad?

In my view the survey's findings concerning online-shopping cross-border are of special interest. The research group asked if people buy cross-border and to what extent. The answers are compiled in table 3:

Table 3: Cross-order shopping experience

<i>Where did you order ?</i>		
	Physical goods	Digital goods
Ordered in home country only	72.1	59.0
Most of the time in home country	22.3	26.5
Most of the time cross-border	4.8	11.1
Only purchased abroad	0.9	3.3

Legend: Selected and adapted from Chakam et al 2002 p. 26.

Cross border trade seems to be more relevant for digital goods than for physical goods, and in 3.3% it is the only rationale for online-shopping. If we aggregate the data of the last two rows we may say that for more than 5% of online-shoppers of physical goods the possibility to shop cross-border is important and for more than 14% with respect to digital goods. If we include the data of those who purchased abroad, although not most of the time, we might get an indication of the relevance of cross-border online-shopping. For 43,8% of those purchasing physical goods and for 51,4% purchasing digital goods the international market seems to be relevant. Optimists might expect this to be the beginning of an international market for digital goods. Our second hand interpretation of the survey data has of course to be handled with caution. There are many tricky questions involved, e.g. the probable interpretation of compact discs (music, software, movies on DVD) as digital goods by those filling the questionnaire.

[info]

- Chakam, Aline Flore; Heitmann, Annika; Leibold, Kay; Stölzle, Robert; Stroborn, Karsten: Internet-Zahlungssysteme aus Sicht der Verbraucher. Ergebnisse der Online-Umfrage IZV 5. Universität Karlsruhe, Karlsruhe 2002
- More information (in German) about the 2002 (IZV 5) and the former 2001 (IZV 4) survey are available at <http://www.iww.uni-karlsruhe.de/izv5/index.php3>
- Stroborn, Karsten: Internet Payment Systems in Germany – the Technologically Advanced Consumers' View. ePSO-Newsletter – No. 7 – May 2001 <http://epso.jrc.es/newsletter/vol07/7.html>

[14&7]

Internet Banking Workshop – A Spanish and European Perspective of the Future

Clara Centeno (clara.centeno@jrc.es), IPTS, Seville, Spain

/internet banking/on-line banking/security/technology innovation

On 11 January 2002 the Gr@dient Research Group of the University of Girona (Spain) and ePSO jointly organised an expert workshop in Barcelona entitled "The future of On-line banking: a Spanish and European perspective". This article provides an outline of the workshop. The complete minutes are available on-line.

The Research Group on Dynamic Evaluation and Economic Impact of New Technologies on Organisations (Gr@dient) of the University of Girona (Spain), together with the ePSO team organised a workshop on "The future of On-line banking: a Spanish and European perspective", held in Barcelona last 11 January 2002. Workshop participants included representatives from banks, professional associations, consultants, academics, service providers and public institutions, from different European countries. The aim of the workshop was to provide a platform for a discussion of the current state and possible lines in the future evolution of on-line banking in Europe, as well as to identify the challenges for supervisors and regulatory bodies of the development of on-line banking. The workshop was organised into three sessions entitled: "What determines success in on-line banking", "Technological innovation in on-line banking", and "The future of on-line banking".

What determines success in on-line banking

Under this session, different business strategies aiming to meet different views on the demand and supply sides were presented. Mr. J. Solé from "la Caixa", the Spanish leading savings bank with 1,5 million customers with on-line access, presented the bank's understanding of the customer needs as increased availability (24h/7d) and functionality. Consequently, the bank's multi-channel strategy has the objective to distribute all products and services through all channels, including iTV and mobile phone. In this strategy the branch network plays a key role in building the customer relationship by providing physical proximity. Results achieved on consumer adoption, actual use and increased profitability were presented.

The contrary strategy has been followed by Abbey National, a major UK bank, which, through internet-banking, aims to gain access to a new, young and innovation-prone customer segment. Abbey National has thus launched Cahoot, an Internet only bank. Mr. T. Sawyer from Cahoot presented what the bank considers the key success factors (trust, reliability, availability, speed and quality of services, cheaper products and services, multi-channel distribution) and strategies for delivery. Since it started in June 2000, Cahoot has acquired 300.000 customers, but has, however, not yet achieved profitability.

Taking the perspective of the supply side, a third approach was presented by Mr. D. Sáez, from Santander Central Hispano (SCH), the first Spanish banking group. The bank's strategy to become 'Net-ready' involves the reengineering of the bank services production process by making use of new information and telecommunication technologies (including but not limited to Internet technology) as well as by integrating Internet banking to the existing distribution channels. The benefits and challenges of this approach were presented.

Finally, both defensive and offensive strategies followed by the Spanish banks, in response to the entry of foreign Internet-only banks, and some of the current profitability challenges were analysed by Mr. E. Bernal from the University of Jaén, Spain.

Technological innovation in on-line banking

Under this session, the important role of the consumer's perception of security for the adoption of new security solutions was stressed by Mr. Naatsaari, from Nordea, Finland, a leading financial services group in the Nordic and Baltic Sea region with more than 2.5 million on-line customers. The challenge to find the right balance between consumer trust, safety, familiarity, habit, low cost and business and technology innovation in a multi-channel approach was presented. Finally, Mr. Naatsaari expressed the view that despite the expected decrease in online-banking technological investment, the security expenditure will maintain its high priority.

Mr. J. Vacarisas from FESTE (the Spanish Foundation for the Study of Security in Electronic Telecommunications), presented his views on the opportunities that legally recognized electronic signatures bring to Internet banking. A number of barriers, however, were also presented as factors hindering adoption.

The future of on-line banking

Mr. Ch. Goldfinger from the FIWG (Financial Internet Working Group) presented Internet banking to be a consequence of a continuous banking evolution as a result of the introduction of ICTs rather than an e-banking revolution and a separate service. He summarised the main strengths and weaknesses of on-line banking, and explained why pure Internet schemes are unlikely to succeed. He finally stressed the need for standards in the task of developing cross-border e-banking in Europe.

Round table discussions

Three round table discussions, chaired by Prof. J. Valls (Gr@dient Research Group), Mr. B. Clements (ICT Unit, IPTS) and Mr. I. Uriarte (AECE, Spanish Association for Electronic Commerce) respectively, brought interesting discussions around among others, the following topics: the difficulties for Internet-banking to achieve profitability in the short term (mainly due to the unexpected cost of introducing the new technologies, of security and of customer acquisition), sustainable business models and major barriers for internet-banking take up (such as limited Internet access); the role of culture in Internet banking take-up; the potential influence of some "niche" banking activities on the industry structure, in a cross-subsidised product model that characterises most European economies; the limited potential role of digital signatures and public key infrastructures to increase the security of on-line retail banking in short term; the trade-off that banks face between outsourcing technology and developing proprietary systems; the potential contribution of on-line banking to the integration of European national markets and enabling factors; the expected banks investments slow down in the short term, and the more adequate EU policy to let market forces act and promote innovation and co-operation.

[info]

- Gr@dient – ePSO Workshop Minutes: The Future of On-line Banking: a Spanish and European Perspective, Barcelona, Friday 11 January 2002 (ePSO: electronic Payment Systems Observatory at the DG JRC – IPTS <http://epso.jrc.es/project/M5Agenda.html>)

[14&8]

Recommendation 97/489/EC Revisited: A Case of Frustrated Expectations?

Leo Van Hove (Leo.Van.Hove@vub.ac.be), Free University of Brussels, Belgium

/review/regulation/EU/

The European Commission is reportedly planning to turn the 1997 Recommendation concerning transactions carried out by electronic payment instruments into a (legally binding) Directive. This review has a look at the detailed study that lies at the basis of the Commission's decision to do so.

In 1999 the European Commission issued a call for tender for a study that was to investigate how far the *Recommendation 97/489/EC of 30 July 1997 concerning transactions carried out by electronic payment instruments and in particular the relationship between holder and issuer* [hereinafter the Recommendation] has been effective in improving the position of electronic payment instrument (EPI) holders, both as a matter of substantive law and in actual practice. The results of this study were published in May last year [see info]. At the ePSO Final Conference last February, Mr. Thébault, Director Financial Institutions of DG Internal Market, stated that "the results were disappointing on several aspects" and that the Commission is preparing a proposal for legally binding legislation. This review has a look at the study that lies at the basis of the Commission's decision.

The study was undertaken by a consortium of 10 academic research centres led by CRID, University of Namur and the Centre for Commercial Law Studies, Queen Mary College in London. The full study comprises more than one thousand pages but fortunately it is organised into a core report of some 90 pages and a slate of appendices. The report provides an overall assessment of

compliance across the member states and identifies the main problem areas, whereas the appendices contain more detailed EU-level results, as well as 15 country reports. The study concentrates on 5 topics, covering the most important provisions of the Recommendation: (1) the transparency of conditions, (2) the obligations and liabilities of the parties, (3) the means of notification in the case of loss or theft, and the liability of the issuer after such notification, (4) the burden of proof, and (5) the settlement of disputes.

Overall, the study is an impressive effort – and this not only on account of its sheer size but also because of the way the findings are presented. I particularly liked the ‘statistical analysis’. For this part, the researchers in each of the countries were asked to give compliance marks - between 1 (very weak) and 5 (very strong) - for a selection of issuers and EPIs, and for each of the 5 criteria mentioned above. These data were subsequently used to calculate average country and criterion marks. Although such scores are by definition subjective, they do simplify comparisons and allow to make tables and graphs that provide the reader with an easy-to-interpret general picture.

Findings that struck me are the following. For one, the statistical analysis shows that the more novel instruments, such as ‘electronic money instruments’ and ‘electronic tokens’, are by no means the black sheep of the herd. Electronic tokens even have the highest score of all EPIs studied. When analysing the compliance per country, Denmark clearly stands out, with an almost perfect score. But then it is the only country that has specific legislation to implement the Recommendation. (Belgium and Luxembourg do have draft legislation aimed at doing so.) Italy, Spain, Greece, and Portugal invariably score below average.

The nature of the problems identified differs across countries but the deficiencies seem most serious for criteria (2), (4), and (5). A problem that is emphasised is that in many countries – the UK being a notable exception - the burden of proof in situations of dispute is not legally reversed; and even if it is, in practice holders of EPIs find it almost impossible to bring forward counter-proof. Other problems relate to the failure to limit the liability of holders after notification and the absence of a specific dispute resolution mechanism. It is noted that most of the disputes brought to the attention of consumer organisations concern the liability of the holder c.q. the issuer in case of loss or theft of payment cards. Although the study does not explicitly recommend the introduction of a Directive, its overall stance is that there is still a substantial degree of non-compliance with the Recommendation.

This said, the study itself is not without its deficiencies either. For one, the executive summary is plainly deceptive as it simply lists all examples of non-compliance found without any qualification whatsoever (that is, without indicating how many countries are concerned, and whether or not it really presents a problem). The result is that the reader is left with an overly negative impression. Secondly, one of the goals of the statistical analysis was to determine "if significant relations exist between characteristics of EPIs, issuers and countries on the one hand, and their ‘performance’ in complying with the Recommendation on the other hand" (p. 13). However, nothing is said about possible reasons for non-compliance. Thirdly, the findings are based primarily on (qualitative) desk research performed by the researchers. Little use is made of the (small-scale) surveys of EPI holders – perhaps because the surveys were not representative anyhow (p. 12). Also disappointing is the input from contacts with consumer organisations. As the tables in Appendix 2 show, in most cases "no information was obtained from contacts with consumer panels". So clearly no "analysis of the profile and frequency of the complaints" (p. 9, Appendix 1) was performed. This in fact lies at the heart of my main criticism. What the study appears to have done well is a comparison of member state laws and contracts on the one hand and the Recommendation on the other hand. Ergo, the study does give the reader an idea of the current degree of (non-)compliance with the Recommendation. What the study fails to show in a decisive way is that the Recommendation has (or has not) improved the position of EPI holders. It does not demonstrate, for example, that the frequency and severity of complaints brought forward by EPI holders is lower in countries with a high degree of compliance, and vice versa.

The study therefore provides less guidance than one could have hoped for as to the question whether a Directive is really needed. I am not indifferent to the argument put forward in a recent working document of the DG Internal Market (2002, p. 6 and 9) that the increasing integration of the national payments markets also increases the need for a coherent common legal framework that would do away with the sometimes large country differences highlighted by the study. But that still leaves the question which topics should be included in the regulation and which issues do not need regulating. For example, the UK experience shows that the banks' internal dispute resolution mechanisms deal successfully with most complaints (p. 76) and that in a large number of instances

holders are not charged for pre-notification losses, even where the account terms permitted the issuer to do so (p. 77). The report also shows that providing extensive information - in compliance with the Recommendation - does not necessarily reduce the ignorance of holders (p. 12). Another difficulty is the evolution in technologies. The migration from magstripe to chip cards, for example, may have implications for the provisions concerning the burden of proof. Stronger still, the drafters of the Directive will have to free themselves from traditional card-based thinking and will have to make sure that the provisions are also suited for server-based wallets, novel Internet payment systems, m-wallets, etc.

The recent working document shows that the Commission is clearly aware of the latter problem. It explicitly states that the new legal framework "should cover payments or fund transfers effected by *any kind of EPI ...*" (DG Internal Market, 2002, p. 34; my emphasis). Stronger still, it states that "ideally, the provisions should be general enough to incorporate also the payment methods of tomorrow" (ibidem). As for the direction of the upcoming Directive, judging from the working document the Commission intends to focus on provisions related to the burden of proof, the liabilities of the holder and the issuer, and the means that enable the holder to notify the loss or theft of the EPI (and to obtain proof of such notification). The document has recently been made available on the Internet and the Commission is currently inviting comments.

[info]

- Study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment instruments and in particular the relationship between holder and issuer, May 2001
http://europa.eu.int/comm/internal_market/en/finances/payment/instrument/.
- Directorate General Internal Market, A possible legal framework for the Single Payment Area in the Internal Market, working document, May 7, 2002 http://europa.eu.int/comm/internal_market/en/finances/payment/area/index.htm
- Van Hove, L., E-money not ECLIPsed by regulation, ePSO Newsletter, Nr. 11, December 2001
<http://epso.jrc.es/newsletter/vol11/8.html>.

With thanks to Jean Allix for background information and to Knud Böhle, Clara Centeno, Malte Krueger, Simon Lelieveldt, and Arnd Weber for comments on an earlier version.

EPSO Newsletter – Issue 15, June 2002

Focus: South East European Transition Economies

[15&1]

Editorial: Payment Transition from the Balkans to the Dnjepr

Arnd Weber (arnd.weber@itas.fzk.de), ITAS, Karlsruhe, Germany

/electronic banking/mobile phones/debit cards/Bulgaria/Romania/Ukraine

Economic transition in South East European countries, in the 1990s, led to an increase in poverty for significant parts of the population, and to high inflation and bankruptcies of banks. More recent developments in the monetary sphere, such as high growth rates for banking services, must be seen against this background. This issue of ePSO-N focuses on monetary developments and emerging payment technologies in the region.

The Eastern European transition economies, including Russia, have about 340 million inhabitants. The European Union is currently conducting negotiations to integrate the most Western of these states. The EU also plans for the integration of about 66 million inhabitants of Turkey, Cyprus and Malta. In all, these are 22 countries to observe. What is the role and future of national and foreign currencies, of banking, and payments in all these countries? From a Western European point of view, it certainly makes sense to observe economic and monetary developments even in countries which will not join the EU in the next one or two rounds of accession, because it is essential that social conflicts be reduced. Certainly, monetary developments are part of the picture. A large share of the people have experienced crises of the monetary systems in the 1990ies, meaning high inflation, loss of savings, bankruptcy of banks, etc. Therefore, today, foreign currencies such as the US dollar or the Euro play a significant role to protect savings as well as for fixing prices despite inflation. In everyday life, cash plays a significant role in consumer payments, and even bills of the utility companies etc. are frequently paid in cash. If these economies continue to grow, the number of such cash payments will certainly diminish. Given recent experience, foreign currencies will likely continue to play a role in several economies, such as some former Soviet Union countries.

In the last issue of ePSO-N Mike Hendry pointed out that the lowest level of costs for fully automated bank transactions in the EU is in the range of 2 Euro-cents [14&3]. Such transactions will, however, only become that cheap if they are automated, i.e. if the account holder uses some electronic device to initiate the transactions, and if the giro system processes billions of transactions. End-user devices to handle them could be bank terminals, mobile phones, or PCs. Given that PCs cost an order of magnitude more than handsets, for Eastern Europe I would find the use of terminals or phones more likely. Given the high number of smaller transition countries, labour migration, and the use of foreign currency, a large trans-border network is obviously the best way to achieve economies of scale. This would not only give people a chance to hold local currency in a loss-tolerant and even interest-bearing way, even foreign currency could be handled. So much on long-term perspectives.

In ePSO-N 9&7 and 10&4, we reported on some developments in the Baltic area, with a focus on innovation in places such as Tallinn, Riga and St. Petersburg. This time we focus on the general situation regarding electronic banking and payments in the large countries of Bulgaria, Romania and the Ukraine. About one third to half of the population in these three countries are poor, even by local standards. To give you a general impression about the "connectivity": About one tenth (5-20 %) use products such as bank cards or mobile phones, while the number of PCs generally is smaller than the number of mobile phones (see ITU for details [info]). Note, however, that people often share Internet access via PCs at home, in offices and in public access points.

After difficult experiences in the 1990ies these countries are currently aiming at a more stable economic development. Ukraine brought its inflation down, and Bulgaria and Romania are reforming themselves and intend to join the EU.

Marian Hanganu, in an interview, describes his company's support for mobile banking in Romania. While a 200 Dollar phone usable for his new service is clearly aiming at more wealthy people, using an always-on connection and pricing per packet points into a cost-efficient direction. Also, transmitting in the 450 MHz spectrum provides a potential cost advantage as compared to GSM and might even be suitable for covering rural areas because it requires only relatively few base stations

[see 15&2]. Assuming economic growth, this could turn out to become something like i-mode for Eastern Europeans.

Bojidar Bojinov subsequently provides an overview of building a banking and card market in a transition economy such as Bulgaria. After the country accepted Western rules and players in 1997, the card market started growing at double-digit rates [15&3]. You will notice in his article that issued cards typically do not go with a credit to the card holder. Rather, banks opted to rely on on-line networks and deployed debit cards, initially for withdrawing cash from dispensers, increasingly for using POS-terminals.

While the majority of the population in both Romania and Bulgaria do not yet use bank accounts for payments, Stefanos Karapetsis reports about an attempt to provide stored value cards for unbanked persons. He envisages transactions on the Internet as a first step, even across borders. Read his report about EU-project Balcard [15&4].

The following article on Ukraine is based on input from local researchers who helped us understand the situation in this large country situated between Russia and the EU's Enlargement Countries. With the disappearance of the "coupons" following privatisation, and the Rouble crisis of 1998, currency competition is also here, though under the magic cap of "udelniye yedenize", see [15&5].

After having mentioned all these difficult topics, let me express my thanks to the friendly people from the Black Sea countries who made this focus possible.

In the remainder of the newsletter, Luigi Sciusco discusses how core competencies of banks can be maintained, while payment services are outsourced for cost reduction. He discusses that a clever way of "co-sourcing" by banks, niche operators and mobile phone companies is needed to avoid business being interrupted or partners going their own way and damaging business [15&6].

Leo Van Hove analyses a paper by Mathias Drehmann, Charles Goodhart and Malte Krueger about traditional cash. While Drehmann et al. point out that cash will remain in demand e.g. due to privacy reasons, Leo Van Hove argues that citizens might decide differently if cash were less subsidised and e-money bore interest [15&8].

As the ePSO pilot project has been completed, it is time to summarise what has been done during the past two years. Ioannis Maghiros recalls the major activities of ePSO, adding statistics demonstrating the success of this project [15&7]. It is also time for the editors of ePSO-N to thank all correspondents, to thank our readers and the ePSO management in Seville that enabled these 15 issues of an analytical and independent newsletter edited by ITAS.

[info]

- ITAS is conducting research in Eastern European countries. It has begun a co-operation with the United Nations/Economic Commission for Europe, on the issue of electronic payments in transition economies (see <http://www.unece.org/trade/entdev/internet/prog.htm>). Please contact Daewon Choi Daewon.Choi@unece.org or the author.
- For statistics, see e.g.:
Central Intelligence Agency: <http://www.cia.gov/cia/publications/factbook/>
International Telecommunication Union <http://www.itu.int/ITU-D/ict/statistics/>

[15&2]

Interview: Mobile Banking on Low-cost Networks in Romania

Arnd Weber (arnd.weber@itas.fzk.de), ITAS, Karlsruhe, Germany, talks to Marian Hanganu (mhanganu@ipacri.ro), Ipacri, Bucharest, Romania

/mobile Internet/mobile payment systems/digital signatures/Romania

The Romanian telecom provider Telemobil is deploying a CDMA2000 network in the 450 MHz spectrum. Transmission in this frequency means a reduced number of base stations, hence relatively low costs and suitability for rural areas. Due to the transmission in packets, the spectrum can be used for a relatively large amount of voice and data traffic. CDMA2000 as well as GPRS will be used to provide for fast mobile banking solutions.

Marian Hanganu is Marketing Manager for Ipacri Romania, an IT Consulting and Software Development company in Bucharest, Romania. Ipacri is owned by Elsag, Italy. Ipacri has developed a mobile brokerage solution for WAP. Currently the company is working on mobile banking solutions for mobile networks such as CDMA2000.

ePSO-N: *Mr. Hanganu, you are planning a banking solution for the CDMA2000 mobile communication technology. What is CDMA2000 all about?*

Hanganu: The technology has been developed by Qualcomm from the US. It is a technology which is a competitor of GSM. GSM is partitioning the frequency, CDMA is sending packages. The difference allows to run on frequencies which are lower than GSM frequencies and achieve higher speed. The frequency on which CDMA2000 is operating here is 450 MHz.

ePSO-N: *Is CDMA2000 already being used?*

Hanganu: There are already millions of subscribers to CDMA2000 in Korea. There were more than 8.7 million CDMA2000 subscribers worldwide at the end of April. In Romania, it is deployed by Telemobil, a relatively small Romanian operator, which has been acquired by Inquam, a Qualcomm company. Telemobil ran already an analogue 450 MHz service. In December 2001 they started a CDMA2000 service, under the brand name Zapp Mobile. They already have 30,000 users. Their service allows up to 153 kilobits per second, this is so-called CDMA2000 1X. It is a "2.5" generation technology.

Coverage is now about 56 % of the country. It is planned to be close to 90 % by the end of the year.

CDMA in Romania

In Romania, CDMA2000 uses the 450 MHz frequency band, as opposed to GSM which uses 900 MHz or more. In general, less information can be transmitted at lower frequency. With lower frequency, one needs, however, a smaller number of base stations. Furthermore, 450 MHz base stations are relatively cheap. With CDMA2000, the lack of bandwidth at 450 MHz can be addressed by sending packets for voice and data. Using CDMA with 450 MHz is a novelty. CDMA stands for "Code Division Multiple Access", while GSM is uses TDMA, which stands for "Time Division Multiple Access".

The approach is potentially important for fighting the digital divide in less well-off countries and in rural areas. In Romania, about 2000 villages do not have any fixed telephone lines. While it would be extremely expensive to wire all these villages, using wireless technology such as CMDA2000 to connect people in these villages might work (cf. Oaca [info]). If Telemobil succeeds, the technology "will spread like wildfire", as explained by Robert Horvitz, manager for Central/Eastern Europe, Global Internet Policy Initiative (GIPI). GIPI is a project aiming to unblock Internet development in places where there are still few users. [A.W.]

The CDMA Development Group (CDG) has reported that CDMA2000 1xEV-DV (data and voice) has been approved by both the Third Generation Partnership Project 2 (3GPP2) and the Telecommunications Industry Association (TIA) for publication, and has been submitted to the ITU for formal approval as a formal 3G standard.

As specified by the 3GPP2, CDMA2000 1xEV-DV will provide services at speeds of up to 4.8 Mbps. CDMA2000 1xEV-DV is backwards compatible with cdmaOne and CDMA2000 1X, providing wireless operators a seamless network evolution. Currently, there are more than 500 individuals working within various CDG subcommittees on cdmaOne- and CDMA2000-related matters.

ePSO-N: *Can you use a Zapp Mobile phone to exchange emails?*

Hanganu: Every user receives an email-address like yourname@zappmobile.ro. You can use any desktop email software and send a carbon copy to your phone. You cannot read attachments.

ePSO-N: *Can I have an always-on connection with Zapp mobile phones?*

Hanganu: Yes. You can also connect your telephone with your laptop. You can get very good speed. You can connect with Pocket PCs or PDAs. This is really great.

ePSO-N: *What sort of a phone do I need to use the CDMA2000 network?*

Hanganu: There are two models, the Hyundai 100 and a newer one, from Synertek, also a Korean company, the S 200, which is smaller and has a wide colour screen. Both are including MS Mobile Internet Explorer 3.0 for Web browsing.

There is a portal under development, where you can look for weather, news, etc. The always-on connection means that when you read information, or key in data, this does not cost you anything.

ePSO-N: *How does the price of a CDMA2000 telephone compare to a GSM telephone?*

Hanganu: For Romania it is not cheap. There are no other suppliers of hardware. The telephone costs about 200 \$, but the company is not charging this. The phone will cost the user 80 \$ or much less, depending on the contract. For example, you can buy a package which includes the Hyundai telephone and 30 minutes/month calls for free, with 70-100 \$ per telephone, but you can also chose another package which includes 175 free minutes, with 50-65 \$. For the first one monthly subscription is 15 \$ and for the second contract we talk about 35 \$. The prices for a one minute telephone call is comparable in the CDMA and GSM operating systems.

ePSO-N: *Does Zapp Mobile advertise their services by saying that the bill will be lower than with GSM telephony?*

Hanganu: They do not say so. But they say you get 3 cents for every incoming call. Yes, it is true, for every one minute incoming call you get 3 cents in your monthly invoice. This is especially very attractive for companies with many calls between the employees and for professionals who receive lots of incoming calls.

ePSO-N: *Can CDMA be used to supply Internet access to SMEs or schools in rural areas?*

Hanganu: Yes, the price is very good starting at 2 \$ per MB [I-mode in Germany costs 10 Euro per MB]. But for e.g. 500 MB they charge only 250 \$.

ePSO-N: *Will Romania remain an island of CDMA2000 at 450 MHz?*

Hanganu: In the US, there are plans for deployment during the year 2002. The 450 MHz bandwidth will soon also be used in China and Russia. There is interest in other European countries. Qualcomm is heavily buying unused frequencies, of 450 MHz, 800 MHz, etc. across the world, including in Western Europe in which 450 MHz is very uninteresting for other companies.

ePSO-N: *Let's now talk about payments. How many people have an account suitable for banking, in Romania?*

Hanganu: Romania has a population of about 22 million. About 2 million people have a bank account, I mean a bank account which is used, not a savings account. There are 2 million credit and debit cards.

ePSO-N: *If you think of an average citizens outside Bucharest, how do they pay for utilities, rent etc.?*

Hanganu: They pay to cash tellers of the utility companies.

ePSO-N: *Do you think the average citizen will have a bank account in a few years?*

Hanganu: The government is very keen to push people to open a bank account. The government considers imposing the rule that any retailer with a turnover higher than a certain amount should accept credit and debit cards. Many banks are building branches.

We expect a boom in consumer credit. There is only one barrier, the credit information. Credit information bureaus are missing. Our company is also part of an initiative which may lead to a credit information bureau. This is very important for mobile telephone operators. They have valid information about the habits of their customers – about 5 million people – and are looking to increase their activities. They are looking for the telephone to become the wallet.

ePSO-N: *Now, what's going on with mobile banking in Romania?*

Hanganu: We have experience with mobile brokerage, via Vanguard, a brokerage house in alliance with Connex, a GSM operator owned by Vodafone. Because of the low speed of WAP-based applications, users have not been very interested. There is not much mobile banking in Romania, apart some modest SMS based applications. So far mobile services have been too slow for users. For example, we have developed a mobile brokerage application based on WAP. According to Connex and Vanguard the application generates rather modest traffic. We have investigated this and the main reason is the slowness and the costs of WAP transmissions. Wireless applications are becoming much more interesting with the speed of CMDA, or GPRS, which is also already in place in Romania. We can build richer applications that will run faster due to the new technologies. Currently, as the retail banking market is booming, banks have interest in finding news channels.

ePSO-N: *What exactly are you planning to deploy for mobile banking?*

Hanganu: In mobile banking, security is an issue. So we started to develop a technology called mSignature. It allows any mCommerce application to use digital signatures.

ePSO-N: *Why is it not enough that a telco or a bank simply verifies a user's password?*

Hanganu: It is not trustworthy enough. Banks say that only digital signatures will be accepted in court.

Last year the Parliament approved the law on electronic signatures. Our company is co-operating with the Italian company SIA to establish the first certification authority in Romania. We plan to launch secure mobile banking. We will also offer to any other provider to use digital signatures in their applications.

ePSO-N: *What has been missing in GSM security?*

Hanganu: You can make secure mobile banking with GSM if you use SIM applications or if you have WAP browsers with WTSL, but you cannot escape from the slow environment. With mSignature you can have digital signatures with WAP phones, but it will run slowly. Or you can do SMS-based mobile banking, which is already in place in Romania, but this is not the road to go on.

Mobile banking needs to be designed for people who are very busy, to pay rent for cars, for utilities, water, gas, without locking him or her to a SIM or an operator.

ePSO-N: *Which hardware will do the signing in the new approach?*

Hanganu: The technology is based on a proxy that will sign the data. The proxy will also authenticate the bank to the user and vice versa. It is not a solution which is beyond criticism. Current phones do not allow to handle signatures. We are looking for new telephones which have more functionality and memory. In the current situation, with many different types of phones, the only solution to deploy mCommerce software rapidly is not to store the digital certificate and the secret key on the telephone. The proxy can get orders from CDMA phones which use the Mobile Internet Explorer 3.0. The proxy will also be able to communicate with GSM/GPRS and communicate with WAP in WML. Anyway, even in the future, users might not want to keep their signing key on a device subject to be lost or stolen.

ePSO-N: *Does it mean that the user has to use a password?*

Hanganu: Based on the password the encrypted key on the proxy will be decrypted and used to sign. The proxy will also identify the telephone using information from the operator.

ePSO-N: *Do you also have plans for payments via mobile phone at the point of sale?*

Hanganu: No, there are no such plans. We studied the issue but we are not optimistic due to the number of agreements that any option will require with the banks, mobile operators, retailers and representatives of Visa and Mastercard.

What has been done is to transmit data from EFTPOS-terminals to the banks. Another company is selling POS-terminals connected to the banking network through Telemobil phones. In Romania, the fixed telephone is not so well developed, so going mobile makes sense.

ePSO-N: *Do you see any chance that your mobile banking solution will be used to pay for e-commerce purchases on the Internet?*

Hanganu: Mobile banking cannot be used to pay for e-commerce directly. To pay for e-commerce you should be able to see the web site and act on the Internet. You can do this with Zapp and you could give your details if you want but not from an m-banking application. However, I doubt that users will choose the small screen of the telephone to buy from the Internet.

ePSO-N: *But you could also send a payment order via mobile phone to an Internet merchant. Would this make sense?*

Hanganu: This would make sense, the merchant could obtain the payment. But nobody is implementing this today. We have plans for such an e-payment application.

ePSO-N: *When will your mobile banking system go live?*

Hanganu: Before the end of the year. The software is ready. The banks are very interested to see reliable security. We forecast that all bureaucratic procedures will be over by the end of the year.

We are partnering with Microsoft because the mobile banking solution is developed in .Net technology. We will have a public presentation of it on June 19 in a conference organized by Microsoft Romania.

ePSO-N: *Thank you very much!*

[info]

- Cellular News: <http://www.cellular-news.com/cgi-bin/database/archiveresults.cgi?week=180>
- CDMA2000 is reported to have 9 Mio. Subscribers world-wide (April 2002), mostly in Korea, cf. CDMA Development Group: http://www.cdg.org/world/cdma_world_subscriber.asp#cdma2000chart
- Global Internet Policy Initiative: <http://www.gipiproject.org/>
- Ipacri Romania: www.ipacri.ro
- Oaca, Nicolae: Alternative telecommunications infrastructure in Romania. IEEE International Conference on Telecommunications 2001. <http://members.fortunecity.com/teleactivities/sessions2.htm> [pdf-file currently unavailable, you may contact nicolae_oaca@yahoo.com]
- SIA Certification Authority: <https://ca.sia.it/home/>
- Zapp Mobile: <http://www.zapp.ro/> ; for info about the handsets see:
<http://www.zapp.ro/offer/phones/hyundai/>
<http://www.zapp.ro/offer/phones/synertek/>

[15&3]**Evolution and Present Status of Bulgarian Card Market**

Bojidar Bojinov (bobi@uni-svishtov.bg), Tsenov Academy of Economics, Svishtov, Bulgaria

/payment cards/Bulgaria

Bulgaria is a small South-eastern European country with a population of 8 million inhabitants in economic transition. During the bank crisis (1996-97) about 1/3 of all banks went bankrupt. On 5 July 1997, the Bulgarian government, jointly with IMF, introduced the Currency Board Arrangement, which lead to economic stabilization and growth. During the last four years the Bulgarian card market has expanded rapidly. The article reviews the evolution and the present status of the Bulgarian card market.

The first trials to introduce cards in Bulgaria and to establish national card networks were made by three private banks. After 1992, the First Private Bank, the TouristSportBank, and the BalkanBank started their own networks; the first two based them on cards with a magnetic strip, while the BalkanBank used smart cards.

During 1993, the Bulgarian National Bank (BNB) decided to establish Borica Ltd. (100% owned by BNB) to develop a new, commonly used national card network, as well as to play the role of a national card operator and acquirer. The actual start of card payments through Borica (Bank Organization for Payments Initiated by Cards) was in March 1995 when the state-owned United Bulgarian Bank started to use the system's services. In the same year, several, primarily state-owned banks, the Bulgarian Post Bank, Bank DSK, First Investment Bank, Credit Express Bank, and the International Bank for Investments and Development, as well as BNB (which issued cards only for its employees) joined the system.

In 1995, BNB published Regulation 16 on Payments Initiated by Bank Cards. According to it, only banks can issue debit or credit cards and the card payments authorization can be made only by the national card operator Borica. Four parallel card systems have been working in Bulgaria until 1997. During the bank crisis from 1996 to 1997, First Private Bank, TouristSportBank and Balkanbank, as well as other banks, went bankrupt. Therefore, from 1997 until present, Borica has been the only functional system for card payments in Bulgaria.

In June 1997, to decrease the high rate of inflation and to stabilize the bank system, the government introduced a Currency Board Arrangement. The amount of banknotes and coins has been limited to "the lev equivalent of the gross international foreign exchange reserves" (Article 18 of Law on the Bulgarian National Bank). The Bulgarian lev has been fixed at the exchange rate of 1 BGN = 1DM (1,955.83 lev to one Euro). In this way, BNB is limited in its monetary policy, the only instrument of monetary policy is the change of minimal reserve rates. After the introduction of the Currency Board, the Bulgarian economy stabilized. The increases of average monthly salaries are from 24 US dollars in February 1997, during the bank crisis, to 107 US dollars in December 1997. This increase affected the cards market development. The number of cards and transactions increased rapidly (see Table 1).

In parallel with the increase in numbers of issued cards, the volume of transactions also increased – from 26.5 million levs in 1999 to 1.28 billion levs in 2001. In 2001, bank cards were primarily used for withdrawals (93,13% of all transactions), while POS payments were only 5.35%, and 1.52% are Internet transactions and payments via telephone. The average sum withdrawn is 80,65 lev (41.23 EUR), close to the minimum salary, and 129,01 BGN (65.96 EUR) for POS transactions.

Table 1: Bulgarian card market – selected indicators

	1995	1996	1997	1998	1999	2000	2001
ATMs	23	69	118	162	279	420	642
POS-terminals	1	27	72	352	497	1,087	1,980
Debit and credit cards	381	19,362	62,733	105,432	270,929	560,934	990,414
of which credit cards	0	0	19	437	1,417	3,332	10,868
Transactions				2,009,701	3,525,699	7,195,350	15,422,497

Source: Borica Ltd.

In the last years Bulgarian employers have started to pay wages into bank accounts in order to decrease their costs for wage payment. This process provoked a new phenomenon – queues behind ATMs when employers transfer wages. This is a result of the typical cash-oriented payment culture in Bulgaria, the high percentage of the shadow economy, as well as of the policy by Bulgarian banks in the card payment area. The banks' policy is to issue new cards and to expand the existing ATM network. In this way, banks attract new, low-interest rate resources (banks pay 1-3% p.a. on card accounts), and increase income by fees (issue, account's service, withdrawals, monthly statements, etc.). At the same time, the POS network is high concentrated in the major cities, a significant percentage of these terminals are even used for withdrawals in bank branches.

In April 2002, Bulgarian banks offered five types of cards:

- domestic debit cards "BORICA" (in BGN): 1 million cards issued
- international "Maestro" debit cards (in BGN): 181,000 cards
- domestic and international "Visa Electron" debit cards (in BGN or USD): 28,000 domestic and 8,000 international cards
- international "Eurocard/Mastercard" credit cards (in USD): 9,000 cards
- international "Visa" credit cards (in USD): 3,500 cards

Some banks offer American Express and Diners Club cards, but information about the number of issued cards is not available.

The low share of credit cards is a result from the requirements, which are too high for Bulgarian living standard: 30-90 USD fee for issue/service, and a deposit of 1,000 – 10,000 USD. The Bulgarian banks prefer to issue credit cards which are denominated in foreign currency, primarily in USD. The cardholders can use a credit line of about 90-95% of the deposit, at 12-18% interest rate, while the bank pays an interest of 3-4 % for the same deposit.

During the summer of 2001 some Bulgarian banks changed the base requirements for credit card issuance. The First Investment Bank started to issue EC/MC credit cards (in BGN and in USD) without an initial fee and deposit, as it requires by cardholders to keep 400-1200 BGN as minimum deposit. After few months, United Bulgarian Bank (since the year 2000 owned by National Bank of Greece and the EBRD) started to issue similar cards. Although the initial requirements for these cards are higher than international debit cards (free issue, 2-20 BGN minimal initial deposit), they are very attractive (more than 13,000 cards issued in April 2002), because they are accepted worldwide.

The starting point of Internet card payments in Bulgaria is the emergence of ePay.bg – an electronic payment system, developed by Datamax. The system allows cardholders to use cards for payments of goods and services at Bulgarian Internet shops. During 2001, 24,754 transactions were made through ePay.bg. Through the system consumers can exchange data with home banking and accounting systems, as well as make on-line applications for domestic debit cards, conduct standing orders, pay bills, make payment orders, request digital certificates, and conduct phone banking (ePay Voice).

As a conclusion, competition in the bank sector leads to a decrease in prices, to a rise of quality of services, to the introduction of new products, and to the expansion of ATM and POS networks. In spite of the economic difficulties of the country during the last 12 years, in the area of card payments, Bulgaria is already a European country. Let us hope that also the Bulgarian living standard will come closer to the European one soon.

[info]

- Bojinov, B.: "What Bulgarian banks offer via Internet: an overview". In: Finance (proceeding of 50th Anniversary Financial Conference, Svishrov, Bulgaria, 11-12 April 2002), (Veliko Tarnovo), pp. 883-888.
- Bojinov, B.: Electronic Money. 2000 (Veliko Tarnovo) [in Bulgarian]
- Bojinov, B.: Electronic Money and Currency Board: the Case of Bulgaria. RSS Grant 1147/2000. <http://www.uni-svishrov.bg/bojinov/rss/rss.htm>
- BORICA Ltd., Sofia 1000, 117 Tsarigradsko Shouse Boulevard.
- Bulgarian National Bank: Payment System in Bulgaria. 2002. <http://www.bnb.bg/bnb/home.nsf/fsWebIndex?OpenFrameset>
- Bulgarian National Bank: Monthly bulletin, 1999, N1. [http://www.bnb.bg/bnb/home.nsf/vPages/periodic_bulletin_1999_01/\\$FILE/EBUL01.pdf](http://www.bnb.bg/bnb/home.nsf/vPages/periodic_bulletin_1999_01/$FILE/EBUL01.pdf)
- Datamax: www.datamax.bg

- ePay.bg: www.epay.bg
- First Investment Bank: www.fibank.bg
- Law on the Bulgarian National Bank. In: National Gazette, N 46, 10 June 1997
[http://www.bnb.bg/bnb/home.nsf/vPages/Laws_BNB/\\$FILE/LBNB.PDF](http://www.bnb.bg/bnb/home.nsf/vPages/Laws_BNB/$FILE/LBNB.PDF)
- Matrozov, Al.; Kostov, Hr.: "BORICA: What has been achieved and what must be done", in: Bank information technologies magazine, 1996 [in Bulgarian]
- Regulation 16 on the Payments Initiated by Bank Cards, National Gazette, N28, 28 March 1995.
<http://www.bnb.bg/bnb/home.nsf/vWebPagesByCategoryEN/5B46E6BF2D490C26C2256B50004AAF9F?OpenDocument&count=-1&EN>
- Todorova, G.: BORICA's first steps are too slow. Capital weekly, 19/1995, 15 March 1995 [in Bulgarian]
- United Bulgarian Bank: www.ubb.bg

[15&4]

EU-funded Balcard Project: Targeting the Unbanked Internet Buyers

Stefanos Karapetsis (s.karapetsis@mellon.com.gr), Mellon Technologies, Athens, Greece

/smart cards/standards/electronic purse/cross-border payments/Bulgaria/Cyprus/Greece/ Romania

Balcard, a European Union IST demonstration project, aims at providing unbanked Internet users with a payment means based on a smart card electronic purse. Including one EU country, Greece, and three non-EU, Romania, Bulgaria and Cyprus, it will address cross-border low value transactions clearing and settlement issues. Using dominant specifications, like CEPS and Finread, Balcard has to resolve some technical and operational issues.

The consortium is made up of three banks, Eurobank (Greece), Postbank (Bulgaria) and Bancpost (Romania), two interbanking organizations, Borica (Bulgaria) and JCC (Cyprus), and two technology partners, SchlumbergerSema (France) and Mellon Technologies (Greece), who is co-ordinating the project. The project started in February 2002 and is scheduled for a duration of 24 months.

The idea is fairly simple: In order to facilitate e-commerce in and between countries like the ones in the Balkan region (hence Balkan Card = Balcard), a payment instrument has to be provided to those Internet users who have neither a credit card nor a bank account. For several reasons credit card penetration in transition countries is extremely small and growth rates are strongly linked to those of their economies, that are picking up rather slowly. At the same time Internet penetration is growing, and the corresponding number of Internet users is larger than in EU countries, since users, and especially young people, share PCs in Internet cafes or academic institutions. Figures on some Eastern European countries' payment systems, including Bulgaria, are in the current issue of ePSO-N [15&3].

Furthermore it is assumed that cash is used for smaller value purchases, i.e. for soft goods and services or hard goods like books. Therefore Balcard is a test of these assumptions.

The selection of stored value smart cards as a means of payment was made in anticipation of two major evolutions: the objective of project DUCATO was to prove the technical specifications of CEPS, and since payments had to be in multiple currencies and there were no key-management restrictions, CEPS was the best vehicle. As a matter of fact just before Balcard kick-off, DUCATO delivered its final reports with a full proof of the CEPS specifications.

Second evolution was the PC connected readers. One aspect was their diminishing price (around € 10 each) and another was their security. Finread had already successfully completed its standardization activities and the prospects of a universal secure card reader are being dealt with in the eEurope Smart Card initiative (TB4, see [info]).

So, the objective is to put things together, make them work and evaluate if the model is well accepted by all stakeholders: consumers, e-tailers and financial institutions.

Since the project workpackages are under-way and will be published on our website [info], one cannot yet publish any final finding or decisions. There are some points though that have been discussed and are worth mentioning in this issue of ePSO-N.

One decision made is that Balcard will differ from CEPS in two ways: *loading will be made in principle off-line with un-linked accounts*. I.e. card-holders will pay cash to bank branches or selected outlets and loading will be done manually. This does not exclude the option of loading on-line, to a linked account, but the initial objective is to involve several thousand consumers (during the pilot) that do not have a bank account.

The second decision is that *all purchases will be made on-line, on the Internet*. So in a sense CEPS is being reversed, since its basic concepts are based on off-line purchases and on-line loading. This is not an innovation, i.e. pre-paid smart cards such as Proton, Mondex and other e-purses can be used to make Internet payments. One Dutch company based its business case on providing this type of services and technically has started the operations successfully. Unfortunately the slow take-up of e-commerce forced the company to cease operations, before using CEPS. Similar uses are claimed in Singapore from NETS.

But when the technical issues are resolved three other issues will be addressed: Micro-payments, cross-border clearing and the level of trust.

The e-tailers that will participate in the pilot will be mostly selling soft goods and services. This is relevant to lower value sales, like music, articles, software and so on. So we will be expecting an interest from their side. The pay-per-use feature of CEPS – like ticking with phone units, will also be tested.

Cross-border clearing and settlement has a technical and a legal aspect. Technically it will be most probably resolved through traditional channels. In DUCATO both Europay and VISA cleared and settled cross-border CEPS based transactions with no problem whatsoever. The legal aspects of cross-border transactions, especially in countries with a very high percentage of the grey economy, pose some challenges that will be faced.

Finally the trust issue has to do with the Internet purchases problems: what happens if the soft good that one has just paid is useless? Can one get one's money back? How can one claim that a physical good has not been delivered? Some detailed work on the existing protocols has to be made, in order to arrive at a level of trust that will satisfy all parties involved.

One final encouraging development for Balcard is the trend to use smart cards with PKI for secure access and digital signature on the Internet. Countries like Finland and Italy are moving to larger scale projects with the aim of national roll-outs. This makes life easier for card based e-purse payments, since the readers will already be installed.

All partners see Balcard as a prelude to a commercially exploitable scheme. With no illusions about the face-to-face e-purse business case, the partners do believe that they could eventually move to the physical world, since the CEPS cards could also be normal debit/credit EMV cards. There is big mobility of the working population in border areas between Balkan countries, where the Euro is the real hard currency. But the overall investment for the use of Balcard on the Internet is relatively small and really demand driven. The business model has not been finalized yet, but, depending on the results we expect that the stakeholders will wish to invest in the scheme.

[info]

- Balcard: <http://www.balcard.org/>
- eEurope Smart Card: <http://eeurope-smartcards.org>

[15&5]

Ukraine – From "Specific Units" towards Electronic Payments

Arnd Weber (arnd.weber@itas.fzk.de), ITAS, Karlsruhe, Germany

/debit cards/Internet/mobile phones/Ukraine

The article first sketches the state of the Ukrainian economy and mentions some of its problems, such as the use of barter or the unofficial use of the US dollar. Subsequently, an overview is given of the use of payment cards, of the Internet and of mobile phones. Though large parts of the population are poor, there are already millions of inhabitants using such modern instruments. Even the use of mobile banking is starting.

"Stumbling our way home across unsecured ditches, we enter a mysterious unlit city which sinks into the black night. On the corner, near the unlit town hall, there is something bright blinking at us out of the gloom. What is beckoning us home turns out to be a cash dispenser." (Badische Zeitung).

Until 1991, the Ukraine was part of the Soviet Union. After Russia, the Ukrainian Republic was by far the most important economic region of the former Soviet Union. Its versatile heavy industry supplied unique machines, e.g. vertical drilling machines and aircraft. After the end of the Soviet

union, the terms of trade deteriorated significantly within a short period of time. Russia asked Ukraine to pay world market prices for gas. The dependence of the Ukraine on Russia for its supply of energy and a lack of major structural reforms made the Ukrainian economy vulnerable to external shocks. Ukrainian economic policy has been criticised as being erratic and for not providing a stable environment regarding taxation and legislation. In the Ukraine a small group of newly rich families now owns a significant part of the economy. Furthermore, accusations of corruption and money laundering have been frequently made. The result is that the Ukraine likely suffered the largest decrease in gross national product of all Eastern European countries. Until 1999, the output of the Ukraine fell to 40% of the output in 1991. The gross domestic product grew by 6% in 2000 and a growth of 9% is estimated for 2001. Ukraine has about 49 million inhabitants. Half of its population is estimated to live below the poverty line, subsisting from gardening etc. The Ukraine is a member of Commonwealth of Independent States.

Money and Payment in General

In 1991, Ukraine started issuing "coupons" as its national currency. Between 1992 and 1993 there was hyperinflation, partially attributed to the Russian central bank. This inflation eliminated almost all monetary savings and destroyed trust in storing Ukrainian currency. In 1996, the coupons were replaced by a new currency, the Hryvnia. The next blow to the monetary system was caused by the crisis of the rouble in 1998. However, a significant part of the economy either uses barter, or is taking place in the black economy. Russian gas is only paid for partially. Official inflation is 6% (2001).

Savings are kept in US dollars. All sizeable private transactions (e.g. buying houses, cars or furniture) take place in dollars as "specific units" (udelniye yedenize), since direct mention of dollars in contracts, shop displays etc. is prohibited. Denominating prices in dollars may lead to prosecution by the Militia.

Payment Cards

The number of payment cards doubles each year and has now attained the figure of 2,700,000, mostly debit cards, such as Maestro. The "Privatbank" is the leading card issuer. There are currently roughly 1,400 ATMs and 12,000 POS terminals.

Internet

In the Ukraine, the Internet is only used by about 750,000 households. During the last two years, the number of Internet users in the Ukraine has trebled. The high costs for access and PCs are a major barrier to the diffusion of the Internet. There are firms offering a new type of access to the Internet in the Ukraine known as the Webcard, which is similar to a prepaid phone card with an access number and a PIN to access the account. The e-Commerce market is in its embryonic phase. The Ukrainian VABANK is preparing the issuance of VISA Virtuon virtual cards for internet use.

In April 2001, the "Privatbank" started an Internet Banking System, Privat-24. Companies can make bank transfers (in Hryvna or foreign currency) via Internet Banking. Private persons can make money orders with Privat-24.

Mobile Telephony

Two leading mobile telephone operators have dominated the market during the past few years: UMC (Ukrainian Mobile Communications) und Kyivstar. In the year 2000 there were ca. 600,000 customers, at the end of 2001 there were already 1.6 million. 50-60 % of these phones are prepaid. A problem is that there are not sufficient new users for the required revenue to offset money invested in the networks. This situation makes it impossible for the operators to pay for the required extensions from current revenues. Experts assume that some providers recruit more customers than the network can accommodate. The problem arises because many customers prefer a prepaid package deal to keep costs low and to use the mobile telephone only in emergencies.

In the field of mobile banking, first approaches were made last year:

- "Kyivstar" and "Privatbank" launched a common project in mobile banking. A customer of "Privatbank" and "Kyivstar" can pay bills by means of SMS messages. In order to use this

service, the customer has to apply for the "Privatbank's" "Starcard" (VISA). The owner of a "Starcard" sends a message with the transaction sum to a target address using his mobile phone, then receives a confirmation from the bank upon which the transaction can be completed.

- The "VABANK" also provides its customers with the opportunity to effect transactions with the help of their mobile phones.

Conclusions

Among about 50 million inhabitants, a few millions have become wealthy enough to use new means of payment, the Internet and mobile telephony. For these customers, in principle similar innovative technologies are deployed as in Western countries. There is a tendency to use debit cards, or even prepayment, in order to avoid credit risks of any kind.

[info]

- Badische Zeitung June 9, 2001
- CIA World Factbook 2001: <http://www.cia.gov/cia/publications/factbook/>
- Privatbank: <http://www.pbank.dp.ua/ar/eng/index.htm> ; <http://www.privbank.com/info/index1.stm> [in Ukrainian]
- Ukraine Europay International Member Bank Association: <http://www.ema.com.ua/> [in Ukrainian]
- Ukrainian News: <http://www.ukranews.com/eng/>
- U.S. Department of Commerce: <http://www.bisnis.doc.gov/bisnis/isa/011114card.htm>
- VaBank Visa Virtuon card: <http://www.vabank.com.ua/cards/private/virtuon.html> [in Ukrainian]

The author wishes to thank Igor Eremenko, Brigitte Schulze, Olena Shvartsburg and an anonymous expert. This article is based on their input.

[15&6]

I-Payments Strategies

Luigi Sciusco (sciusco@tiscalinet.it), Rome, Italy

/Internet payment systems

The ePSO project explored the multi-faceted world of Internet-payments but we still lack clear and accepted business models and technical standards. This article outlines possible scenarios for I-payments evolution. It is concluded that a clever way of "co-sourcing" by banks, niche operators and mobile phone companies is needed.

Maximising revenues is the main goal of a financial institution. Apparently, I-payments (Internet-payments) do not have this feature and this is one of the reasons for the poor success in building critical mass for online micro-payments solutions. There are other factors that the ePSO Newsletters and Background Papers explored in these months: payment habits, technical complexity, privacy and/or authentication issues, delivery against payments (payment and delivery of goods/services are assured), easy and quick means to pay, cost.

I don't believe that I-payments schemes are solutions in search of a problem. In my opinion, financial institutions fail when they try to approach I-payments using their "standard" business model.

Payments revenues are under attack and this is mainly due to regulatory pressures, niche operators that position themselves only on high revenues products, and decreasing switching costs that allow customers to ask for more convenient prices and services. If banks and associations react to this threats applying their "general purpose" strategy to I-payments, they will generate monsters (e.g. SET): I-payments-strategies are needed. In the eighties IBM tried to manage the personal computing business with its usual, mainframe targeted, marketing and technical structure. In this way IBM paved the way for Microsoft and lost its leadership in information systems. Today banks are running exactly the same risk.

I will try to sketch some points that could be useful to define I-payments strategies. I-payments need critical mass and banks are not in the best position to invest resources in this sector because, as mentioned, they are going to reduce their revenues deriving from payments. There is a business sector where there is the opposite situation: wide customer base, impressive revenues, technical skill. This is mobile telephony. Operators can, in my opinion, use revenues from telephone traffic to cross-subsidise

I-payments that, at present, are unprofitable. Why should they do this? They cannot do the job that bankers did for centuries but they understand that payments are at the heart of customer relationship management. And they could use banks as utility providers, mainly for clearing.

As a consumer, I just want online services that are i) secure, ii) convenient to initiate and use, iii) available at appropriate cost, regardless of the provider (mobile operator, bank, new entrant). These are the critical success factors of PayPal. PayPal respects the three key consumer requirements and has succeeded in creating a critical mass with more than 12 million customers. Now PayPal is moving to more profitable customers, from person-to-person to consumer-to-business and even business-to-business payments. My only concern regards security. I believe that regulators should give some form of transparent assurance about I-payments schemes: PayPal does not transfer bits, it transfers money.

If I were an operator, I would need to manage effectively payment costs and outsourcing could be the solution. Again banks should not refer to their usual outsourcing business practices. Payments are a strategic asset and I-payments have a high potential to drive revenues in the future. Outsourcing should not be confused with offloading: banks should not walk away from the core I-payments. I-payments pose new challenges as well as a need for much more integrated partnerships. I-payments demand for a lot less "out" in outsourcing and new rules, focusing more on relationships rather than mere transactions. Control and flexibility are key drivers, with the "traditional" cost reduction, when evaluating outsourcers' proposals. I think that "co-sourcing" between banks, niche operators and mobile phone companies, is the only possibility for banks to survive in I-payments. When IBM tried to do this (do you remember the IBM/Microsoft partnership to develop OS/2 vers.1.3?), Microsoft was already aware of its power and decided to discard IBM and follow the market needs by distributing a simple DOS product (Windows 3.0) instead of a new operating system (OS/2 1.3). Banks must be extremely flexible to avoid that a new, visionary, Mr. Gates puts them apart with a business and technical model for I-payments that is innovative, simple, oriented to market needs and not to bankers' legacy systems.

[info]

- ePSO database on ePayments: <http://epso.jrc.es/>
- The Boston Consulting Group: Global Payments 2002. <http://www.bcg.com>
[Report can be found under "media center", "our practice", "financial services"]
- Deloitte & Touche: Technology trends, Fall 2001. <http://www.deloitte.com/dt/cda/doc/content/fall01techtrends.pdf>

**[15&7]
ePSO Final Report**

Ioannis Maghiros (ioannis.maghiros@jrc.es), IPTS, Seville, Spain

/ePSO/European Commission

An ePSO project report is presented that describes all key development steps and results obtained, demonstrating that the electronic Payment Systems Observatory (ePSO) project has achieved its stated objectives. This report will present a brief summary of all major events organised and of all deliverables produced.

Set-up and Operation of the Electronic Payment Systems Observatory Pilot Project

ePSO is a Shared Cost Action awarded to the IPTS from the Enterprise Directorate General as part of the ISIS programme (Information Society Initiatives in Standardisation) call of 22 May 1999. The project started on May 17, 2000 and was completed after 24 months. The *primary objective* of ePSO was to enhance the information exchange in the field of e-payment systems and thus contribute to promoting e-commerce in Europe. In order to achieve this objective, ePSO set up an *electronic discussion Forum* of relevant actors and experts and facilitated a *systematic exchange of strategic opinions* – across borders and across sectors – with a view to assist standardisation and to keep regulatory bodies in step with the evolution of underlying technologies. The project foresaw as well the creation of a *Steering Group*. Mrs. Christa Randzio-Plath, Member of the European Parliament, and President of its Economic and Monetary Affairs Committee, kindly accepted to chair the Steering

Group. The Steering Group was the guiding force of the Observatory; its impartiality, transparency and openness were intended to bring forth the support and confidence of all concerned.

A number of IPTS staff were assigned to the various tasks of the project from its beginning. They were involved, in leading, managing and executing various operations (including support activities on the web, secretarial support, etc). The CEN/ISSS virtual partner was also involved since the very beginning in an advisory role. With the help of staff from ITAS (Institute for Technology Assessment and Systems Analysis, Karlsruhe Research Centre), the main sub-contractor responsible for the production of the ePSO-Newsletter, a network of experts to contribute to the project was also set-up, the "correspondent network". A number of experts on financial issues external to the Commission that would be able to support it in its Observatory activities from the IPTS premises in Seville were also selected.

Steering Group

The Steering Group was created to become the guiding force of the Observatory; a structure intended to boost the support and confidence of all concerned. As a consequence great care was exercised in selecting its members so that its impartiality, transparency and openness in decision-making were assured. After a series of both informal and formal interactions, Mrs. Randzio-Plath kindly accepted to chair the Steering Group. The Steering Group consisted of financial industry market players, expert consultants, academics, representatives of standardisation, retail, telecommunications operators and consumer protection bodies at a European level, and the relevant Commission services.

The first meeting of the ePSO team and the Steering Group members was held in Brussels on June 15, 2000 where they discussed the project organisation, content scope, and initial deliverable list. They were also presented with a draft version of the ePSO-Newsletter by its editor, Michael Rader of ITAS. The second meeting of the Steering Group (21 participants) took place in Brussels on 22/11/2000, during which the strategic and technical background paper was presented and discussed. The third Steering Group (22 participants) meeting took place in Brussels on 22/5/2001 and the findings of the recently completed background papers 2, 3, 4 on M-payments, I-payments and Payment Culture, were presented, discussed and particular issues deserving further debate were addressed. The fourth Steering Group meeting took place in Brussels on 10/10/2001 and background papers 5 and 6 on E-money and PKI security technologies were presented and discussed.

ePSO Web Site

The ePSO team also developed and operated a web site that was used primarily to disseminate the entire information collected and produced by the ePSO team. The ePSO web site, located on the IPTS web server (<http://eps0.jrc.es/>) has been operational since August 2000 and both its content and appearance were renewed during August 2001. Table 1 presents the total number of hits per month, average number of hits per day, the number of distinct pages downloaded per month and finally the number of distinct visits per month during the 20 month period the ePSO web site has been operating.

Table 1: Web Statistics

	Number of hits per month	Average number of hits per day	Pages per month Downloaded	Number of visits per month
August 2000	7846	253	3010	
September 2000	3390	113	1304	
October 2000	9776	315	3567	1050
November 2000	6961	232	3240	956
December 2000	10918	352	4871	1292
January 2001	17146	553	7118	1958
February 2001	16130	576	7263	2055
March 2001	17998	580	7325	2264
April 2001	30540	1018	12070	3190
May 2001	27733	894	10439	3293
June 2001	34958	1165	12845	4336
July 2001	39567	1276	14195	5255
August 2001	38537	1243	13579	4690
September 2001	70439	2347	15736	4689
October 2001	116078	3895	19823	6955
November 2001	134559	4485	23626	7574
December 2001	90405	2916	19592	6526
January 2002	112320	3623	21980	7845
February 2002	128062	4573	26216	7927
March 2002	127164	4103	27794	7703

The ePSO web site provides access to:

- (a) the detailed project description, related events and selected links;
- (b) the ePSO-Inventory, a structured and searchable information source which consists of a data base of B2C e-payment systems and a bibliographical database on e-purses;
- (c) the ePSO-Forum archive;
- (d) all issues of the ePSO-Newsletter;
- (e) the ePSO Background Papers.

ePSO Inventory

As part of its objective to become a reference point for discussions between all actors involved in electronic payments systems in Europe, ePSO started to build a database on electronic payment systems, related projects and initiatives. The geographical scope of the data base is Europe, but relevant activities outside Europe are also taken into account in a selective way (e.g. innovations). Its focus is on payment systems, but the scope has been broadened by integrating relevant interoperability, technical and/or strategic initiatives (e.g. EMV, PACE, WAP). European Commission funded projects and initiatives are also analysed. The Inventory is searchable through a keyword interface, through free text search as well as alphabetically. More on the Inventory may be found in the analysis paper written for this purpose at <http://epso.jrc.es/Docs/Backgrnd-9.pdf>.

In addition, and again trying to achieve the objective of becoming a reference point on electronic payments, a data base on e-purses was presented through the ePSO web site. Professor of Economics at the Free University of Brussels, Leo Van Hove, a specialist in monetary policy and Internet economics has compiled and is maintaining an extensive, annotated list of links and references about electronic payment systems world-wide, especially electronic purses. The ePSO team developed a special database at the ePSO web site that adds value to Leo Van Hove's work through its sophisticated search features. The bibliography may be accessed at <http://www.jrc.es/cfapp/leodb/recent.cfm>.

ePSO Newsletter

ePSO-N, the Newsletter which was developed, produced and edited by expert staff of ITAS, the ePSO team and an international network of correspondents, delivered thorough and timely analysis of issues

in order to stimulate and structure discussion. ePSO-N was an important means of information and communication to achieve the ePSO project objectives. Three attributes characterised ePSO-N: (a) it was not an isolated publication effort, but was embedded in the context of a European Commission project; (b) it focused on e-payment systems with an eye on their use on the Internet and was thus more specific than many other e-commerce related publications; (c) it was co-produced by an international network of correspondents.

As payment cultures in Europe and world-wide vary greatly and as ePSO-N was to cover a broad area of issues, the expertise of the correspondents network proved valuable. The development of ePSO-N was an interactive process between the editors, the network of correspondents and the ePSO team. In this way, ePSO-N kept the ePSO team informed and in close contact with real market demands and problems. The initial network of correspondents was open for new contributors. The Newsletter also contributed to ePSO-Forum discussions as it provided ample topics to discuss and debate among interested and knowledgeable participants. ePSO-N intended to convey unbiased information and to cover the whole spectrum of opinions, including not only those of the more obvious stakeholders but also of consumer and non-governmental organisations. Thus, ePSO-N targeted three groups: the commercial and technological stakeholders, politicians and the interested public. While in general topics are tackled as a result of the ongoing discussion within the network of correspondents and the editors, in tandem with the ePSO project operation, each issue contained a special focus theme covered by three to five articles. In addition, interviews, country reports, news items, facts and figures, conference reports and book reviews were included. A total of 15 issues of the Newsletter were published, appearing roughly every two months, and these were delivered electronically to all ePSO-Forum subscribers as well as made available and read on the web. The special focus of every issue published is presented in the table below:

Table 2: ePSO Newsletter subject focus per issue

Production month	Number	Number of focus articles	Focus subject
July 2000	1	5	Mobile Phone Payment Systems I
October 2000	2	4	Mobile Phone Payment Systems II
November 2000	3	4	E-purses
January 2001	4	4	Interchange Fees
February 2001	5	4	Internet Payment Systems I
March 2001	6	4	Internet Payment Systems II
May 2001	7	5	EMI-Directive
July 2001	8	4	Security in Internet Payments
September 2001	9	4	Security and the Consumer
November 2001	10	4	Authentication, Privacy and Regulation
December 2001	11	2	Money Services Regulation in US and EU
February 2001	12	3	Integration of Payment Systems
March 2002	13	3	Payments in Transport
May 2002	14	3	Cross-border Payments
June 2002	15	5	South East European Transition Economies

A complete run of ePSO-N issues with additional full indexes and a glossary to add value, have been published as an ePSO deliverable for use as a reference handbook.

ePSO Background Papers

In order to achieve its target, ePSO has set up an electronic discussion Forum (ePSO-F) of relevant market actors and experts to facilitate the systematic exchange of their strategic opinions. Forum discussions are stimulated by selected articles edited and published in the ePSO-Newsletter that is distributed electronically to all Forum participants as well as through background papers drafted by Observatory experts. Background papers are short synthesis study reports, whose aim is to structure the strategic and technical issues on a selected focal topic of interest to ePSO. These papers provide analysis beyond the simple presentation of technical and/or quantitative data by integrating a prospective view of what the likely future impact of the issue may be and by posing a set of open

questions, effectively leading to fruitful consensus-raising discussion. In this way it is hoped that they will effectively raise awareness of the issues where market players have conflicting views – and therefore where consensus building may be needed. Moreover, alternative choices are presented whenever possible in an effort to start the discussion on policy options.

The ePSO team, the expert staff of the Observatory, draft the background documents on the selected topics, by integrating information from various sources, such as: selected documentation, personal interviews, specific requests for data and analysis through ePSO-F. The Newsletter was also scheduled to address the same focal topic through a series of dedicated articles. Discussion on the content of these articles among the network of expert correspondents authoring ePSO-N was yet another source of information for the background papers. Draft versions of background papers were peer-reviewed internally and externally. All background papers were presented and reviewed by the Steering Group members. The final draft version was then presented to the ePSO-F members where payment system experts and a broad range of market players are invited to further discuss the issues raised. All comments and suggestions made are collected, cross-checked and introduced into a final version of the paper which will eventually be edited and printed.

Finally, although the main purpose of the paper is to animate in a structured way the expert discussions, it is believed that the collected material on electronic payment systems, usually presented in an annex as well as the referenced bibliography, will be utilised long after the discussions have ceased. The titles, dates of publication of final version of document and a brief summary of the background papers produced are shown below:

Brief Overview of Background Paper Contents

BP1: Electronic Payment Systems – Strategic and Technical Issues. December 2000

This identifies the strategic and technical issues related to electronic retail payment systems that were to be studied during the project, focussing on the needs of consumers, merchants and SMEs. Special emphasis was to be given to payment methods in the context of electronic commerce on the Internet and the development of cross-border payment systems. The issues that were identified were grouped around eight broad categories: e-money, enhanced access products, micropayment solutions, payment systems infrastructure, regulation and innovation, standardization and interoperability, consumer protection, anonymity, privacy and security, and integration of payments into online transactions.

BP2: The Future of M-payments – Business Options and Policy Issues. August 2001

Telco-entry into the payment market would increase competition and might foster more efficient cross-border payment solutions. However, telcos moving into large-scale payment provision would be faced with considerable challenges in risk-management. In addition, they may be required to become banks or Electronic Money Institutions. On the other hand, they may also offer payment instruments that do not fall under banking or EMI regulation. In this case, there would be strong competition between industries that are differently regulated. So far, the market is characterized by a large number of non-interoperable m-payment schemes.

BP3: The Potential of Server-based Internet Payment Systems. July 2001

A general trend towards a server-based approach to Internet payment systems can be observed. Major advances of this approach are ease of use, standardisation of user experience, and suitability for micro-payments. This approach however seems to abandon the use of smart cards, security based on PKI, and the idea of true electronic cash, at least temporarily.

BP4: Payment Culture Matters – A Comparative EU-US Perspective on Internet Payments. August 2001

The cross-country comparison of Internet payment systems revealed considerable differences between countries. The choice of Internet payment methods in a particular country largely depends on the payment habits at the real point of sale. There are also striking differences at the level of co-operation between banks and payment processors. Surprisingly, there are interesting similarities between the EU and the US: the US is far from being a fully integrated payment area and the federal structure is very pronounced. Even in the US e-money is regulated and falls automatically under a number of existing laws and rules.

BP5: Innovation and Regulation – the Case of e-Money Regulation in the EU. January 2001

Both regulation and technological developments strongly influence the shape of payments innovations. Payment services are often bundled with other financial services such as credit, asset management or other services related to other application areas like loyalty programs in retail commerce, ticketing in mass transport or charging for mobile services. Current regulation regarding e-money as a stand-alone product and restricting the issuance of e-money to banks and Electronic Money Institutions does not take this new situation sufficiently into account. There are also doubts on whether the aim of this regulatory approach, to establish a level playing field, is adequate and will serve the purpose.

BP6: Securing Internet Payments – the Potential of Public Key Cryptography, Public Key Infrastructure and Digital Signatures January 2002

There is widespread belief that public key cryptography (PKC), public key infrastructure (PKI), digital signatures and secure Internet payments can act as enablers for the deployment of secure e-payments over the Internet. This paper points out: (a) the risks linked to the Internet environment and the resulting security requirements for on-line Internet payments; and (b) the concepts and security building capabilities of PKC, PKI and digital signatures. Current practice, and the current use of these techniques for Internet and mobile payments and also in other application fields such as on-line banking, B2B applications and e-government services is also analysed and notes as to future challenges are drawn.

BP7: Security and Consumer Trust in Internet Payments – the Potential of ‘Soft’ Measures. April 2002

Internet appears to be an easier environment to perpetrate fraud, due to its anonymity, low access barriers, lack of risk awareness and security skills and the complex legal prosecution for low value cross-border transactions. However, the investigation on Internet payment fraud shows a lack of coherent, accurate and publicly available sources of information. Recognizing the importance of the "human factor", the potential that "soft" or non-technology based measures may have in increasing security and consumer trust in Internet payments is analysed. The role of consumer awareness and education, the limitation of consumer liabilities in case of fraud, the provision of redress mechanisms, and the use of merchant trust marks as trust building measures was analysed.

BP8: Integration of Electronic Payment Systems into B2C Internet Commerce – Problems and Perspectives. April 2002

Only few payment instruments are available online and often these are not integrated into the online-shopping process from both the consumer's and the merchant's point of view. Truly integrated payment systems for digital goods and services do not yet exist. A structured picture of various payment-relevant B2C standards is sketched, standardisation problems are discussed, and payments integration in the B2B area is outlined before major findings are summarised in the light of potential policy relevance.

ePayment Systems Database – Trends & Analysis

In addition to the background papers a report was produced that analyses the evolution of Internet-based payment solutions offered to consumers in Europe by describing the main trends observed in these new consumer payment solutions. It is based on the observation of 100 electronic payment schemes taken from the ePSO Inventory. Based on the information collected, and the limited consistency of information released by the payment system providers, the research was structured to investigate a limited set of questions deriving from 9 topics.

ePSO Electronic Discussion Forum

The electronic discussion Forum (ePSO-F) is an open participation Forum of experts, convened on a voluntary basis, animated by the ePSO team, with the objective to address strategic and technological issues in the field of electronic payment systems and related areas. ePSO-F brought together a large number of market players from the banking, payments and card industry, technology providers, retailers, telecommunications, consumers, government, standards bodies, academia, independent consultants and other interested. Participation was managed through individual subscription.

The main aim was to allow Forum members share among themselves information about problems and proposed solutions on electronic payment systems technology and their views on future impacts of the use of this technology. The ePSO team animated the discussion by distributing background papers and the ePSO-Newsletter, to ePSO-F subscribers thus raising awareness on a number of issues and then introducing focused questions provoking debate aiming at consensus. Topics of discussion have included business models, barriers to success, technical difficulties and legal/legislative implementation benchmarking. E-mail was the main tool for information sharing but suitable web-based tools (web-based e-mail lists) were used to facilitate a more interactive exchange of information.

ePSO-F first became operational during January 2001 and 275 persons were subscribed to the Forum by the end of February 2001. The overall number of subscribers varied as new people subscribed and existing participants left the list but there was a monthly growth of almost 10% leading to a total of 755 users by the end of April 2002. Representation was truly European (about 80% of subscribers with almost 560 from EU countries) and market oriented (see Table 3):

Table 3: ePSO Forum Participants Activity Area (April 2002)

Participants Activity Area	Number	Participants Activity Area	Number
Banking, payment	182	Telco operators	66
Retail, users	62	Consultants	74
Technology developers	92	Academic	69
Public, government	37	Others	173

More than 800 messages have been exchanged since February 2001 (an average of 55 messages per month) of which about 15% were IPTS initiated. Many different subjects were raised and discussed but 22 of those had more than 10 interactions each and one included more than 20 e-mail exchanges. More than 200 non-IPTS related subscribers initiated messages some of which submitted more than 5 messages each. The number of postings (discussion items) during the first month was low and the ePSO team was the main interlocutor but subscribers quickly initiated discussions on various subjects. Forum members were invited to attend the consensus raising conference organised in Brussels on February 19, 2002.

ePSO Conference

As part of the ePSO project the IPTS, of the European Commission's Direction General Joint Research Centre, organised a final conference in Brussels on February 19th 2002. The "ePSO Conference on Consumer Online Payments: Trends and Challenges for Europe" set the stage for state-of-the-art e-payment systems presentations, allowing actors to exchange views on existing trends and future developments, and to reinforce and extend the already established communication links.

Mrs. Randzio-Plath of the European Parliament opened the ePSO final conference. The conference agenda included presentations on payment policy issues, innovation and regulation, standards and interoperability, security and infrastructure, and the future of digital rights management issues. The event, which emphasised cross-border and cross-sector exchange, brought together representatives from the banking sector, payment card industry, standardisation bodies, consumer organisations, telecommunications operators and retail e-commerce associations as well as payment service providers, technology providers and policy makers. The conference content and debated issues have been presented in detail at a previous Newsletter article [13&8].

Recent Dissemination Activities

1. IPTS Report Special Issue on e-Payment Systems Challenges for Europe

Companies are increasingly experimenting with Internet technologies with a view to improving payments efficiency, reducing operating costs and boosting profits. A complex market situation is arising as banks, "near-banks" and "non-banks" are competing through an ever-increasing number of payment channels, such as the Internet, interactive TV, and mobile payments. Business model failures as well as the failure to build trust, fuelled by a number of notorious breaches of security and a general explosion in fraud, are among the main reasons for some high-profile failures. A special issue of the IPTS Report dedicated to e-payments and the challenges these bring for Europe deals with such topics

in a way to ensure that information exchange on the strategic options available has taken place among all interested players.

2. CD-ROM Containing all ePSO Deliverables Including the Conference Presentations

A CD-ROM presenting the ePSO project objectives and organisation as well as all its deliverables including the ePSO final conference presentations has been developed and will be mailed to all conference participants.

[15&8]

Bye, Bye Banknotes?

Leo Van Hove (Leo.Van.Hove@vub.ac.be*), Free University of Brussels, Belgium*

/review/cash/electronic money/costs/government intervention

In a recent article in Economic Policy, Drehmann et al. argue that cash will be able to resist the e-money challenge because e-purse schemes may be relatively more costly than is commonly thought and because e-purses will never be as anonymous as currency. While I agree with their main conclusion that currency is unlikely to disappear anytime soon, I am not convinced by their claim that currency is a highly competitive means of payment. I therefore argue that there might be a task for the government to make e-money more attractive compared to cash.

After 14 issues of ePSO-N cluttered with information on all sorts of novel payment schemes, it seemed a good idea to devote my final review to the impact of this electronic brute force on good old paper currency. "Will the traditional transaction medium be able to resist competition from the new technologies?", that is the central question of a recent article by Mathias Drehmann (Universität Bonn), Charles Goodhart (London School of Economics) and Malte Krueger (formerly with ePSO, now with a Frankfurt-based consultancy). Their answer is a straightforward 'Yes'. Stronger still, they argue that "currency and central banks are among the safer financial institutions to survive the new millennium" (p. 217).

Drehmann et al. offer three reasons why traditional cash is - and will be - widely used: anonymity, cost, and convenience. To start with the most important one, it is clear that currency leaves little trace. As a result, it is favoured by people engaged in activities which they do not want to become known, especially not to the tax authorities. More specifically, Drehmann et al. argue that there are essentially two, largely separate, markets for currency: first a market for small bills for ordinary, every-day consumption expenditure, and second a market for large value notes to facilitate 'bad behaviour' (as well as local and foreign hoarding). In their view, such 'bad behaviour' should be interpreted broadly, in that it not only includes illegal activities, but also "legal activities that are regarded by some as sufficiently immoral, or suspect, to want to avoid others knowing about them – for example gambling, alcohol, purchases of pornography, ..." (p. 197). In order to underpin the existence of these two separate market needs for currency, Drehmann et al. estimate a number of currency demand equations for 16 OECD countries covering the 1980-1998 period. In these regressions they include a set of variables which might influence 'bad behaviour' motives for currency holding - the hypothesis being that their impact should be larger for large bills. Where the tax ratio is concerned, Drehmann et al. do indeed find that it is a significant factor in determining the demand for high-value banknotes, whereas it has almost no effect on small bills. The results of their attempts with a crime index, however, are mixed. Drehmann et al. also examine the impact of alternative non-cash means of payments on the use of cash but most of them turned out to be entirely insignificant. These include the volume and value of card (and cheque) payments. The only two technological variables that appear to have had a reasonably close relationship with currency usage are the number of ATMs (positive) and EFTPOS terminals (negative). The authors conclude from their econometric research that the effects of modern payment technologies on the demand for cash have so far not been strong. They also argue that because it is implausible to envisage authorities allowing a completely anonymous e-money system, 'bad behaviour' will ensure a continuing demand for large bills, which account for over half the stock of outstanding currency in many OECD nations. In short, all evidence to date is that cash is not about to disappear. Stronger still, "the legalization of drugs could make a much bigger dent in the demand for currency than competition from e-money" (p. 217).

As the second characteristic that may favour the use of currency, Drehmann et al. point towards the relative costs involved. They present international evidence to show that in terms of volume of transactions, cash is still king and conclude that "these numbers show that cash is a competitive payment product" (p. 203). In Part C of the Web Appendix, they also present results of cost studies by retail organisations. Again the conclusion is that "cash still is a highly competitive means of payment" (p. 5). Strangely, this message changes in the conclusion where it is stated that the improvement in economic efficiency stemming from a generalized move to e-money would be large (p. 217). Perhaps this has something to do with the fact that the article is co-authored.

The third and final advantage of cash, according to Drehmann et al., relates to convenience. They argue that cash is fast and, unlike e-purses, usable throughout the euro area. They also argue that while counterfeiting is hardly a fundamental threat for currency it may well be one for e-purses. In order to defend themselves against hackers, e-purse issuers will thus have to upgrade their systems continuously, exclude P2P payments, limit the maximum amount that can be stored on cards, etc. Drehmann et al. emphasize that these measures either reduce the convenience of e-purses for users (the cards will not be suitable for anonymous transactions nor for hoarding), or increase the costs for issuers – thus further degrading their business case (the seigniorage potential being low already).

Overall, the article by Drehmann et al. is interesting and I agree with their main conclusion that cash is unlikely to disappear anytime soon unless central banks would stop issuing banknotes. However, I disagree with Drehmann et al. on two important points. Firstly, I am not convinced by their argument that "the competitiveness of cash is reflected in its continuing high market share in retail payments" (p. 203). As I have argued elsewhere (Van Hove, 2002), consumers are typically spared the true cost of cash – implying that cash is actually subsidised. Hence, usage figures do not show that cash is a competitive product. I am also not convinced by the results of the cost studies presented. The reasons are explained in more detail in Van Hove (o.c.). The essence is as follows: quite apart from the quality of the cost estimates, a first criticism is that the data refer to a period – 1998 – when the uptake of e-purses was still way too low for the new payment instrument to benefit from economies of scale. In short, it was too soon to make a fair comparison of the cost of cash and e-purse. Another important point is that not only the private costs of retailers matter but also the social costs. All available estimates indicate that the social cost of cash is very substantial. I therefore see no reason to change my conviction that e-money has the potential to ultimately provide a more efficient alternative to cash (primarily because it eliminates a number of labour-intensive steps in the flow of funds). That is why the use of cash should be discouraged.

This brings me to my second point of disagreement with Drehmann et al. In their concluding Section, they tackle the public policy issue of how far the authorities should go in trying to suppress 'bad behaviour'. This is their answer: "How far would we want to go down the road of giving up privacy (and anonymity) to enhance efficiency? Not far. We agree that governments should not wilfully encourage 'bad behaviour', and hence we agree [...] that the issue of 'large value' notes is undesirable. But any attempt to force a complete shift to electronic transfer, and to try to ban, or to prevent, the domestic use of cash would in our view be *appallingly illiberal*" (p. 217; my emphasis). Personally, I am less concerned about the impact on privacy. E-money can be programmed. It should therefore be possible to strike a balance between privacy concerns and law enforcement needs. In the trade-off between anonymity on the one hand and enhanced efficiency and the suppression of 'bad behaviour' on the other, I also appear to attach a greater weight to the equal distribution of the tax burden than do Drehmann et al. As a result, I would be willing to go further down the road described above. In my view, the use of cash should be actively discouraged by making it more expensive; see (Van Hove, 2002).

To conclude, let me note that although Drehmann et al. are convinced that "it is unlikely that interest will be paid on e-money balances" (p. 207), in Singapore the monetary authorities are seriously contemplating doing just that - as part of their electronic legal tender plans (Low, 2001, p. 3). Clearly, the introduction of such interest-bearing electronic legal tender, issued by the central bank, would completely change the setting. If they go ahead with their plans, Singapore will be an exciting case to watch. Who knows, perhaps there is a cashless future after all ...

[info]

- Drehmann, M., Goodhart, Ch. and M. Krueger: The challenges facing currency usage: will the traditional transaction medium be able to resist competition from the new technologies? In: Economic Policy, Vol. 17, Issue 34, April 2002, pp. 193-227 <http://www.economic-policy.org>

- Low, S. K.: Singapore Electronic Legal Tender (SELT) - A proposed concept. Paper presented at the OECD Future of Money Forum. Luxembourg, July 2001.
- Van Hove, L.: Electronic money and cost-based pricing. In: Wirtschaftspolitische Blätter (Economic Policy Papers; Austria), Vol. 49, No. 2, April 2002, p. 128-136.

[15&9]

Masthead

Electronic Payment Systems Observatory-Newsletter

ePSO-Newsletter – 2002 – No. 15 – June 2002

Homepage: <http://epso.jrc.es/newsletter>

Subscription page: <http://epso.jrc.es/newsletter/subscribe.cfm>

The Electronic Payment Systems Observatory-Newsletter (ePSO-N) is an activity within the "electronic Payment Systems Observatory" (ePSO) project of the Institute for Prospective Technological Studies (IPTS), one of the eight institutes of DG Joint Research Centre. The Institute for Technology Assessment and Systems Analysis (ITAS) of Karlsruhe Research Centre edits this newsletter.

The editorial staff currently consists of Knud Böhle, Michael Rader, Ulrich Riehm and Arnd Weber, supported by a network of highly qualified correspondents. This network consists of the following members (in alphabetical order)

Ülle Adamson – Latvia

Anna Arbussà – Spain

Piero Bucci – Italy

Clara Centeno – Spain

Erik Dahlström – Sweden

Laura Edgar – United Kingdom

Morten Falch – Denmark

Andreas Furche – Australia

Rüdiger Grimm – Germany

Mike Hendry – United Kingdom

Masanobu Higashida – Japan

Stefanos Karapetsis – Greece

Malte Krueger – Germany

Simon Lelieveldt – Netherlands

Peter Mair – Australia

Walter Peissl – Austria

Rufus Pichler – USA

Anita Ramasastry – USA

Luigi Sciusco – Italy

Oliver Steeley – United Kingdom

Jaume Valls – Spain

Leo Van Hove – Belgium

Michael Walters – Australia

Thorsten Wichmann – Germany

Hans-Dieter Zimmermann – Switzerland

Disclaimer: The views and opinions expressed in the articles of ePSO-N do not necessarily reflect those of the European Commission, DG Enterprise, IPTS or ITAS. All articles are regarded as personal statements of the authors and do not necessarily reflect those of the organisation they work for.

The editors retain copyright, but reproduction is authorised, except for commercial purposes, provided the source is acknowledged. The editors would appreciate a short message if articles of ePSO-N are reproduced.

Contact: Michael Rader
co-ordinating editor

rader@itas.fzk.de

Institute for Technology Assessment and
Systems Analysis (ITAS)

Research Centre Karlsruhe

– Technik und Umwelt –

Postfach 3640

D-76021 Karlsruhe, Germany

Phone.: +49-7247/82-0

Fax: +49-7247/82-4806

WWW: <http://www.itas.fzk.de/>

Contact: Yannis Maghiros

ePSO project leader

ioannis.maghiros@jrc.es

Institute for Prospective Technological
Studies (IPTS)

Directorate General Joint Research
Centre, European Commission W.T.C.

Isla de la Cartuja s/n

E-41092 Sevilla, Spain

Phone: +34-95-448 8318

Fax: +34-95-448 8300

WWW: <http://www.jrc.es/welcome.html>

Table of Contents 2 - organised by topics

About ePSO-N, Contacts, Correspondents and Disclaimers

[10&7] ePSO Final Conference on Consumer Online Payments: Trends and Challenges for Europe	41
[11&5] Integration of Internet Payment Systems – What’s the problem?	50
[14&7] Internet Banking Workshop – A Spanish and European Perspective of the Future	112
[15&7] ePSO Final Report	128
[15&9] Masthead	138

General analytical articles on e-payment developments

[10&6] Failure of Beenz and Flooz indicates the end of Digital Web-Currencies?	39
[12&5] Paybest, an emerging micropayment solution for digital goods and services	69
[12&7] How can PKI services take off in Finland? From one ID card to Multiple Company and customer cards	74
[13&5] Billing woes	87
[14&6] Expanding niches: Some results of an online survey about online shopping and paying	109
[15&6] I-Payment strategies	127

Security

[9&1] Editorial: Security and the Consumer	9
[9&2] Risks in using personal computers for electronic signatures and electronic banking	10
[9&3] Fraud in Electronic Payments: Achieving security Standards	13
[9&4] DASIT: Privacy protection on the Internet by user control	15
[9&5] Creating consumer confidence: Current efforts towards international quality criteria for e-commerce	16
[9&6] Security and trust: taking care of the human factor	19
[10&1] Editorial: Authentication, privacy and regulation	27
[10&2] Guaranteed transactions, the quest for the ‘Holy Grail’	28
[10&3] Interview: Largest German credit card issuer on massive reduction of charge backs	31
[10&4] Hi-tech payment technologies in Russian: The case of Paycash	34
[10&5] JAP: A cloak of invisibility on the Internet	37
[11&1] Editorial: The vulnerability of technology – the Achilles heel of globalisation	44
[11&2] The day after	45
[11&3] Worms, disputes and rolling blackouts – protection for the citizen	47

[13&6] Success factors for credit card fraud? An illustrative example: the Yescard	89
[13&7] Internet and mobile security in Singapore	91
Country Reports	
[9&7] Mobile payments in the Baltic States	21
[12&6] The CashCard: Lessons from Singapore	72
[15&1] Editorial: Payment transition from the Balkans to the Dnjepr	116
[15&2] Interview: Mobile banking on low cost networks in Romania	118
[15&3] Evolution and present status of the Bulgarian card market	122
[15&4] EU funded Balcard project: Targeting the unbanked Internet buyers	124
[15&5] Ukraine: From 'specific units' towards electronic payments	125
Money Services Regulation in the US and Europe	
[11&6] The European Electronic Money Institutions Directive and the US Uniform Money Services Act – Similarities and differences	53
[11&7] e-Money regulation in the United States	55
Standards for Payment Systems Integration	
[12&1] Editorial: Elegant standards and everyday B2C e-commerce	60
[12&2] The Internet Open Trading Protocol: What is it and why is it needed?	62
[12&3] Interview: Whether or not the Internet Open Trading Protocol (IOTP) is successful depends on the definition of success	64
[12&4] The CEN/ISSS eWallet project presents its work	67
e-Payments in Transport	
[13&1] Editorial: e-Payments in transport – High speed systems or customer monitoring?	79
[13&2] Payment solutions for automotive telematics	81
[13&3] New technology for mobile electronic fee collection	83
[13&4] ERG buys Proton	83
Small Value Cross-Border Payments	
[14&1] Editorial: Cross with old banking boys' cross-border retail payment networks	95
[14&2] Interview: The road to efficient cross-border retail payment systems in Europe - long and winding or straight through?	97
[14&3] Cross-border low value payments: What is likely to emerge from EC legislation?	102
[14&4] The cross-border payments malaise: M-payments to the rescue?	106
[14&5] Back to tinfoil and banknotes: The trials and tribulations of petty cross-border trading	108

Reviews

- [9&8] The payment blues of German Internet merchants 24
Bock, P & Spiller, D: Kassieren im Ecommerce – eine Analyse relevanter Zahlungssysteme aus Händlersicht, Berlecon Research, February 2001 (available in German only)
- [10&8] Meet the heavyweight of payment systems statistics: ECB's 'Blue Book' 42
European Central Bank: Payment and securities settlement systems in the European Union ('Blue Book'), third edition, Frankfurt, June 2001
- [11&4] Innovations for an e-society. Challenges for technology assessment: A note on the e-Commerce track of the Conference. 48
 This article is based on the 'e-Commerce track' at the 'Innovations for an e-society Challenges for Technology Assessment' Conference, Berlin 17 – 19 October 2001
- [11&8] e-Money not ECLIPsed by regulation 58
Newman, S (ed): Smart Cards – ECLIP II Report, September 2001.
- [12&8] Survey of electroning money developments: BIS repetita placent 77
Committee on Payment and Settlement Systems (CPSS): Survey of Electronic Money Developments, Basel, Switzerland, November 2002 (update on report of same name of May 2000)
- [13&8] The ePSO Final Conference: Hopefully not the end 92
 Personal impressions on the Final ePSO Conference, Brussels
 19 February 2001
- [14&8] Recommendation 97/489/EC Revisited: A case of frustrated expectations? 113
 Study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment instruments and in particular the relationship between holder and issuer, May 2001
- [15&8] Bye, Bye Banknotes? 135
Drehman et al.: The challenges facing currency usage: will the traditional transaction medium be able to resist competition from the new technologies?: In: Economic Policy, Vol. 17, Issue 34, April 2002

Index

This Index includes names and acronyms found in the ePSO-N articles. Names of ePSO-N authors and all names related to sources and the **[info]** sections have been excluded.

@

@UK PLC, 68

3

3D-Secure, 27, 28, 31, 34, 53

3D-SET, 25, 26

3G, 86, 125

3GPP2. *See* Third Generation Partnership Project 2

3KP-SET, 16

4

4Friendsonly.com AG, 73

A

Abbey National, 118

Academy of Entrepreneurship and Management, 48

ACH, 109. *See* Automated Clearing House

ADR, 17

AECE. *See* Spanish Association for Electronic
Commerce

AGES, 88

AgV. *See* VZBV

Airmiles, 41

Alkor, 35

Alkor Paycash, 36

Alkor Ukraine, 36

Allbank, 31

Alternative Dispute Resolution. *See* ADR

Amazon, 34

Amdocs, 93

American Express, 91, 129

AmEx, 31, 90

ANZ Bank, 91

API, 69

ASK, 83

atCredits, 68

ATMs, 143

Audi, 85

Austrian Academy of Science, 49

B

B+S Cardservices, 31

Balcard, 123, 130

BalkanBank, 128

Baltijas Tranzitu Banka, 24

Bancpost, 130

Bank DSK, 128

Bank for International Settlements, 63

Bank Identification Codes, 104

Bank Identifier Codes, 108

Bank of Finland, 100

Bank of Greece, 82

Bank Organization for Payments Initiated by Cards. *See*
Borica

Bankgesellschaft Berlin, 27, 31

Banking Directive, 55

Banksys, 90, 91

BarclayCoin, 61, 81

Barclays Bank, 33

Baycorp, 79

BBBonline, 18

Beenz, 27, 28, 40, 41

Berlecon Research, 10, 24, 26

Berlin Savings Bank, 31

Berlin State Bank, 31

Berliner Bank, 31

Better Business Bureau, 18

Better Internet Bureau, 18

BEUC, 18

BICs, 108. *See* Bank Identification Codes

Bidder's Edge, 50

BIS, 80. *See* Bank for International Settlements

Biztalk, 65

Blue Book, 43, 44

BMW, 85

BMW, 15. *See* German Ministry of Economics

BNB, 128. *See* Balkan National Bank

Borica, 128, 129, 130

Brokat Technologies, 66

Bulgarian Post Bank, 128

Bureau van Dijck, 61

C

Cahoot, 118

Card Technology, 83

Card.etc, 90

Cardholder Authentication Verification Value. *See*
CAVV

CAs. *See* Certification Authorities

CashCard, 63, 64, 75, 76

CAVV, 29

CDG. *See* CDMA Development Group

CDMA, 127. *See* Code Division Multiple Access

CDMA Development Group, 125

CDMA2000, 124

CDR, 93. *See* Call Detail Record

CEN/ISSS, 63, 71, 72, 106, 135

Centre for Commercial Law Studies, Queen Mary
College, 120

CEPS, 76, 105, 130, 131. *See* Common Electronic Purse
Specifications

Certification Authorities, 78

CfIT. *See* Commission for Integrated Transport

Chipper, 81

Choreology, 71

CIA, 38

Citibank, 101

Citroen, 85

COBOL, 34

Commerceworks, 71

Commission for Integrated Transport, 88

Connex, 126

Consult Hyperion, 98

Consumers International, 17

Convergys, 93

Coyota, 27

CPSS, 80, 81, 82. *See* Committee on Payment and
Settlement Systems

Credit Express Bank, 128

CRID, 120
C-SET, 94
Cubic, 83
Cybercash, 40
CyberComm, 94
Cyphermint, Inc, 36
Cyscom, 71

D

D 21, 18
Danmønt, 44
DASIT, 9, 15, 16
Data Protection Directive, 61
Datamax, 129
Delivery Versus Payment, 105
Delphi, 94
Deutsche Bahn, 90
Deutsche Bank, 53, 101
Deutsche Telekom, 90
Development Bank of Singapore, 76
DG Bank, 9
DG Information Society, 50
DG Internal Market, 99, 121
Digicash, 35
Diners Club, 129
Directive 2000/12/EC. *See* Banking Directive
Directive 2000/46/EC. *See* EMI Directive
DIRECTS project, 88
Distance Selling Directive, 61
DSRC, 88, 89. *See* Dedicated Short-Range
Communication
DUCATO, 130
Ducato CEPS-pilot, 43
DVD, 117
DVP. *See* Delivery Versus Payment
DZ Bank, 15. *See* DG Bank

E

E.ON, 48
Easyride project, 84
Easyticket, 84
EBA. *See* Euro Banking Association
eBay, 50, 98
EBIP, 49. *See* Electronic Commerce Business Impacts
Project
EBRD, 129
ebXML, 65. *See* Electronic Business Extensible Markup
Language
Ecard, 91
eCash, 40, 61, 81
ECB, 41, 44, 100, 109, 111, 114
ECBS, 106, 110. *See* European Committee for Banking
Standards
ECHELON, 38
ECI, 29. *See* Electronic Commerce Indicator
ECLIP, 61. *See* Electronic Commerce Legal Issues
Platform
ECLIP II report, 61
ECML, 63, 65, 69. *See* Electronic Commerce Modelling
Language
EDI, 78
EDP, 46
EEJ-Net's. *See* European Extra-Judicial Network
EFC, 88, 89. *See* Electronic Fee Collection
EFTPOS, 127, 143
Electronic business Extensible Markup Language, 70
Electronic Commerce Indicator, 32. *See* ECI
Electronic Fee Collection. *See* EMT

Electronic Money Directive, 64, 81
Electronic Money Institutions, 61, 75
Electronic Money Institutions Directive. *See* EMI
Directive
Electronic Payment Instruments. *See* EPIs
Electronic Toll Collection, 87
Elisa Communications, 22
Elsag, 124
EMI. *See* Electronic Money Institutions
EMI Directive, 55, 56
E-Money Directive, 81
EMT, 22, 24
EMV, 31, 90, 131, 137
EMVCO, 31
ePay Voice, 129
ePay.bg, 129
EPIs, 120. *See* Electronic Payment Instruments
e-plus, 92
ePSO, 51, 62. *See* Electronic Payment Systems
Observatory
ePSO Forum, 10
ePSO-Forum, 42
ePSO-Newsletter, 10
ERG, 83, 91
ERG Group, 90
ERP systems, 52
Estonian Mobile Telephone. *See* EMT
ETIS, 72
eTrust Mail, 11
ETSI. *See* European Telecommunications Standards
Institute
Euro 1, 43
Euro Banking Association, 108
Eurobank, 130
Eurocard, 129
Eurocheque, 100, 101, 114
euroConex, 71
Eurocred, 110
Eurogiro, 108, 114
Eurogiro News, 108
Europay, 43, 98, 131
European Banking Federation, 110
European Central Bank, 28. *See* ECB
European Commission, 18, 19, 45, 48, 62, 78, 88, 102,
103, 107, 111, 119, 137, 145
European Committee for Banking Standards, 72
European Extra-Judicial Network, 48
European Parliament, 55, 141
European Payments Group, 110
European PRoGR€SS project, 89
European Telecommunications Standards Institute, 70
European Union, 100
Eurovignette system, 89
eWallet, 64, 71, 72
Extensible Markup Language. *See* XML
Ezpay, 68

F

Fareway consortium, 88
Fastest, 91
Federal Ministry of Economics, 39
FESTE. *See* Spanish Foundation for the Study of Security
in Electronic Telecommunications
FhI-SIT, 15
Fiat, 85
Financial Internet Working Group, 119
FINEID, 98
FINEID card, 63, 64
FIN-NET, 48

Finnish Ministry of Finance, 77
Finnish Population Register Centre, 77, 78
First Investment Bank, 128
First Private Bank, 128
FirstGroup, 90
FIWG. *See* Financial Internet Working Group
flash-EEPROM, 94
Flooz, 27, 28, 40, 41
Ford, 85
Fraunhofer Institute for Secure Telecooperation. *See* FhI-SIT
Free University of Brussels, 137
Freedom, 38

G

Game SpinOff, 73
GDtrust Mail, 11
Geldkarte, 26, 66, 69, 81
German Ministry of Economics. *See* BMWi
geZeroLee, 94
GFP, 74. *See* Game Feature Platform
GIPI. *See* Global Internet Policy Initiative
GNSS/CN. *See* Global Navigation Satellite System with Cellular Networks
Goner Worm, 48
Government Multipurpose Card, 98
GPRS, 124, 126
GPS, 84
Gr@dient Research Group, 118, 119
GSM, 85, 112, 122, 126
GSM Association, 22
Guta Bank, 35

H

Hansabank Group, 23
Hansabanka, 23
HCI, 19, 20
Hitachi, 66, 68
HTML, 69
HTTP, 68
Human-Computer Interaction. *See* HCI

I

IBAN, 106, 108, 110. *See* International Bank Account Number
IBM, 134
IESG. *See* Internet Engineering Steering Group
IETF, 52, 63, 65, 67, 69, 106
IETF TRADE Working Group, 63, 68
IMF, 128
IMO. *See* International Money Order
i-mode, 92
INBIS, 50
Independent Centre for Privacy Protection, 39
Info2Clear, 98
Information Society Initiatives in Standardisation, 135
ING Direct bank of Canada, 20
INITIATIVE. *See* Industry Initiative to Introduce Automatic Tolling in Vehicles in Europe
Inquam, 124
Institut Européen Interrégional de la Consommation, 107
Institute for the Protection and Security of the Citizen, 48
Intellect, 71
Interactive Voice Response, 110
Intermobil, 84

International Bank for Investments and Development, 128
International Money Orders, 100
International Organisation for Standardisation. *See* ISO
Internet Engineering Steering Group. *See*
InterPay, 68, 90
InterPay Nederland, 91
IOTP, 52, 63, 65, 66, 67, 69. *See* Internet Open Trading Protocol
Ipacri Romania, 124
IPIN/BT, 72
IPTS, 49, 119, 135, 141, 145. *See* Institute for Prospective Technological Studies
ISIS. *See* Information Society Initiatives in Standardisation
ISO, 17
ISO 15408, 14
IT Law Unit. *See* Centre for Commercial Law Studies, Queen Mary College, London
ITAS, 50, 123, 135, 138, 145. *See* Institute of Technology Assessment and Systems Analysis, Karlsruhe Centre
ITI Services, 68
ITS, 88, 89. *See* Intelligent Transport Systems
ITSEC, 14
ITSEC E1, 15
ITSEC E3, 13
ITSEC E5, 15
ITU, 125
IVR. *See* Interactive Voice Response

J

JAP, 39, 40. *See* Java Anon Proxy
Java, 68
Java Anon Proxy, 38
JAWAwallet, 72
JCC, 130
Joint Research Centre, 48, 141
Jupiter Research, 73

K

Klebox, 61
Kleline, 81
Kontiki, 91
KPN mobile, 92
Kyivstar, 133

L

La Caixa, 118
Latvian Mobile Telephone. *See* LMT
LETS. *See* Local Exchange Trading Systems
Liberty Alliance, 27, 53, 64, 72
Linux, 12
LMT, 23
Local Exchange Trading Systems, 41
London School of Economics, 142

M

Maastricht Economic Research Institute on Innovation and Technology, 50
Maestro, 129
Mail Order Telephone Order, 31
Maksekeskus, 24
MAS. *See* Monetary Authority of Singapore
Mastercard, 27, 28, 30, 31, 33, 101, 109, 112, 127, 129

MCI, 53
Mellon Technologies, 130
Mercedes, 85
Merchant Category Codes, 32
MERIT. *See* Maastricht Economic Research Institute
Micropay, 72
Microsoft, 27, 134
Microsoft Passport, 27, 72
MIME, 68
Mixes, 27
MLSA. *See* Money Laundering Suppression Act
Mobipay International, 98, 112
Mondex, 66, 67, 81, 131
Mondex USA, 65
Monetary Authority of Singapore, 84
MOTO, 32, 33. *See* Mail Order Telephone Order
Motorola, 66, 67
Movilpago, 99
MS Passport, 53, 64
MSBs, 55. *See* Money Services Businesses
mSignature, 126

N

Nacionalais Maksajumu Centrs. *See* NMC
National Bank of Greece, 129
National Express, 90
NCCUSL, 55, 56, 58. *See* National Conference of
Commissioners on Uniform State Laws
NetMaks, 36
NETS, 64, 76, 131. *See* Network for Electronic Transfers
(S) Pte Ltd
Network for Electronic Transfers (S) Pte Ltd, 75
NewGenPay, 71
NMC, 24
Nordea, 118
Norges Bank, 44
Novotrust, 77, 79

O

OBU. *See* On-board units
Octopus, 81, 83, 90
OECD, 17, 49, 143
OKO Bank, 98
On-board units, 88
Orbiscom, 27
OTP, 67. *See* Open Trading Protocol
Oversea-Chinese Banking Corporation, 76

P

PACE, 43, 137
Paiement CB sur mobile, 94
Pay Per View Service, 98
Payback, 41
Paybest, 63, 64, 73, 74, 75
Paybox, 25, 68, 98, 101, 113
PayCard, 90
Paycash, 27, 35, 36
Payment Service Providers, 52
PayPal, 56, 58, 98, 101, 109, 134
Payware, 72
PCL. *See* Prepayment Cards Ltd
PCN. *See* Pseudo Card Number
PDAs, 12
Pentagon, 45
Perseus, 12
PKC. *See* Public Key Cryptography

PKI, 63, 64, 78, 90, 131, 139. *See* Public Key
Infrastructure
PKSCrypt, 11
POI. *See* Points of Information
Point of Sale, 32, 139
Points of Information, 85
Portal Software, 93
POS. *See* Point of Sale
Postbank, 130
Prepayment Cards Ltd, 90
PriceWaterhouseCoopers, 50
Privatbank, 132
Proton, 81, 83, 90, 91, 131
Pseudo Card Number, 34
PSPs, 66, 68. *See* Payment Service Providers
PSSC. *See* Payment and Settlement System Committee
Public Key Cryptography, 140

Q

Q-GSM, 23
Qualcomm, 124, 125
Quick, 81

R

Radiolinja Estonia, 22
RAND Corporation, 47
RATP, 83
Rhein-Main Verkehrsverbund, 91
Road User Charging, 87
Royal Bank of Canada, 66, 68
Russalvbank, 35
Russian Central Bank, 36

S

Safeguard Sign&Crypt, 11
Santander Central Hispano. *See* SCH
Saules Banka, 24
SCH. *See* Santander Central Hispano
Schlumberger, 83
SchlumbergerSema, 93, 130
Secure Payment Application. *See* SPA
SET, 21, 27, 31, 33, 66, 68, 69, 134
SETCO, 31
SIA, 126
Singapore Telecommunications Limited, 76
Single Payment Area, 102
SMILE, 68
Sonera, 22
SPA, 30, 34
SPA/UCAF, 27, 28, 31, 34, 53
Spanish Association for Electronic Commerce, 119
Spanish Foundation for the Study of Security in
Electronic Telecommunications. *See* FESTE
SSL, 33, 64
Stagecoach, 90
STEP-1, 43, 108
STEP-2, 108
STOA. *See* Scientific and Technological Options
Assessment
STOA report, 100
STP. *See* Straight Through Processing
Straight Through Processing, 110
Swedbank, 23
Swedgiro Group, 24
SWIFT, 108. *See* South Wales Integrated Fast Transport
Swissair, 41

Synertek, 125

T

TAM. *See* Technology Acceptance Model

TARGET, 43

Tavrishesky Bank, 35

TCPA, 12

TDMA. *See* Time Division Multiple Access

Tele 2 AB, 23, 24

Telecommunications Industry Association, 125

Telematics Valley, 85

Telemobil, 124, 127

Telia, 22

Telstra, 91

The Economist, 98

Third Generation Partnership Project 2, 125

TIA. *See* Telecommunications Industry Association

Time Division Multiple Access, 124

TIPANET, 114

T-Mobile, 112

TNO-STB, 49

Toll Collect, 88

TouristSportBank, 128

TRADE, 70

TRUSTe, 18

Trusted Computing Platform Alliance. *See* TCPA

TrustedMIME, 11

U

UCAF, 30. *See* Universal Cardholder Authentication Field

UCC. *See* Uniform Commercial Code

UCITA. *See* Uniform Computer Information Transactions Act

Ühispank, 24

UK Banking Code, 61

UK Consumers' Association, 18

UK Post Office, 90

UMC. *See* Ukrainian Mobile Communications

UMSA, 45, 55, 56, 58, 59. *See* Uniform Money Services Act

Unibanka, 24

UNICE, 18

Uniform Computer Information Transactions Act, 56

United Bulgarian Bank, 128

United Overseas Bank, 76

United States Congress, 58

Universal Cardholder Authentication Field. *See* UCAF

Universität Bonn, 142

University of Girona, 102, 118

University of Jaén, 118

University of Karlsruhe, 115

University of Muenster, 62

University of Namur, 62, 120

University of the Balearic Islands, 61

uSwitch.com, 48

V

VABANK, 132, 133

Vanguard, 126

VDI/VDE, 50

VDI/VDE IT, 49

VDV. *See* Verband Deutscher Verkehrsbetriebe

Verkehrsverbund Rhein-Ruhr, 90

VISA, 27, 28, 29, 31, 33, 34, 53, 90, 101, 109, 112, 127, 129, 131

VISA Virtuon virtual cards, 132

Visa XMLInvoice, 65

Visanet, 29

Vodafone, 112, 126

Volvo, 85

VPS, 88, 89. *See* Vehicle Positioning Systems

VZBV, 18

W

W3C Micropayment Initiative, 65

Wall Street Stock Exchange, 45

WAP, 23, 137

Washington School of Law, 45

Webcard, 132

Weberbank, 31

Webtrader, 18

Webtrust, 18

Western Union, 114

World Trade Center, 45

Worldpay, 28

WORM-media, 9

WTSL, 126

X

XML, 52, 65, 66, 70

XMLDSIG, 70

XMLPay, 65

Y

Y2K, 47

Yescard, 84, 94, 95

Z

Zapp Mobile, 124

Zero-Knowledge Systems, 38

ZKS. *See* Zero Knowledge Systems