ELECTRONIC PAYMENT SYSTEMS OBSERVATORY-NEWSLETTER

ePSO-Newsletter – No. 12 – February 2002

http://epso.jrc.es/newsletter

Table of Contents

Focus: Standards for Payment System Integration

Other Articles

Leo Van Hove's Review Corner

Of Contacts, Correspondents and Disclaimers

The Institute for Prospective Technological Studies (**IPTS**), has established the "electronic Payment Systems Observatory" (ePSO) on behalf of DG ENTR within the ISIS programme. One activity of ePSO is the publication of this monthly electronic newsletter: **ePSO-N**. The Institute for Technology Assessment and Systems Analysis (**ITAS**) of Karlsruhe Research Centre has been commissioned to edit this newsletter (cf. [12&9] Masthead for details).

Michael Rader

co-ordinating editor
rader@itas.fzk.de

Yannis Maghiros

ePSO project leader
ioannis.maghiros@jrc.es

Browse or search the ePSO-Newsletter at http://epso.jrc.es/newsletter.
For subscription you may go directly to http://epso.jrc.es/newsletter/subscribe.cfm

[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.

[reply] To start discussion on this article in the ePSO-Forum just click the reply-button.

[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 load 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.

[reply] To start discussion on this article in the ePSO-Forum just click the reply-button.

[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-N: 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.

[reply] To start discussion on this article in the ePSO-Forum just click the reply-button.

[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 our 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.

[reply] To start discussion on this article in the ePSO-Forum just click the reply-button.

[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 unbanked 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.

[reply] To start discussion on this article in the ePSO-Forum just click the reply-button.

[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.bruenken@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.

[reply] To start discussion on this article in the ePSO-Forum just click the reply-button.

[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 it’s 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.

[reply] To start discussion on this article in the ePSO-Forum just click the reply-button.

[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 non-transit-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?

[reply] To start discussion on this article in the ePSO-Forum just click the reply-button.

[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.

[12&9] Masthead

Electronic Payment Systems Observatory-Newsletter
ePSO-Newsletter – 2002 – No. 12 – February 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 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)

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.

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