Electronic purse interoperability
Mike Hendry
Payment Systems Consultant

With the advent of relatively secure storage and on-board encryption, smart cards offer the possibility of storing value on a card. When the value is restricted to a closed circuit (for use, for example, in public transport or vending) then we call it a Stored Value Card. In Europe, at least, the term Electronic Purse is reserved for those cases where the value can be used in many different situations; this makes the value much more like cash, and central banks normally want to control its issuance.

Many organisations have seen the advantages such a scheme can offer in terms of:

- Convenience: not having to find the right change for a parking meter, road toll or telephone call; travellers can keep cash in several currencies without weighing their pockets down with change.
- Security: schoolchildren can be given money which can only be used for specific goods. With some schemes, if the child loses the card, it can be blocked and the money restored.

Around 100 organisations world-wide are already issuing such cards. Until very recently, none of these schemes was compatible with any other; the emphasis was on gaining market share in this new and exciting market. This was scarcely in their customers' interests, and many of them are now taking steps to try to ensure compatibility with at least a selection of other schemes.

This presentation takes a look at just what interoperability can offer, what it involves, and what steps the existing schemes around the world are taking to get there. With such a large number of schemes, it cannot be comprehensive, but it should give the broad picture to anyone who might be considering implementing a smart card-based electronic purse scheme, or even accepting purses in a retail or service operation.

What is interoperability?

The key aim is to allow holders of electronic purses issued by different issuers the ability to pay for goods or services using a single piece of equipment. Retailers just won't accept having two terminals for two card schemes.

If I pay for things, then my balance runs down, and eventually it runs out. Then I need to load it again. Conventionally, I can load a purse either using cash or from an account; it will be easier to provide the cash loading facility than loading from an account. It is also quite important for me to be able to check the balance on my card, so that I know when to reload it.

Where the card has other features - it may also carry my library pass or travel season ticket - these do not need to be interoperable with other schemes, since they will normally be valid only within a closed circuit.

Layers of an electronic purse scheme

Let us consider the components of the schemes we are trying to make compatible. An electronic purse scheme consists of four key elements:

- A brand: its name, and the logo which we use to recognise it
- Rules and procedures: these dictate how the scheme operates and what we can do with our money
• A security scheme: the all-important element which protects the value within the purse, allows value to be transferred securely from customer to merchant, and lets the scheme operator detect any security breaches.

• The hardware and software of the cards, terminals and network.

We could have two schemes using the same hardware and software, but simply not allowing compatibility because of their rules; conversely, we can use one piece of hardware to implement two completely different schemes (as they have done in Manhattan). In other words, we can have different levels of interoperation based on brands, procedures, security schemes and hardware; each is largely independent of the other.

In the next part of this paper we will look at the factors which make interoperation both difficult and yet possible to achieve.

Technical

To use a single card slot, cards must be the same shape and size: usually they will conform to the ISO 7816 standard. Some schemes use contactless cards, others use protected memory cards whilst a third group uses special high-security microprocessor cards. The ISO standard allows many options in protocols and timings, and schemes will make different choices as to which they use. Some schemes try to restrict the choice used by the terminal, which will limit the scope for interoperability. The ISO standard offers a very simple way of selecting an application from a list and negotiating a protocol; this allows us to implement a limited range of different schemes using different application programs - we do not need a single unified application, and indeed one promising approach would be to have a "Vanilla" application on every card allowing the lowest level of use and reloading.

Standards

To achieve interoperability, there must be some agreed standards. Standards take time to evolve, and so it is tempting for any powerful organisation to write its own and try to impose them on the rest of the world. It is already clear that this will not work in the case of electronic purses, and we need some consensus amongst the different groups and sectors involved. For true world-wide interoperability of all inter-sector purse schemes, it is likely that we would need a Public Key Infrastructure agreed, if not organised, between governments.

Operational

Schemes will differ from one another in the way they operate: for example, does the cardholder or the merchant insert the card? What currencies can be used - for interoperability, we need one or more common currencies. Can the card carry floats in several currencies and if so how do we select which one to use for each transaction? Does the scheme offer other services, for example the ability to link to a point of sale system to pick up the amount? And does the cardholder need to enter a PIN or provide another form of identification? Most schemes allow payment without a PIN.

Human factors

One of the difficulties faced by many electronic purse schemes is that of persuading customers to use their cards. Although the standard way to encourage use is through easily recognised logos in shops and on machines where the cards can be used, schemes often suggest, through their advertising, ways and places where the cards can be used - customers start to associate the card with a sector or type of payment rather than with the logo. The range of logos is so large as to be bewildering for many shoppers, and the range of card types has the same effect on most shop assistants.
We also have to recognise that people are different: the international jet-setter uses an epurse in a different way from a schoolchild, or from the African mine-worker for whom the card is a form of protection against being attacked just after drawing his salary. Schemes are successful because they hit a "hot button", meeting a current need with a large enough group of people. Different schemes will meet different needs.

**Commercial**

From the point of view of two operators seeking to make their schemes compatible, many issues need to be resolved: we need to ascertain which elements of the transaction incur additional costs, and who will pay these charges - the schemes may well amortise their fixed costs in quite different ways. One way in which electronic purses recover their costs is through the float - the money stored on the purse. (Although most open schemes are required to lay aside an equivalent amount of money, they can still earn interest on it). Who owns the float and how can it be transferred between schemes?

Many schemes offer additional benefits to their merchants, sometimes in return for a transaction fee. They may install or maintain terminals, including keeping the software and keys up to date. If they make their schemes interoperable with many others, this makes the task of maintenance much more complicated. And what happens if there is a fault, if a transaction is lost or if a merchant defrauds a cardholder? Who can be held liable?

**Legal**

There are major differences in financial law between countries, and this is made more complicated because it is often unclear how the law should be applied to electronic purses. Attempts by countries such as Denmark or Germany to clarify this only increase the differences from other countries. A common theme is cardholder protection, but countries protect their citizens' privacy and financial interests in different ways and to different extents, so it is important to know what jurisdiction applies to any given transaction. It will often be difficult for a card issuer to ensure that all its cardholders' rights are maintained all the time: it might be impossible to meet Italian requirements for tax disclosure and German law on cardholder privacy.

**Government and central bank regulation**

Governments must make and communicate clear decisions as to their attitude to electronic purse schemes. In the developed world, most governments take the view that such schemes are purely commercial undertakings; nevertheless they affect the money supply and so should be regulated to some extent. The potential "social benefits" (benefits which accrue to the whole of society, not just the operator or customers) of an electronic purse scheme include:

- Protection of children, older people and those less able to manage their money
- Reduction in theft, fraud and similar crimes
- Benefit payments can be targeted directly at the family member with the need, and indeed spending can be restricted to eligible transactions
- The payment card can be linked to other Government schemes, such as proof of age or entitlements.

Some governments have even been prepared to allow or encourage a monopoly electronic purse supplier. While this may be tempting in a small economy, it will tend to isolate that country when it comes to interoperation with other schemes.

A central bank will have other concerns about the way any scheme operates, and will want to ensure that it meets national requirements for reporting and controlling the money supply,
maintaining the stability and integrity of the monetary system, and preventing money-
laundering.

Electronic purse schemes world-wide

Round the world today, we can see four major groups of electronic purse schemes emerging:

- those linked to the Visa Cash brand (although they are not all the same technically) in
  Argentina, Australia, Brazil, Canada, Colombia, Hong Kong, Japan, Spain, the UK and
  the USA.

- Mondex (in the UK, Canada, Hong Kong and Manhattan). Mondex is now majority
  owned by MasterCard.

- the Proton schemes (Belgium, Australia, Brazil, the Netherlands, Sweden and
  Switzerland); American Express is now using Proton technology.

- those using contactless (Mifare) technology, for example in Australia, Brazil and Korea.

Zolotaya Korona, which operates in over 100 regions in the CIS, can also claim to be a
regional collection of purse schemes. Most of the remaining 20 or 30 schemes are free-
standing, operating within a single area and with no technical or commercial links to any
other. They include some quite large schemes such as Geldkarte in Germany and Chipper in
the Netherlands, and some of the longest established schemes such as Danmønt in Denmark,
Avant in Finland and PMB in Portugal.

Those schemes which use public key encryption (such as Mondex, Zolotaya Korona and the
more recent Visa Cash schemes) will be better placed for interoperability at the level of
security scheme, whilst the larger groups (such as Visa Cash and Proton World) will find it
easier to sort out the commercial issues. Contactless technology makes it easier to resolve
some of the ergonomic and electrical interface issues. There are, as we will see, many groups
working on the technical standards, but it is really only in Europe that there is any concerted
action to resolve the legal and regulatory differences.

Inter-scheme schemes

There are almost as many groups working on the interoperability of electronic purses as there
are separate schemes.

We have already mentioned the brand groupings: Visa Cash, Proton World, Mondex
International and Zolotaya Korona; they are important because they can help to set rules and
contractual conditions between their members as well as setting standards.

Among the more traditional standards groups, the European standards centre CEN has
produced a standard for inter-sector purses, but it is so general that many schemes can meet it
without being compatible with one another. This standard is being followed most closely by
the Global Chipcard Alliance: a grouping of telecoms companies, all of which issue prepaid
telephone cards and GSM smart cards, and their suppliers. Within the banking sector, the
spotlight has been on standardisation of credit and debit functions, through the "EMV"
(Europay - MasterCard - Visa) group, but EMV has decided that it will not attempt to
standardise electronic purses, for the time being at least. There remain co-ordination efforts
within the European Committee for Banking Standards and within the European Union.

Achieving interoperability

In the end, the driver for interoperation will come not from any technical standards but from
the desire of schemes to extend their scope and market share. Because schemes meet the
needs of different cardholders (and this differentiation is likely to increase rather than
Electronic Purse Interoperability

decrease), there will be a range of schemes with different characteristics. Retailers and other acceptance points will want to accept all cards, and their banks will want to acquire all their transactions. Where there is a commercial need for interoperability, the technology can easily find a way.

What is needed on the technical side is not a single specification, but a clearly defined set of standards and specifications, for both cards and terminals. Applications must be defined and written in a modular way, and schemes must be prepared to type-test both hardware and software modules.

The rules and procedures must be flexible and capable of being adapted to different accepting environments, customer needs and legal systems. They must allow acquirers and scheme operators to compete with one another.

Security schemes should include a public key element for authentication of the card, issuer and terminal; the actual value transfer may be symmetric or public key. Scheme owners should set up libraries of certificates which they can accept. There must be a minimum set of common message functions (probably restricted to selecting a currency, checking a balance, making payment and loading from cash or another external source). In order not to make cards too complicated, terminals must perform most of the selection and conversion tasks.

Conclusions

As the Manhattan trial has shown, schemes can achieve interoperability if they want to. Most scheme operators will want to maximise their commercial reach by joining one of a small number of international alliances; in the longer term, there is room for many small schemes serving closed groups or niche markets, but probably only three or four international and cross-sector schemes. It is likely that two or three of these will come from the banking sector, and at least one from the telecoms sector.

Barring some cataclysmic event, electronic purses will not displace cash during our lifetimes. But we can look forward to more convenient payment in some sectors and by some groups of society, and this will include a gradual increase in interoperability between schemes internationally.