A White Paper

The Euro in the Electronic Purse

Interoperability issues of smartcard based e-payments in Europe

Prepared by

the SmartEuro project partners

on behalf of

EUROSMART

This White Paper has been prepared thanks to the support of the European Commission's Framework Programme IV Esprit Project “SmartEuro” (referenced EP29196), with the contributions from:

Bruno	Allard	GEF
Edmond	Alyanakian	BBS
David	Ankri	OBERTHUR SMART CARDS
Thierry	Collin	DASSAULT AT
Bruno	Cucinelli	ARTTIC
Jean-Michel	Desjardins	BULL
Mathieu	Destrain	GEMPLUS
Bruno	Dupont	EURALIA
Fernando	Exposito	FNMT
Albert	Galloy	GEMPLUS
Charles	Goldfinger	GEF
Youzec	Kurp	OBERTHUR SMART CARDS
Alberto Perez	Lafuente	MICROELECTRONICA ESPAGNOLA
Mark	Salter	HITACHI
Tarik	Slassi	SCHLUMBERGER
Olivier	Trebecq	GEMPLUS
Leo	Vanhove	FREE UNIVERSITY OF BRUSSELS

Edited by:

ARTTIC
58A rue du Dessous des Berges
F-75013 Paris
Tel : +33 1 53 94 54 60
Fax : +33 1 53 94 54 70
Email : cucinelli@arttic.fr

Introduction

Well over one billion smartcards were manufactured in 1999. Although the majority were destined to become disposable telephone cards, around 400 million were true long-term-use smartcards containing personalised information related to a myriad of commercial and industrial applications, from the ubiquitous mobile phone to national health-care systems - the vast majority being for use within the European marketplace.

Europe was the birthplace of the smartcard and leads in both its manufacture and its applications. Europe was also the birthplace of the World Wide Web, enabling new trading opportunities for buyers and sellers alike. Such electronic commerce (e-commerce) demands new concepts in how goods and services are paid for. Digital or electronic cash (e-cash) enables a purchaser to pay for goods over the Internet in a truly anonymous way. E-cash behaves just like real-world cash, except the 'cash' is in the form of tokens rather than coins and bank notes. As e-cash is cash in electronic form and does not exist physically, there is a need for a medium to make it portable - which is transferable between one entity and another. Two such media are already well established to support e-cash, the Internet and the smartcard. The Internet enables e-cash payment for on-line merchants, and the smartcard enables e-cash payments for merchants in the real world. However only smartcard based e-cash has the potential to enable payments in both worlds, the real and the virtual world.

Electronic money (e-money) is a currency system where the electronic value is purchased by the consumer, and refers to a whole range of electronic payment methods including e-cash, credit (pay later), debit (pay now), and the newest product dedicated to electronic payment, electronic-purse (pay before). Electronic purse (e-purse) is a small, portable device that contains e-money, just like a real-world purse or wallet. It can be either disposable or re-loadable and the best medium for the e-purse is, of course, the smartcard.

Today, one of the major challenges for smartcard suppliers, acceptors and users is the integration of smartcards into these different, yet complementary, electronic payment systems.

For many applications that correspond to a large number of small (micro-payment) transactions, only real world card based e-cash payments make sense. Most small retailers (corner shops, pharmacists, newsagents etc) are unlikely to move to on-line trading in the short or medium term. Unattended terminals such as parking meters, ticketing machines and vending machines will always need to be 'fed' with real-world cash - albeit hard cash or e-cash. The smartcard is therefore the most suitable medium for the pervasive use of e-cash.

The smartcard addresses the need of e-cash portability perfectly, combining characteristics such as strong security on a low cost medium with ultra-portability, popularity and familiarity of many millions of consumers with the card's look and feel, ease of use. Smartcards are already deployed in their hundreds of millions in a myriad of applications ranging from the disposable 'phone card to the sophistication of individual's health-care records. The technology has thoroughly proven itself over many years in such applications as banking and mobile telephony. The smartcard provides independence from a physical location and specific application environments. The same card can potentially be used in a real world point-of-sale terminal or cash machine, as well as in Internet based applications, in mobile phones and Telematics terminals such as the French Minitel or public kiosk, in TV set-top boxes and pay-as-you-view video on demand.

On January 1st 2002 European citizens will be able to use their 'domestic-issue' Euro payment means (coins, banknotes, cheques) in any other country within the eleven

European Monetary Union (EMU) nations. It is therefore a basic requirement for e-cash that it can be handled as comfortably as traditional cash when the Euro becomes the single cash currency in Europe.

Despite the adoption of electronic payment by e-purse in many countries in the European Union, its overall acceptability is being hampered by the multiplicity of solutions that do not interoperate with each other. This is not just a cross-border situation - different, non-interoperable e-purse systems exist in the same country, preventing most e-purse programmes from attaining an economic balance and realistic return on investment for their issuers. Today there are some twenty-three e-purse schemes operating in Europe, either running 'live' or in trials, which are not interoperable either technologically or commercially. Furthermore, although all these systems focus on small-amount transactions (micro-payments), they are extremely diverse in their basic philosophy, design principles and technical choices. In this situation an e-purse can only be used on the terminals of its own scheme.

The freedom to use an e-purse issued by one e-purse scheme for transactions on the infrastructures of any other e-purse scheme can only exist if the schemes are interoperable. Interoperability and ubiquity are key for both consumers and merchants. The larger the deployed e-purse supporting infrastructure, the higher the value of the e-purse for cardholders and card acceptors. The e-purse must support Europe's citizens both in their own country and when travelling abroad, irrespective of how they chose to pay. With the introduction of the Euro as a cash currency, the ability to use an e-purse for payments in Euro in any country of 'Euroland' is obviously a key requirement.

In this context, two major factors would improve the acceptability and subsequent profitability of e-purses. The first entails combining different payment services on a single smartcard, with electronic cash added to each service. The other is by enabling interoperability between existing e-purse systems, both on a national basis and, with the introduction of the Euro as a cash currency, on a pan-European scale. At present, the technical infrastructure, the business practices between card issuers and acceptors, as well as commercial conditions for the use of card based electronic payment instruments varies from one European country to another. Interoperable systems not only require a technical infrastructure compatible with common standards, but also agreements on business relations, the management of common security and clearing procedures.

In March 1999 the Common Electronic Purse Specification (CEPS) was published - a major event in the e-payment interoperability domain and to date the most advanced initiative targeting interoperability of e-purse transactions.

Faced with this challenge, e-purse issuers are at the front line in preparing the required adaptations to their existing infrastructure. In conjunction with the European Committee for Banking Standards (ECBS), key organisations in electronic payment systems have already launched major initiatives to define elements of a common functional specification that will enable migration to interoperable schemes.

EUROSMART, the European smartcard industry association, working with card issuers (banks), card acceptors (merchants) and cardholders (consumers) is proactively involved in the global process of interoperability definition. As part of this effort EUROSMART members launched the SmartEuro project with support from the European Commission. The focus of SmartEuro was to determine the best conditions that would facilitate the interoperability of e-purses in the context of the introduction of the Euro as a cash currency. The project reviewed the current situation and analysed the requirements of card issuers, acceptors and consumers, as well as other industries involved in electronic payment solutions and services, national and European authorities, consumer and retailer associations. A working group of technical experts was established to identify and analyse different CEPS based e-purse interoperability migration scenarios with a view to validating the CEPS concept. A summary of the working group's findings is included in this report and the complete document can be downloaded from the SmartEuro Website - http://www.SmartEuro.net.

In April 2000 the project presented its findings, together with a set of recommendations, to the European Commission. With contributions from over thirty organisations involved in all aspects of electronic commerce and payments, the results of these investigations are the conclusions drawn are now presented in this book - The Euro in the Electronic Purse.

The SmartEuro Consortium would like to thank the following organisations for their invaluable assistance and support throughout the project:

Banksys
Banque de France
BBS
Bull
CECA
Chipper / Chipknip
Dassault AT
De La Rue
ECBS
Euralia
Eurocommerce
Europay International
European Central Bank
EVA
FNMT
GEF (Global Electronic Finance)
Gemplus
GIE Carte Bancaire
Hitachi
IEIC
Infineon
Ingenico
Interpay
La Poste Mercatel
Microelectronica Espanola
Modeus
Oberthur Smart Cards
Orga Kartensysteme GmbH
Philips Semiconductor
Proton World International
S4B
Schlumberger
Sermepa
SIBS
SNCF
Visa International
ZKA

Table of content

Executive Summary

This report is the result of an eighteen-month investigation by the members of the European smartcard industry association, EUROSMART, and their SmartEuro project supported by the European Commission. It examines the impact the Euro as a cash currency will have on electronic commerce and electronic payments using electronic money, especially the electronic purse or e-purse. It assesses the role of the smartcard based e-purse in cross-border transactions, from a business, technology and applications perspective. It argues the urgent case for interoperability between Europe's existing, emerging and future e-purse schemes.

Chapter 1 - Electronic commerce and electronic cash

Examines the state of electronic commerce in Europe today and the effect the Euro will have on this market when it becomes the single cash currency in 2002.

Chapter 2 - Electronic cash systems

Is devoted to examining some of the distinctions and differences between various electronic purse schemes across Europe - a cause for concern when the Euro becomes the European 'domestic' currency.

Chapter 3 - E-purse business

Looks at the economics of the electronic purse - the costs involved in establishing an e-purse scheme, the benefits and pitfalls of the e-purse as a replacement for hard cash, and the financial aspects of several of Europe's existing e-purses.

Chapter 4 - Essentials of E-purse interoperability

In a single currency domain it is essential to be able to use an e-purse between different schemes in different regions. The Euro creates a single currency domain (or market) for 290 million consumers. The Internet knows no boundaries. How can today's national e-purse schemes interoperate in such a market? What does interoperability actually mean in terms of security and international standards? This chapter looks at the technology and the existing and emerging standards for e-purse interoperability, as well as recent initiatives to create a Europe-wide common electronic purse specification.

Chapter 5 - Impact of interoperability for system suppliers

Looks at the impact interoperable e-purses will have for suppliers and manufacturers of card products and card readers. It looks at how these suppliers migrate their products to become interoperable whilst ensuring the mandated levels of system security from the e-purse card itself to the central processing system.

Chapter 6 - Card issuer's strategies

How card issuers in Belgium, France, Portugal and Spain are planning to manage both e-purses and interoperability. Their specific requirements and the constraints and challenges they face, are discussed in this chapter.

Chapter 7 - Card acceptors' expectations

Looks at how merchants see the growth of the electronic purse. Will they be prepared to accept it as a replacement for some cash transactions? What are their concerns and expectations? A section is devoted to vending machine suppliers and operators and the challenges they will face as electronic purses start to become the norm rather than the exception.

Chapter 8 - Consumers' expectations

Very little has been done to assess the reaction of the general public to the electronic purse. This chapter looks at some of the consumer opinions that have been gathered through various sources and presents an opinion on the factors that condition consumer attitudes - the main

The final chapter pulls together the investigation and makes some significant and far-reaching ***conclusions and recommendations*** covering all aspects of a European electronic purse - the potential business opportunity, the costs involved, the new infrastructures that will be required, and the technology and standards that will be needed.

1. Electronic commerce and electronic cash

Electronic commerce in Europe

Electronic commerce (e-commerce) offers enormous opportunities for consumers and for business in Europe. By the year 2002, 280 million people are expected to be connected to the Internet world-wide and the value of the business-to-consumer electronic commerce market is estimated to exceed 100 billion Euros (source: eStats). In many sectors such as financial services, Internet based transactions are already having a great impact on the way business is conducted.

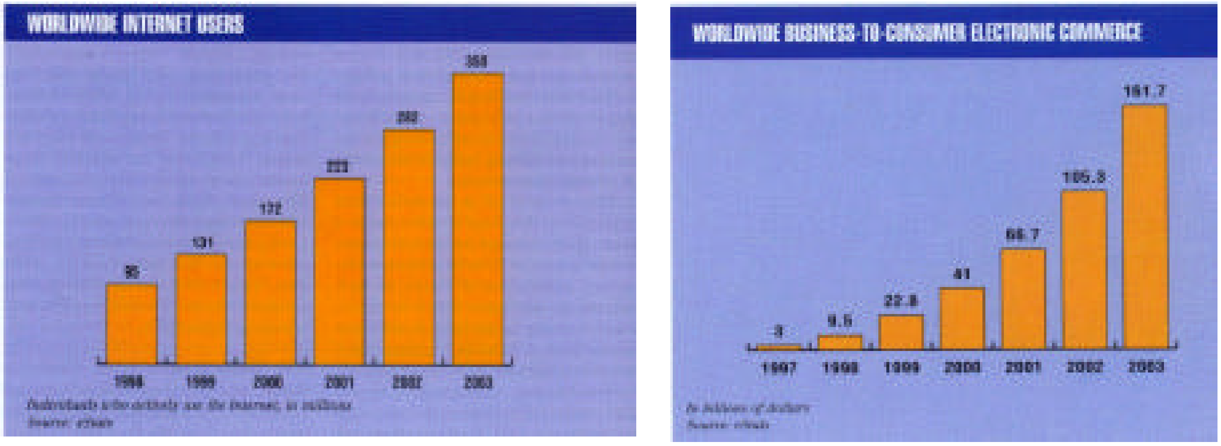


Figure 1: World-wide Internet users and B-to-C e-commerce
(Source: Card technology)

Europe is moving to electronic commerce. According to a recent Forrester Research study, by 2001 online revenues in business trade, consumer retail and content in Europe is expected to climb to over 70 billion Euros, with 53 million users connected to the Internet. Today, Finland has one of the highest Internet populations of any country world-wide. In relative terms there is more online shopping in the Netherlands than in the USA. The number of Web pages in Italy grew by over 600% in 1999, the highest growth in Europe.

It is anticipated that electronic commerce will be the driver for the modernisation of industry and services in Europe and the motor for the creation of many new business and employment opportunities. At the same time, e-commerce will have an impact on existing industries and patterns of employment. Across different countries and sectors 'critical mass' will be achieved in the coming years by companies who will standardise on doing business through the Internet.

In its initial report on this topic, the European Information Technology Observatory (EITO) concluded that the practice of some form of Internet based e-commerce (marketing, sales, purchasing or services) in Europe will multiply by a factor of eight in just three years - from 6% in 1996 to around 47% in 1999.

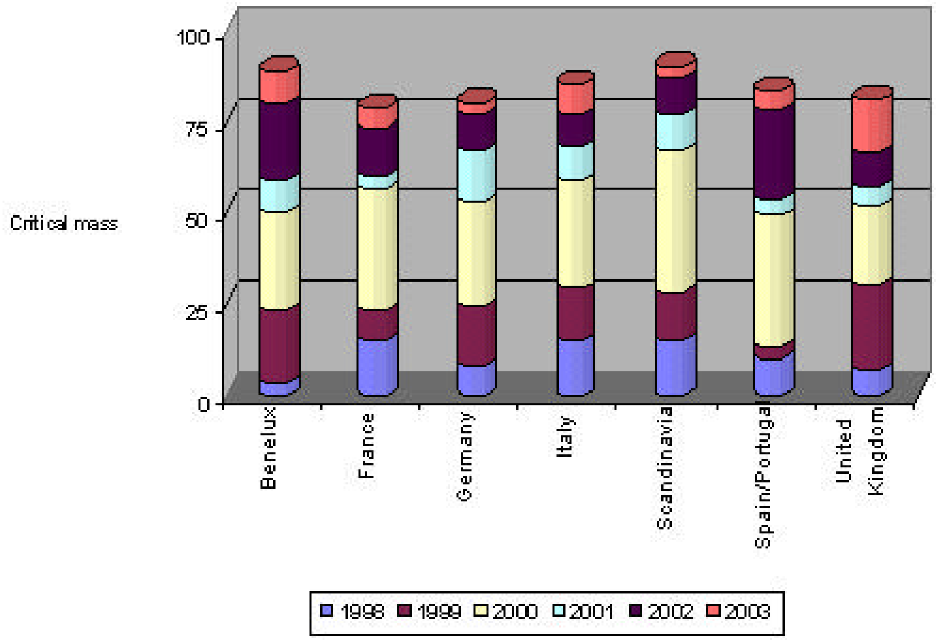


Figure 2: E-commerce penetration in Europe (source: EITO)

ANEC - the European association for the co-ordination of consumer representation in standardisation - has stated that to achieve the enormous predicted growth in e-commerce, not only the demands of business must be met but also the demands of the consumer. E-commerce will have to compete with existing methods of making purchases and completing customer transactions. Consumers have a choice as to how they make their purchases and they will not be slow to exercise that right.

ANEC has identified the following as the main consumer priorities for electronic commerce:

- Interworking between standards
- Standards for all delivery technologies
- Research into consumer aspects of e-commerce
- Security
- Privacy
- Design for all
- Error tolerance
- System status information
- Cost transparency
- Order confirmation.

The Euro and e-commerce

The single European currency is a paradigm shift for Europe, where confidence must be established in an exchange currency on the basis of financial policies carried out by different sovereign authorities. Under such circumstances, monetary confidence presupposes perfect financial orthodoxy based on the management of bank guarantees.

The immediate consequence of such centralised management is the dematerialisation of monitoring, traceability and transparency in companies' operations and risks. Electronic commerce will solve a large number of the issues raised by the single currency through the management of financial guarantees in real-time.

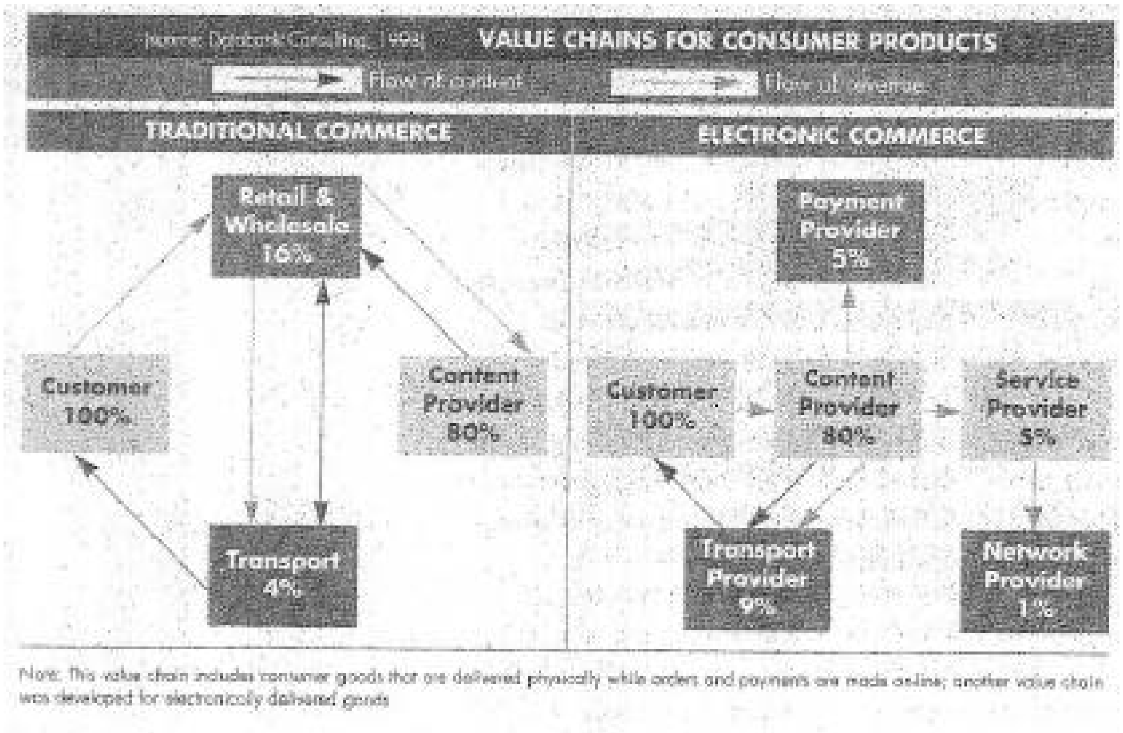
It is anticipated that European Monetary Union will strengthen the position of Europe as an economic power. As an entity, the Union will produce 20% of world exports and the European Central Bank will have four-times the reserves of the US Federal Reserve. From a business perspective, the introduction of the Euro will bring about lower transaction costs, as companies in member countries will no longer suffer from exchange rate fluctuations when doing business with each other.

The Euro will give Web merchants access to a market of 290 million people, all of whom can be sold to in a single currency, boosting European e-commerce. The Euro will remove the barrier of multiple currency transactions that today holds back many users from shopping online and vendors from launching e-commerce sites. Gartner Group predicts that by 2001 the number of cross-border, business-to-business e-commerce transactions in Europe will increase by 60% to 100%. In the business-to-consumer market, they estimate that the increase will initially be more modest, at between 25% and 50%, but that the introduction of the Euro as a cash-currency in 2002 will greatly increase business-to-consumer electronic commerce.

With all goods priced in Euros, businesses and consumers will easily be able to compare the price of items sold in different countries, without having to calculate exchange rates. Furthermore, e-commerce coupled with the Euro will put considerable pressure on companies to equalise their prices across Europe.

Electronic payments and e-commerce

The Internet has created a huge potential for electronic payment systems. E-commerce cannot happen without e-payment facilities and services. Consequently, financial services, such as Internet banking, are a critical market segment for e-commerce.


(source: Databank Consulting, 1998)

Note: this value chain includes consumer goods that are delivered physically while orders and payments are made online; another value chain was developed for electronically delivered goods

Figure 3: Changing value chain from traditional commerce to electronic commerce

The relationship between electronic commerce and electronic money is complex. One of the key requirements of e-commerce is the ability to make secure payments over the Internet. There is growing consensus that this could be achieved by a Public Key Infrastructure (PKI) and Digital Signatures (DS). As various projects to implement PKI and DS progress, it is becoming apparent that smartcards can play a very useful role in the management of public key and digital signatures. As an example, the Secure Electronic Transaction (SET) protocol for the use of credit cards over the Internet relies on digital signatures and is slow and inefficient. When smartcards are introduced to handle key and signature management performance improves dramatically. As well as increased system efficiency, smartcards offer another major advantage - secure mobility. Customers are no longer tied to their computer to carry out secure transactions but can use any Internet terminal with a card reader. For these very reasons, EUROSMART anticipates that by 2005 some 30% of Internet transactions will be made via smartcards.

For the banking sector and its card segment, the Internet represents both a major opportunity and a threat. Internet banking is becoming significant business and is likely to represent one of the largest areas of e-commerce. If the SET protocol becomes a major medium for retail payments, then it would firmly anchor the bank card in the Internet universe. However, because it would not be actively involved in public key infrastructures and digital signatures management, the banking sector run the risk of alternative secure settlement channels emerging, leading to their role as financial intermediaries being reduced. Internet Service Providers (ISPs) or other specialised suppliers could establish secure billing arrangements to handle on-line transactions, particularly for very small payments. Banks would of course hold final balances for ISPs and suppliers but would lose direct customer access and transaction processing business. Killen and Associates, an American consulting company, estimate that by 2001 non-banks could capture as much as 50% of Internet-based smartcard transactions.

Obviously such an outcome is not pre-ordained. Some European payment organisations are already seeking to integrate smartcard and Internet. Mondex, for instance, considers the Internet as one of its strategic priorities and is working with banks such as Wells Fargo to design a Multos-based card for Internet banking. In the UK, Barclays Bank has launched a smartcard called 'Endorse' to manage digital signatures for authentication purposes. In June 1998, the French organisation 'Groupement des Cartes Bancaires' (GIE-CB), together with France Telecom and Europay France, created a new company - Cyber.com - that will allow the use of French bank cards for SET transactions. The stated objective of Cyber.com and its shareholders is to create an international standard, which integrates SET and the smartcard.

Electronic purse and the Internet

E-commerce is considered as one of the driving factors for the electronic purse. The e-purse provides a micro (i.e. very small) payment solution for Internet based on-line transactions, enabling the Internet to potentially increase the added value of the e-purse for its user. For example:

Electronic payment for low value goods (books, CDs, shareware software, on-line information, cinema tickets, pizzas, etc.) requires a cost-effective solution for micro-payments. Traditional debit/credit card transaction costs are too high for payments of such small amounts. E-purses can operate more cheaply and support business-to-consumer e-commerce for small transactions, providing both parties with the highest level of confidence - even for consumers with a poor credit history. E-purses do not need to be linked to a specific bank account for carrying out Internet-based payments and do not require confidential data (credit card numbers, etc.) to be transmitted across the Internet.

An Internet enabled e-purse provides the user with a number of benefits that increase the added value for the user of the e-purse over physical cash. The Internet provides the e-purse with a number of features (such as the on-line withdrawal, deposit or transfer of electronic cash) independent of the user’s physical location.

2. Electronic cash systems

The idea of replacing physical cash by smart-card based e-purses has generated considerable interest amongst financial institutions all over the world. This is especially true in Europe, where the level of development, the number of pilot sites and actual deployment activities is very high and growing on almost a daily basis.

All told, there are seventy-two e-purse systems operating (either as pilots or as live systems) in thirty-nine countries world-wide. This includes twenty-three schemes operating in sixteen European countries. Although all these e-purse schemes have focussed on small amount transactions, they are extremely diverse in their basic philosophy, design principles and technical choices. Whilst there would not seem to be many ways of designing a physical cash system, there appears to be a considerably variety of approaches to electronic cash. Furthermore promoters of various initiatives have traditionally shown little interest in compatibility and interoperability with other schemes, to the extent that in mid-1998 none of the European e-purse schemes were interoperable with each other.

Distinctive e-purse features

There are two key distinctions in e-purse system design:

1. Between disposable and reloadable cards.

   A disposable card functions in a similar fashion to a public 'phone card. It is issued for a fixed amount and once this amount has been used the card is thrown away. One of the advantages of the disposable card is that it does not need to be linked to a bank account.

   In case of a reloadable card, the system allows for the recharging of the card once the value on the card has been used up, enabling the card can be used again. The easiest approach to reloading the card is via the bank account of the cardholder. The great majority of e-purse systems today are based on reloadable cards, although the method of the reloading process varies.

2. Between accountable and non-accountable systems.

   This distinction defines the extent to which e-purse transactions are centrally cleared, settled, recorded and tracked as the basis of the audit trail for the transaction. Some systems are closer to a traditional cheque/card scheme, where all transactions are linked to specific accounts and centrally cleared and recorded. Others seek to emulate the characteristics of cash transactions between parties, which are anonymous and therefore less traceable.
   In an accountable system the value transfer from a card to a terminal may be immediate, but the settlement between the issuing and acquiring institutions is deferred and consequently could be revoked.

   In non-accountable systems the value transfer is immediate and irrevocable. Ultimately, the value is not settled but needs to be redeemed from the issuing institution.

These distinctions define a range of trade-offs between e-purse manufacturing costs and processing e-purse transactions on the one hand, and the operational and financial security of e-purse schemes on the other. Non-reloadable cards are less expensive to manufacture and to process than reloadable ones. Non-accountable e-purse schemes are cheaper per transaction than the accountable ones. Conversely, reloadable and accountable schemes offer greater operational control over e-purse transactions for issuing institutions. They also enable regulatory authorities, concerned with the soundness of electronic money and its macro-economic impact, to more closely monitor e-purse systems.

E-purse schemes in Europe

The following overview of existing e-purse systems shows that at present there are a number of non-interoperable schemes existing in an almost autonomous world, confusing card acceptors and consumers alike.

The current trend is to offer multi-function cards that combine an e-purse with other payment applications. Stand-alone e-purses are a difficult business case to justify, due primarily to the total system costs involved. The cost of the whole e-purse system (cards, card readers, payment transaction management network, etc.) must be paid for by all those involved with a stand-alone e-purse system - the banks (issuers), the acquirers (Visa etc.), the merchants (acceptors) and the customers (cardholders). This is difficult for the merchants and cardholders to accept as they are used to receiving and paying with real cash, which they perceive as 'free'. In fact, real cash is not free but its cost is socialised, so appears as free for the individual. Stand alone e-purses for closed environments do not have this constraint as their users have very little choice. For example, closed environments where not adopting the e-purse can have significant drawbacks - such as the phone cards, student cards and corporate cards used to pay in canteens or on vending machines.

A consumer is unlikely to be prepared to pay for a card that does no more than 'free' real cash. However, a multiple service card can be perceived as having added value. Combining the e-purse with other applications (credit / debit, transport ticketing, etc.) enables the system costs to be shared between the various applications and increases its intrinsic value for those involved. The opportunity to dovetail an e-purse with standard credit and debit business, loyalty scheme etc. can provide value-added services for transaction business - such as small-amount payments for parking, vending machines, Internet purchases, news agents and transport ticketing - providing enhanced usefulness & convenience for the cardholder, as well as off-setting some of the global costs for all concerned.

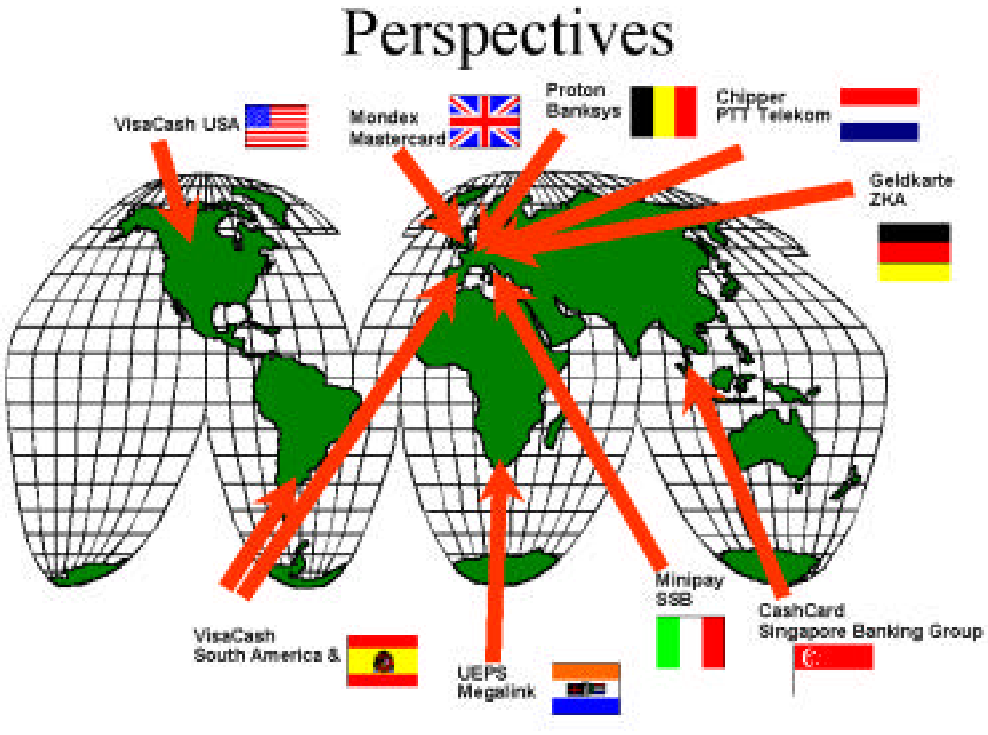


Figure 4 : Overview on e-purse schemes

The following table provides a general overview of existing European e-purse systems be interpreted as indicators of commercial success or acceptance by card acceptors and consumers. Consequently, the card volume figures shown in the table have been gathered from various sources, including publications and should therefore be treated with some caution.

E-purses are often combined with other payment functions - such as debit/credit - on the same card. In these cases, the e-purse function available to the cardholder may or may not have been activated. Figures for the number of activated cards compared to number of total cards issued are rarely available. It is also difficult to obtain accurate figures for the average number of transactions per card in a given time period, or the number of e-purse accepting devices in a given region. These differences may be quite important. For example, there are about 2.3 million PMB e-purse cards in circulation in Portugal, of which only 384,000 (16%) had been activated by December 1998, whereas of the 1.55 million Spanish Euro6000 e-purse cards in circulation, some 425,000 (27%) have been activated. In November 1999, Proton claimed seven million cards in circulation in Belgium with about three million (42%) activated.

Scheme	**Country**	**Starting date** (pilot phase)	**Cards in Circulation**[1] (January 2000)	**Reloadable / disposable**	**Euro / CEPS adoption ***
Avant	Finland	Jan. '94	1,550,000	35% reloadable 65% disposable	Yes / ?
Cash Sweden	Sweden	Nov. '95	2,500,000	reloadable	No / Yes
Cash Switzerland	Switzerland	July '96	3,800,000	reloadable	No / Yes
Chipknip	Netherlands	Oct. '95	12,500,000	reloadable	Yes / Yes
Chipper	Netherlands	3Q '95	7,000,000	reloadable	? / Yes
Danmønt	Denmark	Sept. '92	1,800,000	99% disposable	No / Yes
Euro 6000	Spain	July '96	1,000,000	reloadable	Yes / Yes
GeldKarte	Germany	April '96	50,000,000	reloadable	Yes / Yes
miniCash	Luxembourg	January '99	230,000	reloadable	? / ?
Minipay	Italy	June '96	1,000,000	reloadable	Yes / Yes
Mondex	UK	July '95	100,000	reloadable	Yes / No
Monedero 4B	Spain	Oct. 95	1,500,000	reloadable	Yes / Yes
PMB (Porta Moedas Multibanco)	Portugal	End '94	3,200,000	reloadable	Yes / Yes
Proton	Belgium	Feb '95	7,100,000	reloadable	Yes / Yes
Quick	Austria	Dec. '94	4,500,000	reloadable	Yes / ?
TIBC VISA Cash	Spain	Feb. '96	4,480,000	reloadable	Yes / Yes
VISA Cash[2]	Italy - Bormio		90,000	disposable	? / -

* Source: Card Technology

Table 1: Overview on e-purse schemes in Europe

With respect to the number of trials, the leading e-purse scheme is Mondex with trials in some 50 locations, however none of these has yet been rolled out nationally. Geldkarte is the largest e-purse scheme in number of issued cards - 50 million at the end of 1999 - and Proton

[1] 'Cards in Circulation' applies to issued cards which are, or which contain, an e-purse. It should be noted that such cards may or may not be in actual use.

[2] VISA Cash (Bormio) figures are difficult to monitor as holiday resort card volumes depend on

for the total number of transactions, at around 45 million annually amounting to a total of 120 million transactions by January 2000.

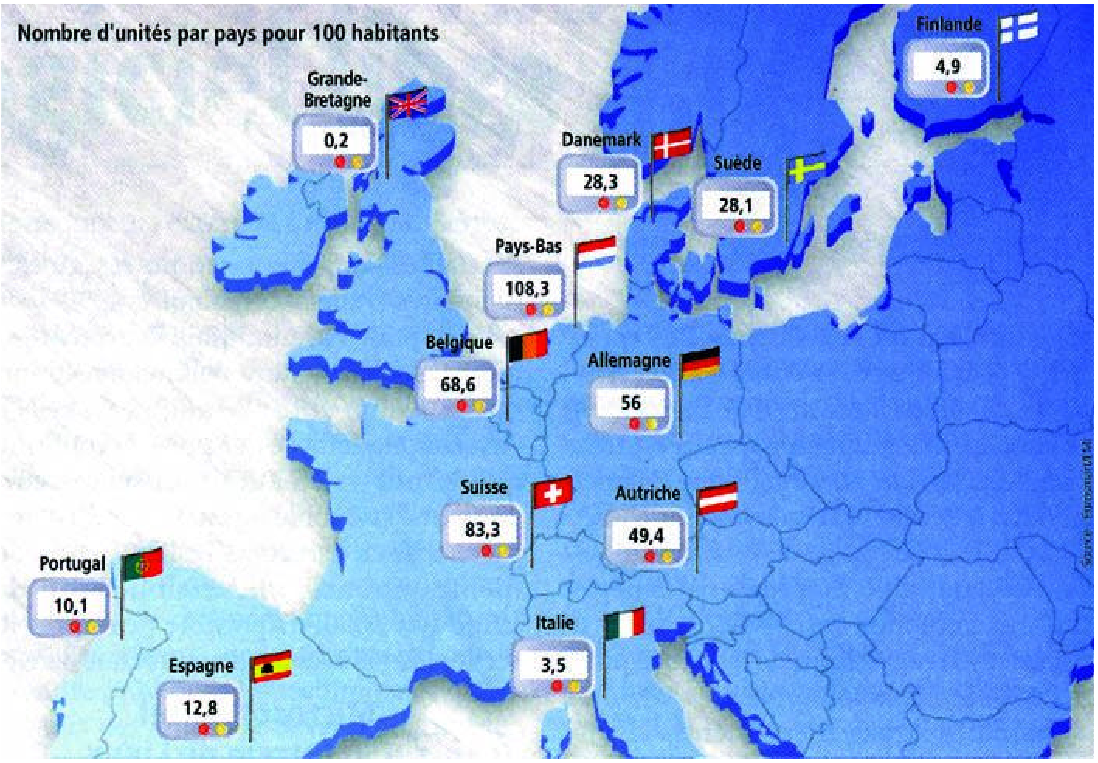


Figure 5 : Penetration rates of e-purses in European countries
(Number of e-purse users per 100 inhabitants)

Source: Le Monde de l' Informatique

Characteristics of different e-purse systems

To highlight the different concepts used in European e-purse schemes , some of their main characteristics are listed below:

Proton - Belgium

History

- Conceived in 1989.
- Introduced in Belgium in February 1995 and rolled out partly in May 1996 and second in September 1996.
- Banksys is acquirer and banks are issuers.
- Today, Proton counts such organisations as VISA International and American Express as very significant shareholders.

Type of Scheme

- PIN always required for loading, not required for purchase
- Float is held by Banksys but shared with issuers per daily monitoring and reconciliation

Mondex - UK

- Conceived in 1990 and originally launched by National Westminster Bank.
- First release of specifications in 1994
- Operated by MONDEX

Type of Scheme

- Purse to purse transfer
- No transaction detail
- Security based on RSA

VISA Cash - USA

History

- Conceived in 1989
- First release of specifications in 1995
- Operated by VISA International

Type of Scheme

- Connection with VISA network
- Float management by issuer
- Payments traceability
- Multi-currency
- Two phases in the scheme :
  - disposable card
  - reloadable purse and/or multi-application card
- Server provider
- Agreement of card and equipment

GELDKARTE - Germany

History

- First trial in March 1996
- Rolled out in October 1996
- All banks act as issuer; Banks and POS network providers act as acquirers

Type of Scheme

- No PIN verification for payment
- PIN verification for loading
- Float is held by the issuing bank
- Security based on 3-DES

EURO 6000 - Spain

History

- Introduced in February 1997
- First release of specifications in 1996

- Member banks are issuers and CECA (Savings Bank federation) is acquirer

Type of Scheme

- Based on CEN 1546 standard
- Can be loaded in whatever currency the cardholder desires
- Security based on 3-DES
- Multi-application card
- Reloadable purse
- PIN verification for loading

As can be seen from the variety of different components within the above schemes, achieving true interoperability between the different systems presents an interesting challenge for today's European e-purse operators.

E-purse systems in Europe

Proton / Banksys

The Proton card was developed by Banksys, which manages the major banking payment systems in Belgium (Interbank, ATM and EFT-POS). Banksys began to develop the Proton system in 1992. Pilot projects were launched in 1995 and national roll-out began in May 1996. In November 99, there were over 7 millions cards in circulation with about 3 million actually activated. There are now about 40,800 terminals supporting e-purse load transactions and about 58,300 card accepting devices supporting payment transactions (merchants, vending machines, parking, public phones)

Proton has been designed as a reloadable and fully accountable system. The Proton card is loaded from a bank account and all transactions are fully accountable, with centrally available audit trail. Fraud detection algorithm monitors balance evolution and allows card black-listing. At the same time, the Proton server has built-in safeguards to prevent either Banksys or the government from surreptitious access to transaction details.

Value loading on the card can be done from an ATM; from a public payphone which has been fitted to accept the Proton card; or from home via a 'smart phone', designed in association with Belgacom, the main Belgium telephone company, or via the Internet using a dedicated terminal, C-ZAM/PC. Loads are carried out on-line, while merchant terminal purchases can be carried out off-line. Proton guarantees end-to-end security of its system via HSM (Hardware Secure Module) and SAM (Secure Access Module) and DES for the card.

Proton can be reloaded with amounts raging from 100 BEF (2.5 Euros) to up to a maximum of 5000 BEF (124 Euros). The average amount of a transaction is 6.23 Euros for purchases at merchants and 0.63 Euro at vending machines. The average amount loaded in the purse is 25.48 Euros.

Basis economic data of Proton:

- Card cost : 100 BEF (2.5 Euros) to Proton, 200 BEF (5 Euros) annually for the customer.
- Terminal cost: around 20,000 BEF (500 Euros) to the merchant;
- Load fees to the customer 20 BEF (0.5 Euro) daytime and 10 BEF (0.25 Euro) overnight

- Merchant fee: 0.45% (down from 0.9% initially).

While Proton has been designed primarily for e-purse and small amount purchases, its promoters believe that the technology has a much wider application. It is already used for instance in the Belgium health insurance card scheme and pilot projects are under way (or under consideration) for loyalty, contactless ticketing and multifunctional cards. Banksys has entered into a strategic partnership with ERG, an Australian system integrator, which, among things, has designed and operates the Octopus Hong-Kong transit project. Intensive technology development effort is accompanied by aggressive marketing strategy in Belgium and internationally.

The Proton technology is owned by Proton World International who has been very successful in exporting it. Proton World has Visa International and American Express as major shareholders. By May 1998, Proton technology had been sold to payment organisations in 15 countries, including The Netherlands, Sweden, Switzerland, Malaysia, Brasilia, Canada and United States (American Express). Proton World announced a total number of over 50 million cards in circulation world-wide in November 1999.

Proton World attributes its success not just to its basic technology but also to its marketing flexibility. Each Proton licence purchased can be adapted to the specific needs of the licensee and, more importantly can market under its own brand.

Mondex

Mondex differs radically from Proton both in its technical design and its marketing approach. The system was originally created in 1994 in the UK as a joint venture between National Westminster Bank, Midland Bank and British Telecom. Its first pilot was launched in 1995 in Swindon.

More than other monetary stored value cards, Mondex stresses cash replacement as its primary focus. Each transfer occurs directly between the involved parties. Value can be transferred directly and immediately from one customer card to another (using an electronic wallet or another reader). Mondex works off-line without a third party clearing system, which means it has no ability to centrally monitor transactions - transaction history of which is stored on cards and on merchant terminals. As with traditional cash-based systems, the total monetary value circulating is fixed. In order to avoid value leakage, the system is absolutely closed. Only the system Originator can create or destroy Mondex value. Banks participating in the system and issuing cards have to remain collectively under the ceiling fixed by the Originator.

Mondex transactions can only take place within the Mondex system. Consequently, even though Mondex is multi-currency (up to five), each currency is handled separately. If a UK customer wants to load US dollars on his card, he will receive 'digital' dollars issued by the Mondex Originator for the United States.

The major implication of this system design is a need for an extremely high level of security and strong encryption to ensure secure authentication and communication. For this reason, Mondex has implemented a public key cryptography (RSA) on its cards and readers. Because of the strong encryption, Mondex can use open communication networks such as the public telephone system or the Internet. Mondex can therefore be used for secure financial transactions over the Internet and several pilot projects were launched in this area.

Because of its sophisticated chip design, the Mondex card is considerably more expensive than the Proton card, with a unit cost estimated at between 8 and 10 Euros. Mondex management believe that this higher cost is more than offset by the economical non-accountable system design that avoids monitoring and central processing of a huge amount of transactions.

While Mondex has been designed specifically for electronic cash handling, the sophistication of its design, particularly at the card level, led its promoters to believe that it can be used as a operating system, which aims to become the open industry standard. However, the notion of a closed system and proprietary technology is reflected in a marketing approach that stresses the unity of the brand. Mondex seeks to franchise its technology through local association with leading banks and technology providers.

Mondex has been extremely successful in gaining endorsements from major financial and non-financial organisations. Among its supporters and shareholders are some of largest banks in the world, such as Hong Kong Shanghai Bank (HSBC) or Chase Manhattan. Its technological partners include AT&T in the United States (until mid-1998) and Hitachi in Japan. The most spectacular indication of institutional support has been the massive investment of MasterCard, which in 1997 took a 51% stake in Mondex international and its affiliates, in a series of transactions amounting to close to 100 million US$. This means that the second largest global banking network has endorsed Mondex technology as one of the main, if not the main, vectors of migration to the smartcard.

At the same time, Mondex remains highly controversial. Articles have been published about its vulnerability to hacker attacks and many banks on the European continent are adamantly opposed to the concept itself, which in their view does not conform to the requirements of the European Central Bank set out in its August 1998 report on electronic money.

Doubts about technological and economical viability of Mondex are reinforced by its limited presence on the ground. As of May 2000, there was nowhere in the world that Mondex had been deployed on a scale comparable to Proton World or Geldkarte. Its largest installation is in Hong Kong, where there are about 300,000 cards in circulation. Furthermore, the various Mondex pilots in different countries have not been viewed as particularly successful.

The disparity between the level of institutional support and that of market acceptance raises an interesting question on how the Mondex system will evolve. At present, Mondex have chosen not to support CEPS. However, MasterCard's 51% share backing of Mondex International is highly likely to keep the competitive pressure on other schemes. According to the Financial Times, changes of direction are being discussed, as described in the following article published on 29 November 1999:

> 'A realignment of the smartcard industry is looming after the decision by Mondex International, the London-based electronic cash group, to seek new investors apart from the banks that make up its shareholders. The company, in which credit card association MasterCard has a majority stake, is looking for a strategic partner to raise £30m ($ 48m) and provide access to new markets. But a full sale or flotation of Mondex has not been ruled out, with leading technology or telecom companies considered potential buyers.
>
> Both Microsoft and Sun Microsystems, the leading rival providers of operating systems that make smartcards work, are considered possible buyers of Multos, the operating system developed by Mondex. A move by either to buy Multos, the only system yet to pass rigorous security testing, would give them a dominant position in the rapidly growing market for multi-function smartcards. However, they would have to accept that their systems - Windows for Smartcards and JavaCard - were inferior. […]
>
> The decision to seek new investors has not yet been cleared with MasterCard, which owns 51 per cent. Any significant new share issue would dilute its holding and leave it without a controlling stake, which could be a barrier to any deal. So far Mondex, which was spun off from National Westminster Bank in 1996, has succeeded in licensing its e-cash product to more than 50 countries, most recently Mexico and South Korea, but only about 1m Mondex cards have been issued through a series of local trials.'

VISA Cash

VISA has taken yet another approach to the e-purse, which could be called the 'hundred flowers' approach. Rather than rely on a single technology developed in-house, VISA launched a considerable number of pilot projects under a common name VISA Cash, using a variety of technologies. Some of these technologies have been licensed from existing e-purse systems suppliers, such as Danmønt in Denmark and SEMP in Spain. The underlying idea being to test market reactions to different technical and conceptual approaches.

In some of its pilots VISA tested the use of disposable cards. These are well suited for temporary events with a large, transient population that does not have a local banking account. A large-scale disposable card pilot was launched during the summer Olympics of 1996 in Atlanta, in conjunction with the three largest regional banks - First Union, Wachovia, and NationsBank participating as card issuers. VISA Cash was accepted at the Olympic venue and by several Atlanta merchants (4,300 terminals were installed including public transit and payphones). During the games, 1.5 million disposable cards were sold and hundreds of thousands of transactions carried out. After the Olympics, participating banks intended to continue offering VISA Cash cards to their own customers.

In 1998 there were more than seventy VISA Cash pilot programmes in thirty countries world-wide, including the UK, Argentina, Australia, Brazil, Japan and Russia as well as in the USA. Some of the pilots involved only a reloadable purse (Spain, UK), while others combined purse and debit functions (Argentina) or purse and credit (Japan), while still others sought to use VISA Cash for Internet payments. All together, some 8 million VISA Cash cards have been issued.

The variety of conceptual and technological approaches adopted by VISA means that various VISA Cash e-purses are not interoperable and cannot be used outside their original sites.

VISA Cash is a part of the broader smartcard strategy of VISA. This strategy emphasises the EMV (Europay/MasterCard/VISA) standard and the evolution to multi-functional cards. From the technological standpoint, VISA itself has made a major commitment to JAVA as its preferred operating environment. VISA has also recently announced it will use the Java programming language for its new cards, enabling it to overcome the interoperability issue existing in its current pilots.

ZKA/Geldkarte

The current largest national e-purse scheme was launched in Germany in 1996. It is a collaborative project between German banks, spearheaded by ZKA (Zentral Kreditausschuss), bringing together professional associations of various banking institution categories throughout Germany. Geldkarte competes with two other schemes - PayCard, launched by Deutsche Telekom, the German Post-office and the national railway company, and P-Card, launched by a merchant association (EBS). However, based on the number of cards issued (50 million) Geldkarte is by far the largest scheme. Originally launched on a pilot basis in April 1996, its national roll-out began on January 1, 1997. By the end 1999, some 50 million cards had been issued.

Geldkarte is intended for small payments of between 5 and 25 DM (roughly 2 to 13 Euros). The system is reloadable and accountable. A customer can download the money (up to 400 DM (250 Euros) from their bank account at one of 20,000 re-fitted ATMs. Every amount downloaded is credited to a special account at the card issuing bank and reported to the Data Monitoring Centre. The Centre tracks a 'shadow balance', logging all downloading and payment activities carried out by the card. This allows for the rapid detection of a possible manipulation of the system. System security is guaranteed by an encryption protocol, based on a 'challenge response method'. All commands are integrated in the memory so that external re-programming or a retrieval of the encryption keys is not possible, at least within a justifiable amount of time. Every attempt to manipulate the key ends up in the destruction of all data stored in the security sector, thus making the card useless.

Geldkarte is accepted at 65 000 POS terminals. All transactions are carried out off-line. No PIN is necessary. Transaction fees to merchants are 0.3% of the value, with a minimum of 0.05 DM including the bank clearing fee.

The Geldkarte has been designed to permit additional information to be included on the chip, savings banks intend to use the Geldkarte for authentication purposes in home and Internet banking. Geldkarte also seeks to expand internationally. Agreements have been signed with major French and Luxembourg banks to launch pilot projects in those two countries. In September 1998, ZKA signed a commercial agreement with Europay to facilitate the international acceptance of Geldkarte technology.

CLIP

Based on the Common Electronic Purse Specification (CEPS), Europay International has announced CLIP, its interoperable e-purse belonging to the "Pay Before" family. The first CLIP pilot will be launched at the end of 2001. The e-purse will be able to carry ten different currencies and to operate world-wide. CLIP is intended for small payments of up to 150 Euros. It offers cardholders the possibility to load value from a bank account through an on-line connection to the bank. CLIP also offers cardholders the facility to load their purse even if there is no direct link between the e-purse card and a bank account, with funds coming from other payment product such as a credit card account, a debit card account, (traveller) cheques or even from a cash deposit.

All transactions will be carried off-line. PIN verification will be necessary for loading but not for purchasing. A key element of the security of the transaction is the mutual authentication of a genuine card and a genuine terminal using RSA, together with the guaranty of the integrity of the transaction details along the whole process. CLIP will also offer the possibility of making consecutive and linked low-value payments during a single purchasing action, such as telephone conversation, photocopier, etc.

The aim of Europay International is to expand CLIP internationally. Full specifications of the product are still to be finalised, however the CLIP product will be fully compliant with CEPS features (for more details on CEPS, refer to the section on CEPS features in Chapter 6). CLIP will be seen as an added-value application to Debit and Credit.

E-purse pilots

France

Although France was the pioneer of smartcard technology in Europe, it is one of the last European countries to actually introduce e-purse schemes. Three competing e-purse schemes were announced in 1999:

- **Monéo**: Seven French banks, including Crédit Agricole, BNP, Banques Populaires, CIC, CCF and Crédit Lyonnais and Crédit Mutuel have started to pilot an e-purse based on Geldkarte type technology in the city of Tours. 100,000 cards were distributed between October 1999 and January 2000, which represents one card for every three inhabitants, and 2,000 terminals (merchants, vending machines, parking) deployed. Three card types will be trialed: a dedicated e-purse, an e-purse combined with a banking card, and a disposable e-purse.

  Main characteristics : Combination of a B0' type banking card and a Geldkarte-type e-purse card. Both reloadable and disposable e-purse cards.

- **Modeus**: The Paris transport authority (RATP) and French state railways (SNCF) will pilot Modeus card which will use contactless technology on the subways. The banks involved in this trial are La Poste, Société Générale, Caisses d'Epargne and Banques Populaires. The introduction of the e-purse was initially planned for 1999 but had to been delayed due to the difficulties in reaching the required security rating. A large scale deployment is planned for spring 2,000

Main characteristics: combination of transport ticketing application (contactless operation) and e-purse for micro-payments in the public transport service area (newspapers, snack, etc.). The use of the contactless interface for payment transactions at merchants will also be evaluated.

- **Mondex**: Crédit Mutuel's franchise right to Mondex. Mondex is a centralised system requiring a central point for processing transactions in each currency. A pilot was planned to start in June 1999 in the city of Strasbourg, but was delayed due to the difficulty to chose an originator of Euros for Mondex (the Mondex scheme allows only one originator per currency world-wide). The Mondex card runs on MULTOS 4.0 and supports multiple applications (ID, loyalty, credit/debit, e-purse) as well as providing e-purse payments in Euro. Crédit Mutuel plans to have 100,000 cards in the field in 2000 and to extend their scheme to two additional cities as a prelude to a national rollout in 2001.

  Main characteristics : Mondex based e-purse allows direct card-to-card payment operations. Multi-application support (MULTOS): banking, e-purse, loyalty, etc. Multi-currency support: Mondex e-purse technology supports up to 5 currencies.

United Kingdom

There are two e-purse technologies currently being used or experimented with in the UK:

- **VISA Cash** have a pilot scheme in the city of Leeds, which has the backing of six major banks including, The Abbey National, Barclays Bank, Co-operative Bank, The Halifax, Lloyds/TSB and The Royal Bank of Scotland. The VISA Cash e-purse being trialed is both reloadable and disposable, with three banks issuing stand-alone cards and three banks adding VISA Cash to existing debit products.

  Main characteristics: The technology uses RSA algorithms and is one of the few VISA Cash schemes that uses public key technology (other in Japan). Public key infrastructure is key for the future of interoperability.

- **Mondex** started a pilot scheme in the town of Swindon 1995. This scheme was developed in conjunction with the National Westminster Bank. More than 500 merchants originally signed-up for the scheme, which also involved the Midland Bank and British Telecom. Additional participants included 'closed' user groups at six UK universities.

  Main characteristics: The technology was not MULTOS based, nor did it conform to any existing or draft CEN standards. The actual security protocols used in the system were based on the classic challenge/response techniques.

  A decision was made in 1998 to wind down the Swindon trial. However, the university user groups are still in existence, where some 100,000 cards are in circulation. MasterCard's 51% ownership of Mondex may have an influence over the future of Mondex in the UK.

Ireland (Eire)

One twelve-month pilot is currently underway in Ireland and a second is due to start shortly in the same location.

- **VISA Cash** has a pilot running in the town of Ennis. This 12-month trial has the support of the Allied Irish Bank and the Bank of Ireland. Some 5,000 cards were in circulation by mid 1999. VISA Cash can be used in Ennis to pay for low value purchases - everyday items as well as in parking meters, vending machines and eircom (the main Irish telephone company) cardphones in Ennis.

  Main characteristics:

- In a world first, WAP (Wireless Application Protocol - which enables mobile phone users to browse Internet information) and smartcard technology are to be trialed for an e-commerce application also in Ennis as part of eircom's Ennis Information Age Town. Cardholders will be able to load value to their cards using their Eircell WAP mobile phone. Some 100 units

Spain

Commuters in Spain soon will be using a new contactless TIBC VISA Cash feature on a VISA Electron magnetic-stripe debit card in the transit systems in Madrid and Barcelona. A consortium of transport operators and Spanish banks will launch a pilot later this year using the multi-application card developed by SERMEPA in the two major Spanish cities.

The Sirocco pilot in the Barcelona area will trial a multi-application card combining an e-purse, a transport ticketing application for commuter trains and busses and a parking area access control application on a single-chip contact/contactless smartcard. 10,000 cards had been issued by the end of 1999.

Norway

In September 1999, Norway announced a pilot for Pay-TV that will commence during 2000. Their e-purse is based on Proton technology. Initially only the Proton e-purse application will be loaded, however other applications may be added in the future. The scheme which will be run jointly between Proton World and BBS (Bankenes BetalingsSentral AS) who represent all Norwegian banks.

In the pilot, smart cards will be issued by the banks to their customers, who will load value into the e-purses from their bank accounts, which can then be used to pay for pay-per-view television programmes via existing set-top boxes.

The Norwegian project will be the second national Proton scheme in Scandinavia (following the CASH scheme, established in Sweden in 1996) and the fifth in Europe (after Proton in Belgium, Chipknip in the Netherlands and CASH in Switzerland and CASH in Sweden).

3. E-purse business

The e-purse is still in its infancy. Many countries have not yet introduced e-purse schemes or have set-up only geographically limited trials. In countries where e-purses have been commercially deployed, they have not yet reached a significant share of the payment transactions. It is worth remembering that this was also the situation many years ago when credit cards were first introduced, the success of which nobody would dispute today.

The various operators are still searching for the winning combination of e-purse technologies, the various features supported by the e-purse, the commercial conditions for e-purse use and the required partnership agreements. The evaluation of these issues is still the focus of trials, such as those in France where three competing e-purse schemes with quite different characteristics were announced in 1999. The aim is obviously not to end up with three (non interoperable) e-purses in France, but to test and validate the different systems and to assess consumer and card acceptor reactions.

A study carried out on the Proton e-purse by Free University of Brussels professor Leo Van, concludes:

> If anything, our analysis shows that e-purses will need some time to reach cruising speed. An important reason is that e-purses are subject to so-called 'network externalities' - that is, the utility of an e-purse increases with the size of its network. The nice thing for issuers is that this implies that the success of an e-purse can become self-reinforcing - the more people that use the card, the more merchants will accept it and the more interesting it becomes for as yet unconvinced consumers to start using it, and so on. However, the drawback of this interdependency of demand is that issuers are initially faced with a 'chicken-and-egg' problem. Merchants will be reluctant to invest in the systems needed to accept the cards unless sufficient consumers show their interest, while consumers, on the other hand, will not use the card as long as they can only pay with it in a few places. In short, to get the snowball rolling, issuers first must succeed in convincing a critical mass of consumers and merchants.
>
> According to Wim Philippe, product manager at KBC, Proton tries to overcome this deadlock by means of both a push and pull strategy; that is, by promoting the card simultaneously with consumers and merchants, and this region by region. Philippe is convinced - and, in my opinion, rightly so - that "the engine of the success for Proton will be the usage of Proton in closed user groups (companies, schools, ...) and at vending machines, parking meters, pay phones and so on. These applications will be the 'killer applications', because their added value is very obvious from the consumers' viewpoint". […] In view of the chicken-and-egg problem a slow start was to be expected. Moreover, experience shows that changing people's payment habits takes time.

The potential of the e-purse for electronic payment on-line (on the Internet and on mobile networks, like in the e-purse trial in Ireland) and in the real world is huge. The general use of e-purses should be considered for the longer term. According to Gérard Compain, CEO of INGENICO, the world's second largest card terminal vendor, the e-purse will not become the usual payment instrument for another twenty years. He is probably right.

Commercial performance

The economics of the e-purse are fairly simple in that setting up a scheme requires extensive infrastructure investment, which means high fixed costs. Thus the key to profitability is an intensive use of the system and a high transaction volume per card. E-purse systems have additional constraints. The infrastructure needs to be highly sophisticated (reloading, value transfer, transaction recording) and is therefore costly as unit transaction amounts are small. Furthermore, for a cash replacement oriented e-purse, critical mass is not enough, the infrastructure has to be ubiquitous, in order to be as attractive as cash. And ubiquity is more expensive and difficult to achieve than critical mass. Consequently, more than for a debit card system, an e-purse scheme requires a high transaction volume.

According to calculations made by specialised consulting company, Edgar Dunn and Co, breakeven will not be achieved in less than five years for a scheme with the following parameters:

- medium-size scheme based on a non-accountable system design (Mondex-like)
- 400,000 cards in use (representing a total of around 1,500,000 cards in circulation)
- card unit cost of $5
- cardholder pays an annual fee of $7.50
- load fee of $0.3
- average merchant commission of 0.55%
- average of 250 transaction each year

In the case of an accountable system, the breakeven period is even longer at an estimated seven years.

Cash replacement

For most analysts, stored value cards are synonymous with e-purse systems for small amount transactions - below 25 Euros, to take an arbitrary cut-off point. Traditional credit and debit systems do not handle such transactions cost-effectively, because they are considered uneconomic both for banks (issuing and acquiring) and for merchants. Similarly, banks and merchants are very reluctant to accept cheques as payment for these low-value transactions - which leaves only cash as the payment method.

The principal objective of the e-purse system is therefore cash replacement. E-purses are seen as a vector for converting physical cash into electronic one. The following quote is taken from a paper entitled 'Electronic Cash and the Innovation Process: A User Paradigm' presented at the European Commission's ACTS Fair -

> 'Electronic cash is yet another stage in the evolution of ‘invisible’ money, which has its origins in the debasement of coinage, where the actual value of the metal in the coin no longer represented its face value. This new stage seems a logical continuation of the process that has been going on for as long as human memory stretches, i.e., the development of money from coinage to paper currency to electronic instruments.'

The market potential is enormous. A survey conducted by VISA during 1997 in twenty-nine countries that between them account for 80 % of the world's economic output, showed that cash transactions represent an annual value of 8.1 trillion Euros - of which 22% was for transactions with a value of 10 Euros or less. More significantly, the volume of cash transactions dwarfs that of cheque, card or electronic transfer transactions. In France cash payments represent 70% of the total financial transaction volume, and payments of less than 10 francs (1.5 Euro) represent 35% of the total. In the UK cash accounts for 75% of all transactions.

From the financial institutions perspective, the principal reason for cash replacement is cost reduction. Cash handling costs are estimated by various sources at between 5% and 7% of its face value - considerably higher than for other payment systems. IBM has estimated that cash handling costs banks world-wide around $30 billion each year. According to the Boston Consulting Group, the overall cost to UK banks, retailers and customers of handling cash is £4.5 billion per year. In addition, banks also have to pay a commission or 'royalty fee' to the central banks that issues the cash. In Belgium, such commission revenues represented over 1 billion Euros in 1993. According to BIS (Bank for International Settlements) estimates, if electronic cash were to replace all the banknotes of value smaller than an equivalent of 25 Euros, then the total revenue loss for its eleven Central Bank members would be close to 17

The e-purse, or stored value card, can also be seen as the last step in a payment acceleration and float capture process that led banks from a 'pay later' credit card approach through the 'pay now' debit card approach to a 'pay before' prepaid card concept.

The enormous business potential of e-cash is seen as both an opportunity and a threat for the financial sector. According to a European Commission brochure -

> 'In the financial industry, several banks are leading the development of electronic cash solutions in co-operation with ICT [information and communication technology] suppliers. These initiatives are structured to preserve the banks' traditional central role in clearing and settlement functions, to tie e-cash into other banking services, and to respond to the competition from emerging players such as telecommunication companies, transport authorities and large retailers.'

In addition to banks, the e-purse also offers benefits to the merchant/retailer and to the customer/cardholder. The following table summarises the benefits and the constraints of small-payment e-purses for card issuers (e.g. Visa); card acceptors (merchants) and card holders (customers).

	Benefit	**Constraint**
E-purse issuer	Reduce cash handling costs. Opportunity for revenue generation - float, transaction fees, card issuing fees, renting card terminals, etc. Reduced fraud. Foster customer relations. Good media for marketing.	High investments, complex technical infrastructure. Management of complex business environment. Lack of mature standards.
Acceptors	Reduced cash handling cost - less manual operations for handling cash (particular advantageous for vending machines). Reduce theft and vandalism (vending machines). Reduce leakage and errors in counting. Faster payment operations. No problems with providing change. Simplify sales operations to foreign customers - assuming that the e-purses are interoperable. Increased security - no or less physical cash to handle in the shop or the vending machine. Maintains consumer confidence in the context of the Euro introduction Potential to get more information on payments available in electronic form providing data on micro payment transaction patterns. Enables remote payments. Provides consumer confidence for on-line payments by allowing remote payment without the need to transmit confidential data, such as credit card	Investment in POS terminals. Cost of transaction fees. Are dependent on e-purse issuers who tend to unilaterally define the business conditions. Market standards not yet established.

	buy on the Internet because they are not confident. For example, the French bank BNP receives an average of 700 complaints per week from C/D cardholders concerning fraudulent use of their card).	
Card holder (consumer):	Ease of use - provided it is accepted at a large number and variety of acceptance points. No problem with providing change. No problem with Euro conversion and more confidence in Euro payments (especially for elderly people). Less time spent at the sales-point for the payment operation. Security - less cash carried Suitable e-payment instrument for the young (10 years and above). Can potentially reduce the number of cards required for specific micro-payments (parking, public phone, etc.) More sophisticated card has the potential to reduce the number of card carried by the cardholder, by integrating several applications (C/D, transport, loyalty, social security card, etc.)	Does not efficiently replace all types of transactions· Risk of becoming hostage to card issuers charging for use of e-purse, whilst real cash is virtually free (how to control introduction of new fees, once e-purse largely deployed).

E-purses are network goods

Economists call 'network goods' products and services, whose value is linked to the number of users. Thus network goods have no value in isolation. They derive their value from their connection with other goods. A telephone or a fax is useless unless it allows communication with other telephones and faxes. The wider the connectivity, the higher the value of each product and, more importantly, of the network (physical or virtual) that connects them. Capturing the network value, directly or indirectly, is the strategic objective for goods' suppliers and distributors.

Network goods should be considered from both the supply and the demand perspective. Those who offer network goods face discontinuities and threshold effects. They need to create a critical mass of products and network connections before they can attract customers. Thus network goods have high start up and fixed costs. However, once the critical mass is reached, marginal costs of producing additional goods and/or attracting new customers are low and often decreasing.

For the user, the utility of a network good is determined on the one hand by the number of users and on the other hand by the ease of access. For some networks, critical mass and large size are not sufficient, they have to attain ubiquity at a reasonably low cost. The demand for a network good is discontinuous and marked by the classic 'chicken-and-egg' dilemma. A user is reluctant to join a network with very few users, which keeps the network size small (and access cost high) and therefore discourages others from joining. Thus the demand curve is non-linear, low growth in the initial stage, followed either by a steep decline if a critical mass of users is not reached, or a rapid growth if the critical mass is attained.

Under the conditions of coexistence, the e-purse appears as an addition to cash not as its considered as a success in France if it can reach a share of 20% of the total cash transaction volume in the long term. It should be emphasised that an e-purse is not expected to cover the full range of payments, due to usual limitations in the balance size and the transaction amounts. There may be areas where the e-purse may act as a substitute for other payment instruments, debit cards for example, but this depends very much on the commercial agreements that would apply for the different payment instruments. The situation may also be different from country to country. One should also not lose sight of the fact that commercial agreements concern card acceptors and cardholders as well.

Financial characteristics of e-purse schemes

The financial characteristics of the e-purses are quite different from one scheme to another. Although the e-purses all target payment of small transactions, the total amount held on a card, the maximum amount that can be loaded in one operation, etc. varies considerably. This is also true for the commercial conditions related to e-purse use, such as the fees to be paid by the card acceptor, which could be a percentage on turnover, a fixed fee per transaction or a combination of both, as well as the fees to be paid by the cardholder (card issuing fee, fee per payment transaction, fee per load transaction, etc.). Commercial conditions are traditionally set by the e-purse issuing organisations.

The following table summarises the financial characteristics of some of the e-purse schemes currently operating in Europe.

Scheme	Initiator(s)	Operator(s)	Max card value	Cardholder fees	Retailer fees	Settlement
Avant Finland	Merita Bank, Postibanki & Okobank	Automatia Rahakortit Oy	2,000 FMk (336 Euros)	Unknown	Unknown	Bank accounts
Cash Switzerland	Prosys, Banksys	Europay (CH), Payserv AG	300 SFr	Fee for Eurocheque card	0.7% commission plus 0.02 SFr transaction fee	Central processing through TK Payserv AG
Chipknip Netherlands	Interpay NL	Dutch banks	500 Gld (227 Euros)	Determined by banks	0.80%	Interpay NL
Chipper Netherlands	KNP Research	Chipper NL, Postbank ING Group (PTT) Telekom and KNP	500 Gld (227 Euros)	None	15 Gld per month; 0.08 gld per transaction or 0.7% of amount	From terminal over phone-line to Chipper NL
Danmønt Denmark	Danmønt	Danmønt (PBS)	1,200 DKr	None	0.18 DKr per transaction; 1,250 DKr annual fee for SAM	Off-line cleared by 'concentration point' every 14 days
Euro 6000 Spain	CECA	Saving banks	30,000 Pts (180 Euros)	Unknown	Unknown	By CECA over phone line or collection card
miniCash Luxembourg	CETREL	A group of 9 banks and credit institutions ?	5,000 LuF (124 Euros)	Free, 10 LuF for loading from non-bank terminals	0.7% per transaction with de 0,4 LuF minimum fee;	CETREL
GeldKarte Germany	ZKA	Various banks and saving banks	400 DM (205 Euros)	Depending on banks; 2 DM for loading at other institutions	0.3% of turnover, 0.02 DM min per transaction	Via purse evidence centres for retailers and cards
Minipay VISA Cash Italy	SSB	SSB	300,000 Lir (155 Euros)	10,000 Lir	0.5%	Through the banking system
Mondex UK	National Westminster Bank	Mondex Intl. Ltd., AT&T Universal Card services, numerous franchisees and licensee banks	Set by each originator Swindon: £ 500	Currently none, may be set by member banks depending on market	Same as Cardholder fees	Direct transfer
Monedero 4B Spain	S4B	Issuing banks	25,000 Pts (150 Euros)	Unknown	Unknown	By S4B over phone line or deposit card
PMB Portugal	SIBS	SIBS	40,000 Esc (200 Euros)	Up to 750 Esc	<1%	By SIBS, daily
Proton Belgium	Banksys	Banksys	5,000 BF (124 Euros)	Depends on issuer bank, 200 BF average	0.45% of retailer profit	Via Banksys
Quick Austria	Austria Card, Dr Piller, CZS, EPA /APSS	Austria Card, EPA /APSS	1,999 ASch (145 Euros)	None	0.5 to 1.7%	Unknown
TIBC VISA Cash Spain	SEMP	SEMP	25,000 Pts (150 Euros)	None	None	By SEMP

Table 2 : Overview on European e-purse schemes financial aspects

E-purse interoperability

One of the key lessons of the e-purse experience in Europe is the need for interoperability.

The need for interoperability was not clearly perceived initially as the e-purse was seen as a fundamentally local product. According to Banksys, 99% of e-purse transactions occur within 50 miles of the cardholder's residence. Furthermore, the costs of interoperability were seen as high, making the e-purse business case more difficult. Several factors have contributed to a change in this thinking.

One is the advent of the Euro. A customer may understand that they cannot use their DM-based e-purse in Italy, but may be puzzled as to why they can use their Euro purse in Belgium but not in Holland, which also uses Proton technology.   E-purse scheme promoters also became more aware of the hidden but real costs of non-interoperability - confusion and uncertainty among technology suppliers, merchants and customers has a stunting impact on market growth and concept acceptance. However the move towards interoperable e-purses systems in Europe can be considered more political (due to the Euro) than economics based.

It is pointless to argue whether e-purse systems should or should not attempt to enter the payment systems market in direct competition to existing conventional payment systems products. But if e-purse systems are ever to occupy more than a marginal role in the payments market place, then they will need to include interoperability as a feature. Customers using credit and debit cards today expect interoperability (including cross-border interoperability) to be a basic feature of their card, and much investment has been put in place to ensure that this is so. Without interoperability, it is difficult to envisage the e-purse as a serious mainstream competitor. And if the e-purse is not to become a mainstream payments product, then it is most unlikely that e-purse systems will be able to attract a significant investment required.

4. Essentials for e-purse interoperability

Almost all existing e-purse systems are not interoperable, either technologically or commercially. Although all these systems focus on small amount transactions, they are extremely diverse in their basic philosophy, design principles and technical choices.

With the introduction of the Euro, the case for interoperability is stronger than ever and no one scheme can enforce it alone. It is clear, that common standards will lead to more efficient, faster, more cost effective services for payment schemes, banks, merchants and cardholders alike. Such standards can only be achieved by a common and concerted approach. However, more sophisticated operating systems and application environments are necessary to support interoperability than currently exist.

In the financial services area, the EMV standards were developed by three leading payment networks - Europay, MasterCard and VISA. EMV'96 ICC Specifications for Payment Systems are world-wide and cover cards, terminal and applications. The introduction of EMV standards is clearly a positive contribution to interoperability and has demonstrated that payment schemes, banks and many retailers can reach consensus for the ultimate benefit of the payment business as well as providing cardholders with more security, usability and associated benefits.

In 1998 three events triggered the process for e-purse interoperability - commercial agreements between SERMEPA, ZKA and VISA International; VISA's alliance with Proton World International; and Europay's announcement that it would support the Common Electronic Purse Specification, CEPS. These alliances and commitments effectively account for up to 90% of European e-purses and will aim for the ultimate goal of interoperability. Europay's international new e-purse based on the CEP specification will be branded CLIP.

Global interoperability requires more than independent sets of commercial bilateral agreements. It requires majority commitment to a single concept. Such commitment is really only possible initially within a regionally agreed (Europe here being the region) set of basic e-purse payments services with a basic operating model. The standard determined by the CEPSCo Espagñola, EuroKartensysteme/ZKA, Europay International and VISA International will guarantee this interoperability for both the card and the terminal.

ECBS' three levels of interoperability

True interoperability must cover both technical and commercial aspects. The European Committee for Banking Standards, ECBS, in its Technical Report on the topic, defines three levels of interoperability :

- **Level 1** (Lowest level). The multi-application terminal must be built to host firewall protected applications, each of them separately downloaded, and it must manage its files and host connection. This requires a common application selection routine in order to perform the reset of the card and the initialisation of the card introduced into the terminal, as well as the selection of the appropriate application software. From the point of view of the acquirer, each application is seen as a specific terminal.
  This architecture prevents the retailer from installing several different devices in one terminal as is done today in certain countries (such as Spain) in order to save space. Nevertheless, terminals have to be complex enough with a multi-tasking Operating System, large memory size, etc.

- **Level 2** (Intermediate level). The basic functions performed by the applications are standardised and the architecture is the same as above. In addition to the hardware and peripherals, most of the application software is shared. This is achieved today with EMV for Debit/Credit and is expected with CEPS for e-purse. Management of migration from one each application provider will continue to manage the download of new software versions independently, keeping the freedom to include specific messages or loyalty functionality within the transaction.

- **Level 3** (Highest level). The application software is unique and is capable of processing various card schemes. Transaction data and files may remain separate, as is currently the case with VISA & MasterCard magnetic stripe credit card based transactions. The transaction processor is in charge of software functionality maintenance.

Interoperability at the terminal

Multi-application terminals cater for the interoperability of multiple schemes within one country or within different regions. For cross-border transactions, agreement must exist for the purse holder's own currency to be accepted at the terminal. This solution is based on a physical extension of the domestic scheme and puts the task of compatibility on the side of the acquirer. No modification of the card or the e-purse application at the terminal level is required. The necessary software and additional SAMs (if needed) enable the reconstruction for each accepted e-purse scheme based on the conditions of the domestic scheme. These include domestic keys, domestic security protocols and the associated collecting and clearing procedures.

With respect to the load function, it is assumed that only the issuer of the e-purse has the ability to reload the purse because they are the sole possessors of the load keys.

The following table highlights the advantages and disadvantages of these multischeme terminals:

ADVANTAGES	**DISADVANTAGES**
Identical use of the e-purse whether domestic or abroad with respect to both load and purchase transactions.	Modification of the payment terminals.
No need for extensive modification of the issuer's functions.	The terminal will have to be able to recognise the new e-purses with respect to load transactions.
Merchants will be paid in their own currency. The amount will equal the amount charged to the foreign customer. The currency exchange risk is born by the acquirer.	The cardholder is exposed to the conversion rate supplied by the acquirer. A need for a guarantee to ensure the fairness of the conversion rate in the terminal.
The specific e-purse management and security is handled during the on-line transaction with the e-purse issuer. It will be necessary, however, to provide a common processing service for all e-purses which are supported in the terminal.	

The following schematic represents the software architecture for a multischeme terminal

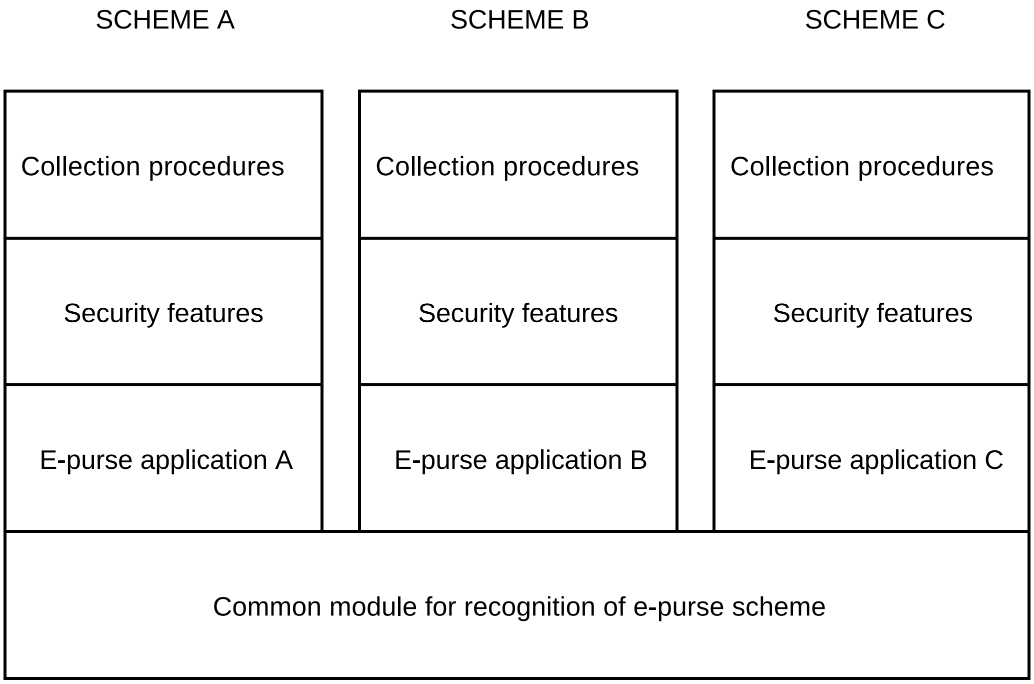


Figure 6*: Software architecture in a multi-scheme terminal.*
(The acceptor scheme is scheme A)

As a function of technical compatibility, the application and collection layer can be shared by different purse schemes.

1. The requirements with regard to the load transaction at the (scheme A) terminal are:
   - The terminal is able to recognise a non-native (scheme C) purse,
   - The terminal is able to perform an on-line connection to the (scheme C) issuer.
   - During the on-line phase of the loading process, the loading device is transparent.
2. The requirements with regard to the purchase transaction at the (scheme A) terminal are:
   - The terminal recognises the e-purse as being a non-native (scheme C) purse,
   - The purchase transaction is effected using the security mechanisms and the software appropriate to the non-native scheme (C),
   - The electronic value is transmitted to the issuer of the non-native scheme (C) through an acquirer of the native scheme (A)
3. The requirements with regard to the conversion in terminal of scheme A are:
   - The merchant types the purchase amount in the local currency,
   - The conversion takes place within the terminal using a conversion table to translate the amount into the purse holder’s own currency, which is displayed to the purse holder,
   - After agreement to the purchase transaction, the e-purse is debited with the amount denominated in the purse holder’s currency using the issuer’s security protocols and keys,
   - The terminal has several slots, which store the electronic value. Establishing a shadow value account in the local currency is an option that needs to be considered.
   - For multislot e-purses that have been loaded with the appropriate currency, there is no need for the conversion process in the terminal at the time of the purchase transaction.

- It is assumed that the necessary business agreements have been established concerning the exchange rate, the collection of the value, the update of the conversion table, the SAMs (if needed) and the security protocols.
- The possibility exists for the issuer to block certain acquirers/countries and for the acquirer to block certain issuers/countries.

Interoperability in the card

There are certain modifications to the card that are necessary for interoperable e-purse schemes. The main challenge is to achieve the same level of application interoperability for e-purses, whose main characteristic is not access to accounts but the ability to hold cryptographically protected value in a uniquely defined currency. Several implementation issues have been identified.

At the operational level, three possible implementation systems can be envisaged:

- The traditional correspondent banking based system.
- The possibility of the interconnection of ACHs (Automated Clearing Houses) in the near future.
- The facilities offered by European and international card schemes.

At the technical level the capacity of the transmission network and the host computers will have to be increased. This is because the additional volumes will have a significant impact especially for fully accounted systems. Truncation and aggregation of unitary transactions should partly solve this problem.

The multischeme card model differs from a multislot purse in the way that the non-domestic purses are implemented as independent and completely separate applications, whereas a multislot purse can contain different currencies within the same application. Authorised e-purse issuers who are different from the domestic purse issuer could create these other e-purses.

This solution is possible only if technical and commercial agreements exist between the card issuer and each of the non-domestic purse issuers. It does not affect the terminals (loading and purchasing devices) nor the exchange and security protocols since the 'new' e-purses are considered as domestic by each of the non-domestic schemes.

The following table highlights the advantages and disadvantages of these multischeme cards:

ADVANTAGES	DISADVANTAGES
No adaptation of the terminal is necessary.	More memory is needed in the card.
The principal or domestic issuer does not have to intervene either in the loading or clearing processes of the other purses	The harmonisation of the specifications (minimum set of commands and data-elements) between the different purse schemes will not be easy to achieve. A strong need for technical agreements
The multi-currency solution is provided because the secondary purse providers may operate in different currencies.	The cardholder is responsible for managing the creation and the erasing of the different purse schemes on his card.

The following schematic represents the logical architecture in a multischeme card.

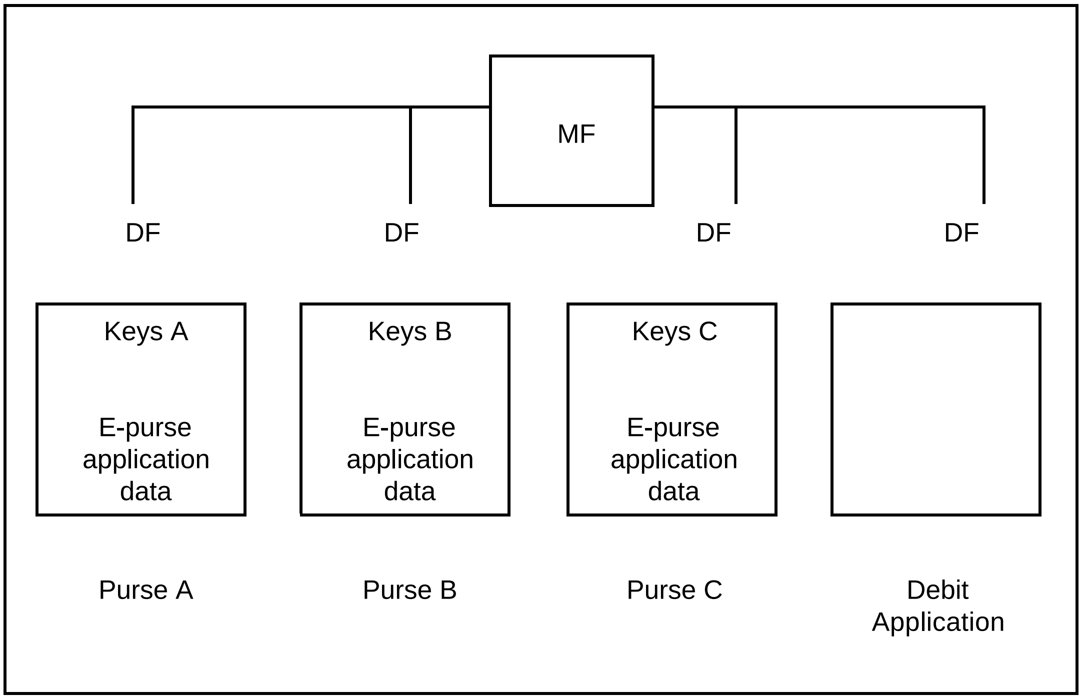


Figure 7: Logical architecture in a multischeme in card.

Note: MF = Master file
DF = Dedicated file

It is assumed that the terminal accepts only one e-purse scheme.

1. Requirements with regard to the load transaction:
   - Loading of the native purse: basic service provided by the card issuer,
   - Loading of the exogenous purse: load is on-line to the issuer of that purse application under his specific security protocol.
2. Requirements with regard to the purchase transaction:
   - Since the card is presented to a terminal accepting only one of the purse applications residing in the memory, the terminal software will have to be able to recognise and select the appropriate e-purse for the purchase transaction.
   - If more than one purse application is common to the card and the terminal, the selection is under the control of the issuer.

The interoperability of payments is shown in the following schematic:

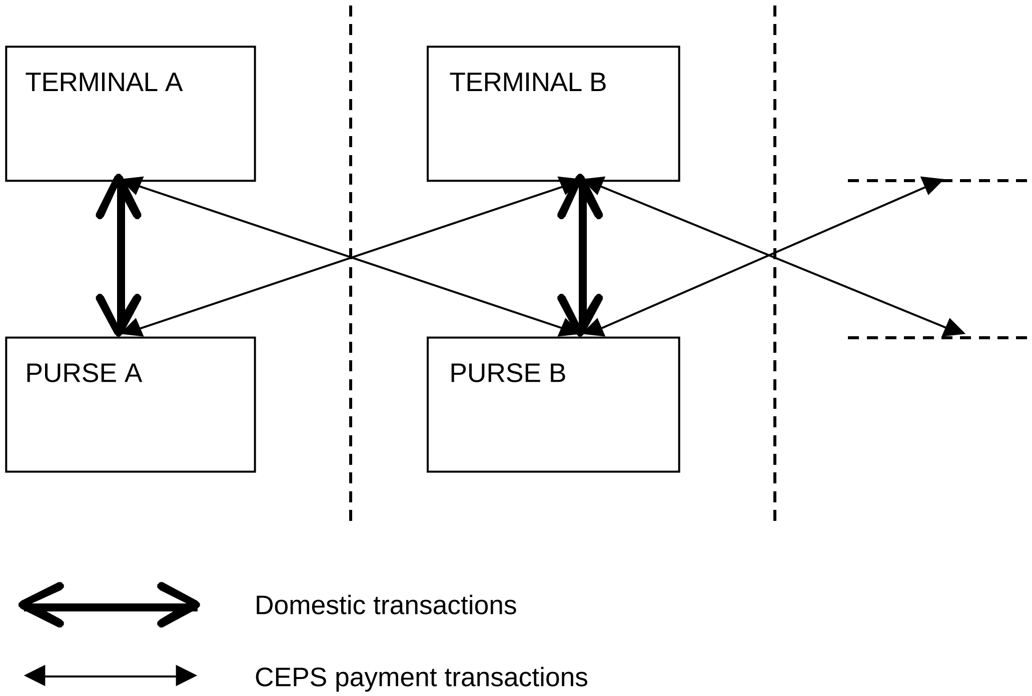


Figure 8: Payment interoperability scheme

Any terminal A must accept its domestic e-purse A and also any e-purse B used for payment. Any terminal B must accept its domestic e-purse B and also any e-purse A used for payment.

Initiatives for e-purse interoperability

Thanks to the requirements of the public network sectors and the consequences of the introduction of the Euro, card programmes are now feeling the pressure to become interoperable as quickly as possible. The rapid growth in e-commerce over public networks requires a product that can handle small payments on an internationally interoperable basis. Cardholders - purchasers - expect a convenient and consistent service when using their e-purse either domestically or internationally.

The original plan to develop interoperable solutions under the EMV banner collapsed in 1998 due to a dispute between VISA and MasterCard scope and product features. In June 1998, ECBS released a technical committee draft for a pan-European stored value standard, covering the interface between the card and the terminal, terminal requirements, key management, card and terminal certification, and clearing/settlement.

Based on the EMV draft and taking into account the preliminary specification produced by the Commission for European Normalisation (CEN) - prEN1546, EuroKartensysteme/ZKA, CEPSCo Española, Europay International and VISA International have worked together on developing a global standard for e-purses, known as the Common Electronic Purse Specifications (CEPS). These four organisations have established the CEPS Consortium (CEPSCo) that is responsible for the maintenance of the specifications, the type approval process and interaction with the industry. The draft specifications were published for the first time in March 1999 and the final version was published in September 1999.

The main features of CEPS are:

Load transaction:

- linked load (loading by debiting a bank account);
- unlinked load (loading by a separate credit card debit transaction);
- cash load (loading at a terminal in exchange for cash);
- internet load & home-banking load (via telephone, mobile phone, PC);
- foreign load (at a load terminal of another e-purse scheme).

Multi-currency support:

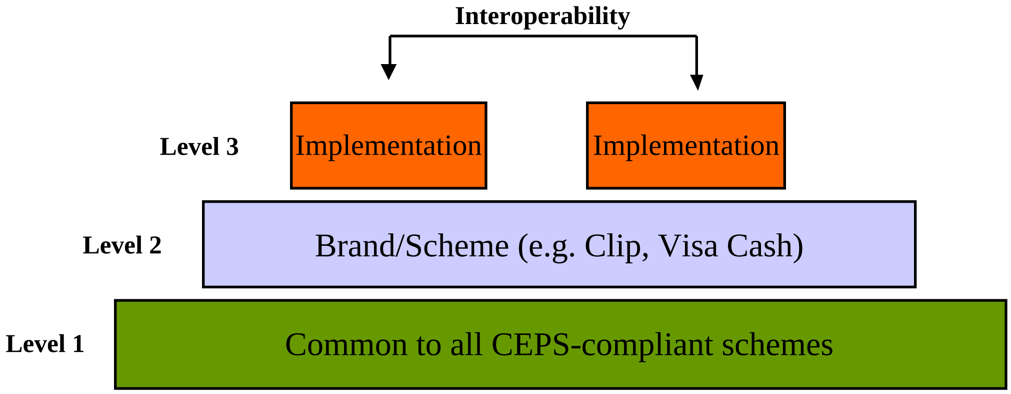
- allowing one or more e-purses to reside on the same card;
- changing of an e-purse's currency;
- converting foreign currency loaded into the domestic currency.

Purchase transactions:

- attended (POS) purchases;
- unattended purchases (e.g. vending machines, parking meters);
- incremental purchases (e.g. at a payphone, photocopier);
- cancel last purchase (e.g. when a vending machine fails to deliver the goods requested).

Security:

- CEPS demands high levels of security, and assurance that all systems are fully auditable and traceable. Consequently card-to-card transactions are not permitted.
- Purchase transactions are off-line and require mutual authentication between card and terminal, using active RSA public key cryptography.
- Load transactions are on-line and are protected by symmetric cryptography and a PIN.


Interoperability
Level 3
Implementation
Implementation
Level 2
Brand/Scheme (e.g. Clip, Visa Cash)
Level 1
Common to all CEPS-compliant schemes

Currently, organisations from twenty-two countries, representing more than 130 million - over 90% - of the world's e-purse cards, have already agreed to implement CEPS, thereby creating a global e-purse standard. In addition, over 150 organisations have signed license agreements for CEPS and have received the specifications.

VISA has positioned itself to accelerate the push for an international stored-value specification by becoming a shareholder in Proton World International, a spin-off of Belgium based Banksys SA and developer of the Proton smartcard technology. In line with its strategy to be at the forefront of technological evolution in the smartcard industry, as soon as the official release of CEPS was announced in March 1999, Proton World declared its intention to support, and implement CEPS in the Proton technology and to be the first to offer CEPS-based solutions to the market.

Proton World, having retooled its technology to comply with CEPS, demonstrated its first CEPS card at the Cartes 99 symposium held in Paris during November 1999. This CEPS purse is scheduled to hit the market in 2001, enabling banks to issue new cards and upgrade terminals prior to the launch of the Euro as a cash-currency in 2002.

The CEP Specifications

The objective of the CEP Specifications is to define and evaluate the business, functional and technical issues related to an open, common and interoperable e-purse environment. New as well as core features of current e-purse products are covered by the definitions, adding a multi-currency capability that offers a consistent service to cardholders and merchants throughout the world regardless of the underlying technology platform or scheme.

The specifications include requirements for all components needed to implement a globally interoperable electronic programme, while maintaining full accountability and auditability. They also outline overall system security, certification and migration.

CEPS does not dictate a card Operating System, only an interoperable application - the computer program and associated data that resides on the integrated circuit chip and satisfies a business function - which must be distinguished by one unique application identifier by brand.

The interoperability levels to be achieved with CEPS are:

- E-purses that utilise technology independent, end-to-end transaction processing.
- Devices that allow e-purse cardholders, merchants and financial institutions, regardless of the underlying technology, to perform e-purse transactions.
- Systems that clear and settle transactions performed by cardholders and merchants, regardless of the card issuer, acquirer and/or scheme provider.
- Applications, devices and systems which meet e-purse issuers expectations of quality, convenience and service for their cardholders.

In order to ensure interoperability, a certification scheme is mandatory. The e-purse must be capable of existing within a multi-application environment and be compatible with other certified applications.

EMV and CEPS interoperability

CEPS define the requirements needed by an organisation to implement a globally interoperable e-purse programme. It requires compatibility with the EMV Specifications for chip cards and defines the card application, the card-to-terminal interface, the terminal application for point-of-sale and load transactions, data elements, and recommended message formats for transaction processing. It also provides functional requirements for the various e-purse scheme participants and uses public key cryptography for enhanced security.

EMV '96 supports applications that enable issuers, merchants and consumers to start using chip cards and terminals - with added security. Divided into three books, the EMV specifications include:

- **Card Specifications:** a common basis regardless of the application. It addresses electromechanical commands, file and data structures, selecting applications and security. Plus secure messaging, post-issuance commands and Dynamic Data Authentication using the RSA algorithm.
- **Terminal Specifications**: a common basis regardless of the application. Provides details for a variety of different terminals.

- **Application Specifications:** traditional payment transactions with the ability to add (if jointly agreed) additional applications, such as loyalty programmes, etc.

CEPS features

CEPS require compatibility with the EMV specifications for chip cards and uses public key cryptography for enhanced security. CEPS defines the card application, the card-to-terminal interface, the terminal application for point-of-sale and load transactions, data elements and recommended message formats for transaction processing. Without being exhaustive, these are their main features:

- The e-purse application can be or not be linked to a specific funding account.
- The following transactions are defined:
  - Load;
  - Unload;
  - Currency exchange;
  - Purchase and purchase reversal;
  - Incremental purchase;
  - Cancel last purchase.
- No currency conversion occurs at the Point of Sale.
- Multiple currencies can by deployed in different slots.
- The system must be able to trace all transactions (that change the balance of the e-purse).
- Electronic value can be transferred from:
  - cardholder to merchant (PSAM);
  - merchant (PSAM) to cardholder only for cancel last purchase or purchase reversal;
  - card issuer to cardholder (load);
  - cardholder to issuer (unload);
  - one application to another non-financial application on the same chip card;
  - one application to another financial application.
- Electronic value cannot be transferred from one e-purse to another.
- Asymmetric cryptography is used for off-line transactions. For this kind of transaction, a mutual authentication mechanism must be followed.
- Symmetric cryptography is used for on-line transactions and for protecting the integrity of data, by MAC (message authentication code) generation.
- The on-line PIN verification capability must be implemented in the card as well as on the off-line PIN verification mode. Plain text or ciphered should be defined by the issuer.
- The card can be locked and unlocked by the cardholder in off-line.

Reference model for interoperability

The following schematic describes interoperability aspects based on CEPS.

E-purse **A** represents any domestic e-purse. The schematic shows that if the CEPS card is used with a domestic terminal, data flow will be directly connected with the e-purse **A**. If the terminal is not domestic, the data flow will go through a CEPS layer to allow interoperability.

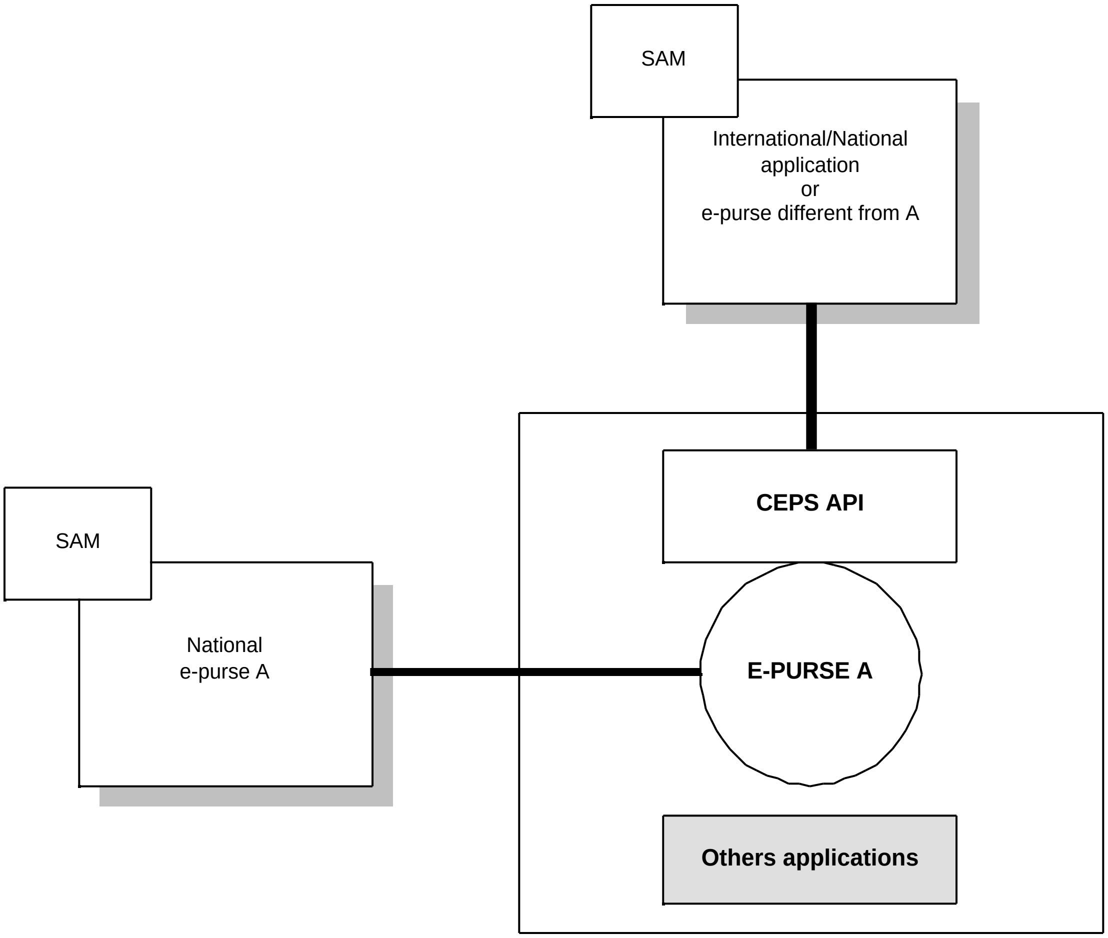

SAM
International/National application or e-purse different from A
CEPS API
SAM
National e-purse A
E-PURSE A
Others applications

Figure 9 : Interoperability in a CEPS scheme

Security aspects

Cryptography is used to ensure safe and secure transmission of sensitive data between one location and another. With cryptography, a message can be encrypted using a key, and the resulting cipher-text is transmitted to another party where a decryption key is used to unscramble the message to its original form.

Two forms of cryptographic technologies have been introduced and used in today's smartcard technology:

- Secret key cryptography;
- Public key cryptography.

Secret key cryptography

Secret key cryptography is also known as symmetric cryptography. The same key is used to encrypt and decrypt the message. The sender and the receiver must share a secret (i.e. the secret session key). The most well known and used algorithm is DES (Data Encryption Standard). Today, in order to enhance security, triple DES (3-DES) is used. Triple DES is based on simple transformation executed several times to make it more robust against attacks than simple DES. The key length is 16 bytes. Messages are subdivided in 64 bit blocks.

3-DES is mostly used to compute MACs (Message Authentication Code). Usually session keys are never exchanged. But if RSA is implemented on the card, a technique called 'wrapping' can be used to transmit in a secure way over the line the encrypted session key.

For security purposes keys are distributed through the key management system, which generates, stores, distributes and destroys keys. Secure modules which share a common key often use that key to send a session key to the other party at the beginning of the transmission. The receiver then decrypts this key and uses it in all further communication in that session. At the end of the session this key is destroyed and a new one will be generated at the beginning of the next session. In order to transfer session keys, both sides need to know a common (or master) key. This is distributed from the key manager using a special distribution key (in the case of DES). This form of technology is used by financial institutions for PIN encryption purposes.

Public key cryptography

Also known as asymmetric cryptography. Public key cryptography uses two types of key, a 'public key' (used to encrypt the message or to verify a signature) and a 'private key' (used to decrypt or to sign a message). The two keys are mathematically related in that the data encrypted with either key can only be decrypted using the other key. Security is based on difficulty to factorise large prime numbers.

The user distributes the public key. Only the user's private key can decrypt the message that has been encrypted with the public key. Therefore it is essential that the user keeps his private key secret. Analogy can be made with a mailbox - the user distributes their address (i.e. their public key). Everybody who has this address can send mail to that address (i.e. a message). To retrieve their mail (message) the recipient uses their personal (private) key to open their mailbox.

For two parties to use public key cryptography, authentication is required to ensure the relationship between the key's pair and its owner. A trusted third party CA (Certification Authority) supplies certificates that assure personal identity. The certificate is a message containing the owner's name associated with the owner's public key and signed by the CA's private key. In order to be widely used, the public key of CA needs to be known to as many people as possible.

The best known algorithm is RSA (devised by Rivest Shamir Adleman). In order to make it difficult to solve, the key size was kept large - the smallest public key length is 512 bit. However, because of the computation time, RSA is impractical for exchanging large messages. Generally crypto-processors are needed in smartcards to perform quickly enough the complex math operations.

5. Interoperability and system suppliers

The following table provides an overview of the technical and security characteristics of various e-purse schemes deployed in Europe. Once again, it highlights some of the differences between the various types of schemes.

Scheme	Card manufacturer	Chip manufacturer / type	ROM / RAM / E(E)PROM	Security	Specific features
Avant Finland	Setec, Gemplus, Bull, G&D Oberthur,	Reloadable: Infineon SLE44C40S, Disposable: Infineon SLE4436E	8 KB / 256 bytes / 4 KB	DES	Unknown
Cash Switzerland	De La Rue, others	STM ST16601	6 KB / 1088 bytes / 1 KB	SAM	Unknown
Chipknip Netherlands	Bull, Philips	STM	CC60: 8 KB / 288 bytes / 1 KB CC1000: 16 KB / 1 KB / 8 KB	RSA, 3-DES, multiple SAM options	Multi-function (CC1000)
Chipper Netherlands	IBM, Schlumberger	STM 16SF48	16 KB / 288 bytes / 8 KB	3-DES	Unknown
Danmønt Denmark	DZ (DK), S-Card, De La Rue, G&D, Schlumberger	Infineon	? / 416 bytes / 1-4 KB	DES, SAM	Unknown
Euro 6000 Spain	Gemplus, FNMT, MESA	STM ST16F42/44/48, Motorola MC68MC05, SC46/48 Infineon SLE44C20 /40/80S Hitachi H8/3152, H8/3151	12-16 KB / 224-384 bytes / 1-8 KB 8KB/24/512 4KB/24/512	3-DES, SAM 3-DES 3-DES	Multi-application, multi-currency
GeldKarte Germany	Gemplus, G&D, ODS	Infineon C805/SE, Motorola, STM, Hitachi H8/3110	12 KB / 256 bytes / … 8 KB/24/512	DES, SAM DES	Multi-functionality
Minipay VISA Cash Italy	Oberthur, Bull	STM 16SF48	6 KB / 288 bytes / 8 KB	DES, SAM	Unknown
Mondex UK	Dai Nipon Printing	Hitachi H8/3112	8 KB /24/1kbytes	RSA 576 locking with PIN	Payment over Internet Card-to-card transactions
Monedero 4B Spain	Gemplus FNMT	Motorola SC24 Infineon SLE44C20/40/80S	12-16 KB / 224-384 bytes / 1-8 KB 3 KB / ? / 1 KB	3-DES, SAM DES, SAM	Multi-application, multi-currency
PMB Portugal	Gemplus, Schlumberger	?	? / ? / 8 KB	DES, PDA/ PSAM	Loading only with bank card and PIN
Proton Belgium	Bull, Oberthur, De La Rue	STM ST16601, ST16F48, Infineon SLE44C40, Motorola SC46	6-16 KB / 128 bytes / 1-8 KB	RSA, 3-DES, SAM	Multi-function, Internet payment, EMV compliant
Quick Austria	Austria Card	Infineon SLE44C42(s), Philips P83C864	16 KB / 256 bytes / 4 KB	DES, RSA, SAM	Multi-application
TIBC VISA Cash Spain	FNMT, G&D, De La Rue, Schlumberger	Motorola MC68H05SC, STM ST16X471, Infineon SLE44C20/40/80S	16 KB / 240-384 bytes / 2-4 KB	DES, SAM	Multi-application, multi-currency, EMV compliant

Table 3 : European e-purse technical aspects

Impact on products and services

Impact on card products

One of the main reasons for the lack of interoperability between existing e-purse schemes across Europe is the difference in the way that session keys are managed. Today's e-purse systems are based on symmetric algorithms for which interoperability means sharing at least keys for payment transactions. The CEPS e-purse system is based on asymmetric algorithms (RSA) , which allows interoperability between different issuers without sharing any key.

Interoperability does not mean a convergence of the different e-purse systems, at least in the short term. Existing e-purse systems do not have to be completely redesigned to comply with the CEP specification. A CEPS layer implemented on an existing purse can ensure interoperability - as is shown in the following schematic. Adopting this route to interoperability will also ensure that the huge investment in existing e-purse systems is protected.

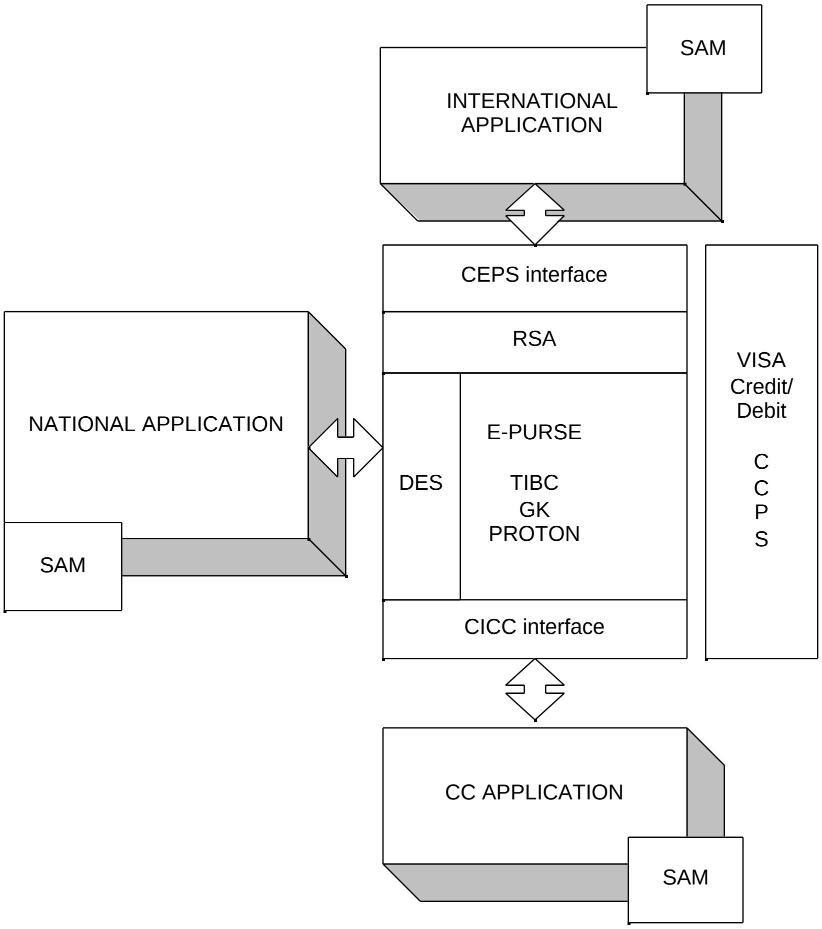


Figure 10 : National e-purse versus CEPS e-purse card

An e-purse application might be supported by different cards such as disposable cards, anonymous e-purse, e-purse linked to an account, and multi-application cards. The multi-application cards might support debit/credit applications or ticketing application (NB: a ticketing application requires a contactless interface).

Some of these existing cards will not be able to support a CEPS layer - at least in the short term. Disposable cards are cost critical e-purses. CEPS require a component with an RSA realistic options in domestic e-purse applications. Furthermore, disposable cards are often used as promotion tools at special, localised or domestic events - such as the Olympic Games held in Altanta. As such, production cost is critical for the promoter and it is unlikely that consideration would be given to a more expensive CEPS-compliant card when it is not really required.

For mixed cards supporting both e-purse applications and ticketing applications, components offering an RSA engine and contactless interface do not exist today in 8 or 16 bit architectures. However, with 32 bit RISC architectures it will be possible to manage RSA function without an RSA dedicated coprocessor.

Today, the range of cards supporting e-purses that could comply with CEPS is as follows :

Disposable card	No	Component cost would be prohibitive
Anonymous Purse	Yes	
Purse linked to a bank account	Yes	
Purse with debit/credit application	Yes	
Purse with CICC applications	No	Would require a move to a RISC architecture chip

Impact on card readers/terminals

In CEPS, a SAM (Secure Access Module) is used for offline (PSAM) and for online (LSAM) transactions. In the current CEPS version, contactless transactions are excluded. The technical study carried out as part of the SmartEuro project focused on offline transactions, so only PSAM has been taken into account within this White Paper.

The PSAM generates a session key and encrypts it using RSA with the card’s public key. It then sends it to the card, which retrieves it using its private key. The PSAM must support both asymmetric (RSA) and symmetric (3-DES or equivalent) cryptography.

The PSAM should store the certification public key index in order to allow interoperability between different card issuers. Two PSAMs, one for domestic use and one for CEPS transactions (Purchase and Cancel Last Purchase) would allow the implementation of CEPS in an existent reader/terminal. It should also be borne in mind that the terminal must be fully compliant with EMV Part I and compliant with Part III Application Selection.

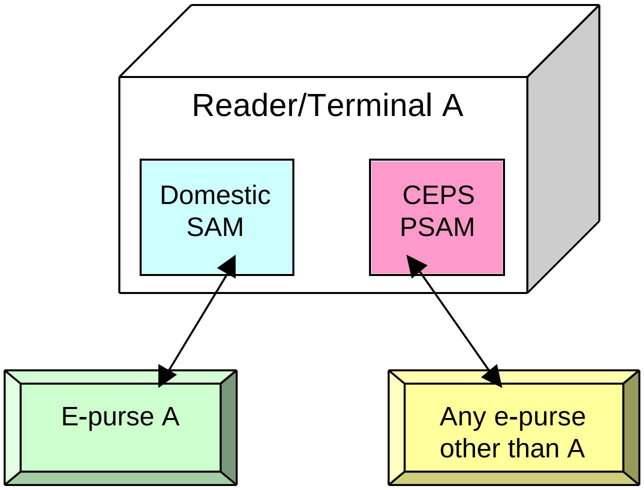


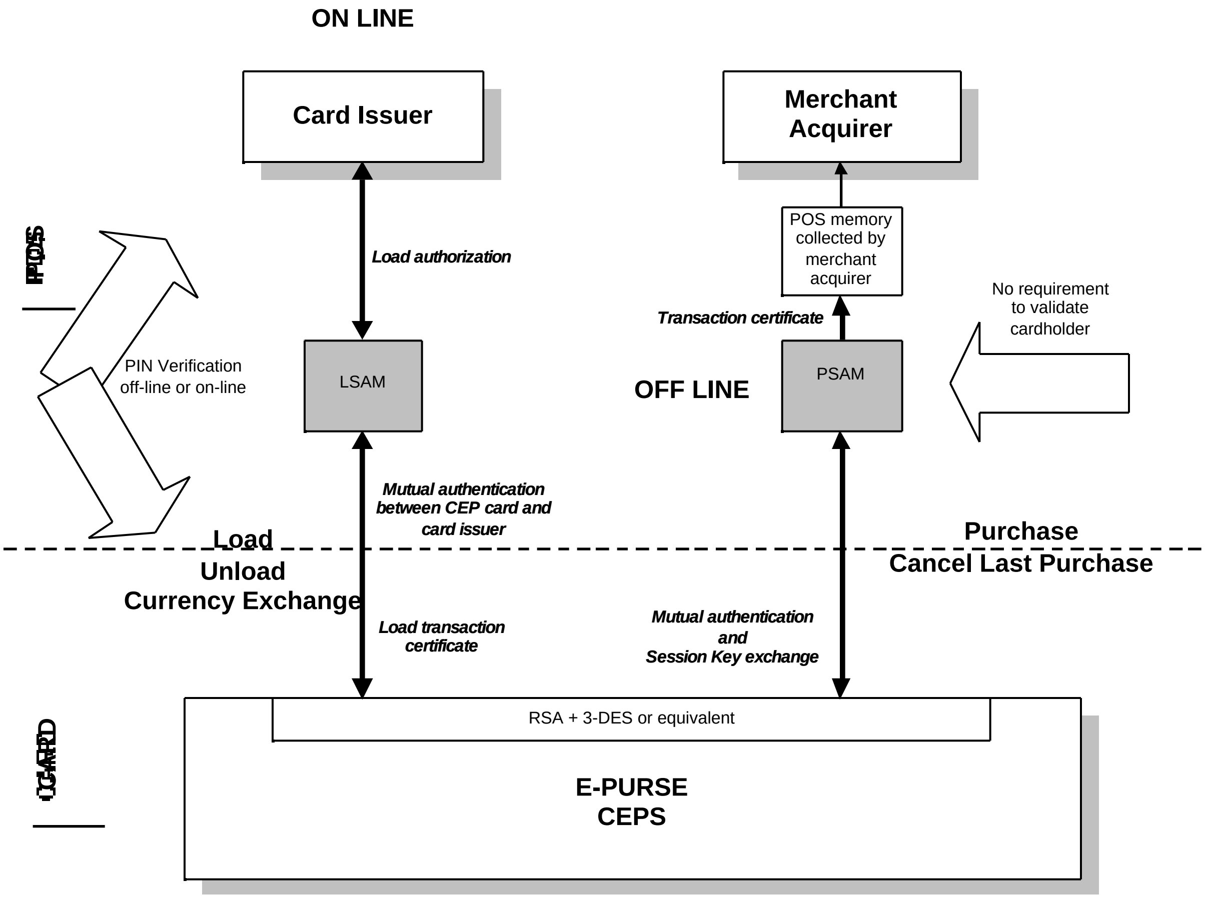
Figure 11 : A possible CEPS implementation in an existent reader/terminal

CEPS security

The following schematic describes the global security procedures used in the CEPS specifications.

- A SAM (Secure Access Module) is used in the purchase device (PSAM) and in the load device (LSAM).
- Two types of communication are supported according to the transactions:
  - Load, Unload and Currency Exchange are realised on-line
  - Purchase, Cancel Last Purchase are realised off-line
- PIN verification is not required for off-line transactions. For loading, cardholder verification is done using PIN verification either on-line or off-line.
- The PSAM must support RSA capabilities. It generates a secret session key that is sent to the card using the 'wrapping' technique. The RSA is used to transmit securely a session key encrypted with a public key. At the same time, a mutual authentication is realised.
- LSAM must allow script messaging from the issuer to the CEPS card. It generates a secret session key that is used to communicate with the card issuer.

The CEP card holds a derived secret session key related to the card issuer. It is used to decrypt the issuer load authorisation.


ON LINE
Card Issuer
Merchant Acquirer
POS
Load authorization
POS memory collected by merchant acquirer
Transaction certificate
No requirement to validate cardholder
PIN Verification off-line or on-line
LSAM
OFF LINE
PSAM
Mutual authentication between CEP card and card issuer
Load
Unload
Currency Exchange
Purchase
Cancel Last Purchase
Load transaction certificate
Mutual authentication and Session Key exchange
RSA + 3-DES or equivalent
CARD
E-PURSE
CEPS

PSAM: Purchase Secure Access Module
LSAM: Load Secure Access Module

Figure 12 : CEPS Security features

Impact on migration path implementations

The big question is if it is possible to undertake an EMV migration (magstripe to smartcard or smartcard to smartcard) and a CEPS migration in parallel.

CEPS require a public key algorithm (RSA) for offline transactions and EMV requires a public key algorithm only if Dynamic Data Authentication (DDA) is chosen. Therefore, a CEPS migration cannot be undertaken at the same time as an EMV migration supporting only Static Data Authentication (SDA).

Public key computation can be executed both with RSA hardware or software. RSA computations are quite long and RSA software is too slow. That is why RSA software solutions are not suitable. RSA hardware implementation requires a technology upgrade, i.e. the use of a chip supporting 3-DES and a crypto-processor. Computation will be faster but the cost will be higher.

In EMV, a three-layer public key certification scheme is used, i.e. the terminal needs to verify two certificates in order to retrieve and authenticate the card's public key. In CEPS, it is the same certificate hierarchy except that there is an optional regional certificate. Thus, a 3 level hierarchy should be chosen to follow EMV hierarchy.

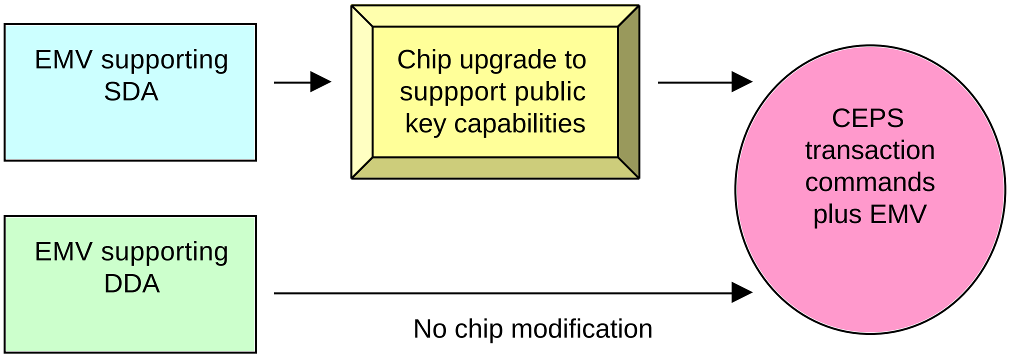

EMV supporting SDA
Chip upgrade to suppport public key capabilities
CEPS transaction commands plus EMV
EMV supporting DDA
No chip modification

Figure 13: Impact of EMV Authentication methods on CEPS implementation

Note: An online only card without SDA or DDA is defined in EMV but does not represent any interest for CEPS.

6. Card issuers' strategies

How do the different card issuers view interoperability and how do they plan to migrate their existing systems to provide interoperability? Three key areas were reviewed:

- specific situations and local market constraints that needed to be considered;
- attitude to various migration schemes;
- attitude toward various standards-related bodies such as CEPSCo, ECBS etc.

The following summarises their various strategies and is the result of interviews that took place between EUROSMART members and the issuers.

France: GIE Cartes Bancaires

Specific situation and constraints of the local market to be considered

- Three e-purse pilot projects exisit in France: Moneo in Tours; Modeus in Paris; Mondex in Strasbourg.
- Main features of existing e-purse projects:
  - Both Moneo and Modeus are fully auditable schemes, Mondex is not.
  - Moneo is based on Geldkarte specification.
  - Modeus is based on a proprietary solution with contact and contact-less interface.
  - Mondex is based on the Mondex International E-purse specifications.
- Specific marketing target of each system:
  - Moneo is targeting all consumers in the Tours area. Focus of the pilot is to insure interoperability with the German e-purse application, and to extend the scheme to other parts of France.
  - Modeus links an e-purse application to transport application, and will leverage on the existing RATP-SNCF (French transport operators) transport infrastructure in Paris and suburbs to reach critical mass.
  - Mondex project is operated by Crédit Mutuel in Strasbourg, and aims at providing real multi-application to the card holders, not only e-purse, using the Multos platform.

Migration schemes towards interoperability

Contribution to a working group:	No
Reference to an interoperable spec:	No
Expected area of interoperability:	Regional
Migration timeframe:	

Relationship between CEPS, ECBS, others

Official contribution to CEPS working group:	No
Official announcement concerning CEPS specification implementation:	No
Support to ECBS/TDC110 workshop:	No

In France, the first step would be to rollout the existing pilot e-purse schemes. It is unlikely that the Mondex scheme will be CEPS compliant due to the company's existing stance. Jeanfor Mondex France has stated that he does not care about (CEPS) convergence and that "we (Mondex) are working on convergence with other banks. If we can't achieve it, as long as merchants acquire POS terminals with several SAMs, they will be able to accept several e-purses for customers.".

Modeus is operating a contactless scheme suitable for transport operators. They will likely focus more on a national rollout than a migration to CEPS. It is worth noting that at present the Modeus scheme does not meet requirements in terms of transaction time.

Moneo is the French e-purse scheme that is best positioned for future migration to CEPS, but again the first target would be a national rollout. We can thus expect SEME (Société Européen de Monnaie Electronique) to start thinking of CEPS migration by the end 2000.

Belgium: Banksys

Specific situation and constraints of the local market to be considered

- One e-purse project exists in Belgium: Proton
- Main features of existing e-purse project:
  - Proton is a fully auditable national banks interoperable scheme.
  - Proton is originally based on a proprietary solution from Bull (CC). Banksys planned to issue new specifications in 2000 and they will have the ownership of the new mask.
  - No compliance to any specific standard.
- Specific marketing target of each system:
  - E-purse is accepted at both e-purse only terminals and combined terminals (credit/debit & e-purse)
  - One of the most used e-purse with an average of two transactions/month/card (figures for active cards).
  - Apart from general retail, the Proton e-purse is accepted in parking meters, vending machines and payphones.

Migration schemes towards interoperability

·	Contribution to a working group:	CEPSCo
·	Reference to an interoperable spec:	CEPS (for next card generation)
·	Expected area of interoperability:	CEPS interoperable area
·	Migration timeframe:	CEPS scheduled in 2001

Relationship between CEPS, ECBS, others

·	Official contribution to CEPS working group:	Yes
·	Official announcement concerning CEPS specification implementation:	Yes
·	Support to ECBS/TDC110 workshop:	?

Belgium will definitely be one of the first countries to migrate its national e-purse scheme to a CEPS compliant scheme. They have been proactive on this issue and plan to operate their e-purse cards in two different modes:

- Domestic mode for Belgium (Proton based)
- Foreign mode for countries where CEPS infrastructure is available.

Spain: CECA (Spanish Confederation of Saving Banks)

Specific situation and constraints of the local market to be considered

- Three e-purse projects exist in Spain: Euro 6000; Monedero 4B; VISA Cash.
- Main features of existing e-purse projects:
  - All projects are fully auditable.
  - VISA Cash is based on a proprietary solution (TIBC).
  - Euro 6000 and Monedero 4B based on CEN 1546 standard.
- Specific marketing target of each system:
  - Euro 6000: local projects of Saving Banks supported with value added applications on the same card.
  - Monedero 4B: Closed small projects.
  - VISA Cash: general audience.

Migration schemes towards interoperability

· Contribution to a working group:	ECBS
· Reference to an interoperable spec:	No
· Expected area of interoperability:	Domestic
· Migration timeframe:	Starting in the middle of 2001

Relationship between CEPS, ECBS, others

Official contribution to CEPS working group:	No
Official announcement concerning CEPS specification implementation:	No
Support to ECBS/TDC110 workshop:	Yes

CECA has adopted a 'wait and see' position for now, as their national e-purse schemes have required important investment so far in infrastructure and human resources. They are more interested in adding value to the purse with additional applications. They will probably join CEPS as soon as they are convinced by one successful field trial.

Portugal: SIBS (Sociedade Interbancaria de Serviços)

Specific situation and constraints of the local market to be considered

- One e-purse project exisits in Portugal: PMB
- Main features of existing e-purse project:
  - PMB is a fully auditable national banks interoperable scheme.
  - PMB is based on a proprietary solution from Gemplus (the whole scheme is SIBS proprietary).
  - No compliance to any specific standard.
- Specific marketing target of each system:
  - E-purse is accepted at all bank POS terminals + additional 30 000 terminals only dedicated to purse.
  - Widely used in small amount retail transactions.

- Scheme is profitable to SIBS.
- Parallel scheme exists for petrol retail combined with loyalty (Magnetic stripe).

Migration schemes towards interoperability

· Contribution to a working group:	No
· Reference to an interoperable spec:	No
· Expected area of interoperability:	Domestic
· Migration timeframe:	Not planned

Relationship between CEPS, ECBS, others

Official contribution to CEPS working group:	No
Official announcement concerning CEPS specification implementation:	No
Support to ECBS/TDC110 workshop:	No

SIBS have also adopted a 'wait and see' position for now, as their national e-purse scheme has required significant investment so far in terms of systems and infrastructure. They will probably join CEPS as soon as they are convinced by one successful field trial.

7. Card acceptors' expectations

There is a large variety of potential card acceptor (merchant) categories for the e-purse. The following list is certainly not exhaustive:

Supermarkets; grocery shops; vending machine operators; newspaper stalls; taxi; fast food and canteens; gaming and amusement arcade machine operators; post offices; public transport operators; on-line merchants; public utilities; petrol outlets; payphone operators; car parking meters; toll operators; mail order companies.

All these card acceptor categories have common and partially diverging requirements concerning e-cash payments - in both domestic currencies and the Euro - and varying interest in adopting the e-purse as a payment method. Detailed studies of card acceptor requirements are, to the best of our knowledge, not available.

In order to get a better understanding of the card acceptor concerns, a series of workshops were organised by SmartEuro and representatives of the different acceptor categories were invited. The following summarises discussions held with attendees during the various workshops.

Merchant organisations

In general merchants did not have any pre-conceived ideas concerning technical solutions for e-cash payments. They considered this aspect as a responsibility of the supply industry.

Merchants are generally open to the introduction of e-purses. For example, around 40 billion low-value transactions occur each year in France, but debit/credit cards are not usually accepted for amounts below 100 francs because of the high transaction costs. Their main concern was to be reassured that any payment systems introduced today would be usable in the longer term. The current situation in France was cited, where after seven years of discussions three non-interoperable e-purse schemes were announced in 1999 concurrently. Furthermore this happened in a context where a lot of effort had already been invested in upgrading existing information systems to cope with both the introduction of the Euro and the Y2K problem. Not surprisingly merchants were adopting a 'wait-and-see' position.

Merchants considered that technical viability had to be proven first, followed by business and financial aspects. It would seem that merchants are receiving conflicting messages with respect to their existing terminals' capability to be equipped for handling different e-purse schemes, or if existing schemes would all survive. Merchants do not believe that the different e-purse schemes will all be ready for the Euro as a cash-currency in 2002. A big concern was which of the schemes would be sufficiently deployed to be able to replace a significant part of the physical cash.

The perception is that the banks are in a hurry to be ready to use e-purses for payment in Euro in 2002. The transition to the Euro has to be carried out in a very short timeframe and consumer attitudes are difficult to predict. 30,000 tons of coins and banknotes need to be exchanged. Payment transactions are being carried out more and more through other means (i.e. non-cash). Banks and companies that transport coins/banknotes are not sufficiently geared up to manage the circulation of such high volumes of legal tender. So the introduction of alternative non-cash methods of payment will help reduce the logistics nightmare associated with the introduction of the Euro.

Furthermore, the introduction of the Euro as a cash-currency in 2002 is seen as an ideal opportunity to change consumer attitudes to payment methods. Studies had shown that around 50% of citizens would initially have problems in dealing with the Euro. With physical cash consumers would be less comfortable and fear mistakes being made by merchants and sales personnel when handling payments in Euro. This could have an impact on the level of consumer spending during the Euro transition period. The e-purse can be seen as a means to maintain consumer confidence and avoid such problems as no 'physical' cash is involved and no physical 'change' given.

In conclusion, the first requirement for merchants is to get a clear and consistent message about the basic services and benefits to be expected from the e-purse. Merchants could not understand why e-purses introduced in 1999 were not ready for payments in Euro. They are open to the introduction of the e-purse but they need a clear vision and they want to be involved in the decision-making processes. Merchants also envisage some important advantages from e-purses, especially related to merchants' obligations to promote payments by cheque rather than cash (for tax reasons). Accepting cheques for very small amounts is a real constraint.

Vending machine manufacturers and operators

Discussions were held with the European Vending Association (EVA) in the context of electronic payment and the Euro.

EVA is a horizontal vending industry association, grouping thirteen national associations and thirty-nine companies. EVA covers all vending activities and aims at representing the vending industry within the EU and world-wide, serving as a meeting point, a source of information and to establish standards for the vending industry.

Vending refers to unattended points of sale. The environment is very heterogeneous in terms of the nature of products for sale, size of vending machines and payment means, locations where the vending machines are installed, actors involved, type of vending machine operators and their size, etc. It is hence very difficult to get reliable figures on this market.

The advantages of electronic payment in this context are primarily threefold:

- reduced cost for cash handling;
- less maintenance;
- reduced risk of vandalism.

There are however major barriers for the introduction of electronic payment:

- Incompatibility of existing electronic payment solutions. There is no standard for vending machines. The payment means (keys, chipcards, magnetic stripe cards, contactless cards, etc.), reader type and size and mounting position, reader interfaces, etc. cover a large number of incompatible components.
- Level of transaction charges and consumer position. By switching to a cash-less system, a vending machine operator could possibly miss sales to consumers preferring to use cash. The situation may vary considerably depending on the country. For example, Belgium may be more open to the introduction of cashless vending machines than countries with less deployed e-purse schemes. And on the location of the vending machine, which could be outside in an urban or rural area, in a semi-open position or in a closed environment. Globally, transaction charges are also a major barrier.

Due to the huge 'mix' of installed vending machines, the impact of the Euro's introduction on vending machines will vary strongly from one case to another. The impact on simple machines will be higher than on sophisticated ones. Only 10% of the installed base today are cashless machines. Networking is seen as a solution for the future.

EVA is currently working on a standard covering the readers, vending machine form factors, user interfaces, etc., but also the requirements of the vending industry towards the equipment and the banking sector.

In conclusion, the vending market accounts for a huge number of small transactions and due to the problems related to cash handling the operators would have a clear interest in cashless payment solutions. Loyalty schemes are very interesting for many vending machine operators, but the situation is very mixed and will depend on the operators’ profile.

Interoperability of payment solutions is an important issue for vending machine operators.

The suppliers of card readers for vending machines may be equipment suppliers, but large vending machine operators, such as Mars, have their own subsidiaries for payment systems. The introduction of a standard for a reader would open the market.

8. Consumers' expectations

Commercially deployed e-purses have not yet reached a significant number of payment transactions.

The e-purse technology providers and the card issuers are still searching for the right combinations of e-purse features and commercial conditions that might benefit from a large user acceptance.

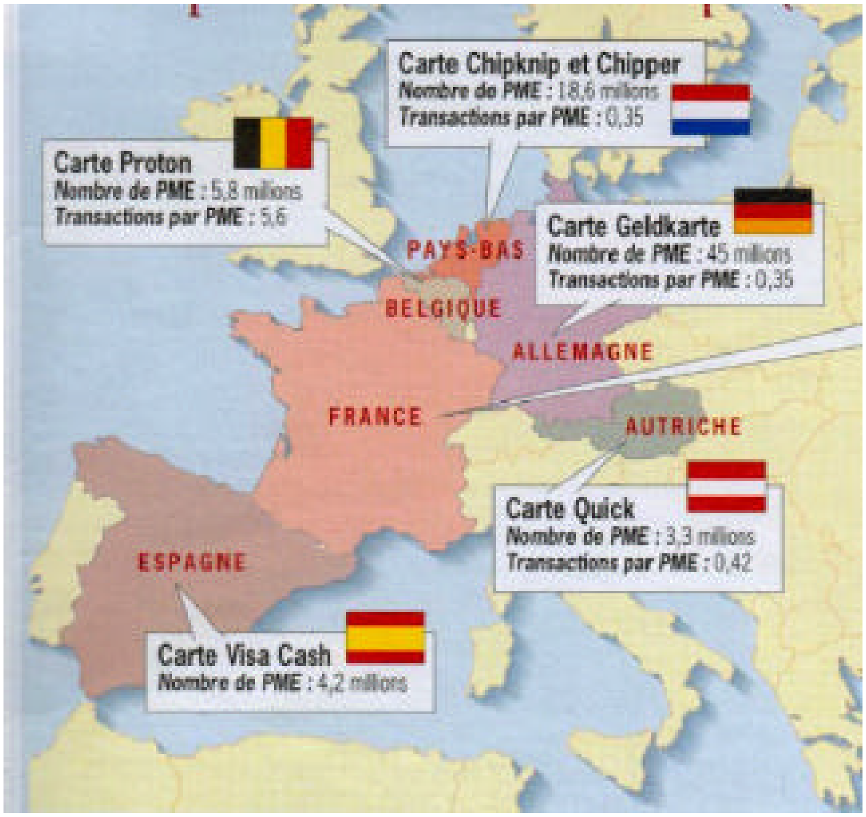

Carte Chipknip et Chipper
Nombre de PME : 18,6 millions
Transactions par PME : 0,35
Carte Proton
Nombre de PME : 5,8 millions
Transactions par PME : 5,6
PAYS-BAS
Carte Geldkarte
Nombre de PME : 45 millions
Transactions par PME : 0,35
BELGIQUE
ALLEMAGNE
FRANCE
AUTRICHE
Carte Quick
Nombre de PME : 3,3 millions
Transactions par PME : 0,42
ESPAGNE
Carte Visa Cash
Nombre de PME : 4,2 millions

Figure 14: Number of cards deployed and average use of some e-purses in Europe

Source: Le Monde de l'Informatique

It should be noted that the figures given in the above map relate to a single moment in time. The e-purse market is extremely dynamic and the above figures were quoted in September 1999. We fully expect that these figures will change significantly over the coming months.

Consumer acceptance has been difficult to assess for two main reasons:

- recent e-purse implementations have all been made in different environments with different approaches concerning the e-purse features, commercial conditions and scale of deployment. The gathering, analysis, comparison of results and creation of general conclusions from all these experiences is an extremely difficult and costly undertaking - best left to those organisations that have a vested interest in undertaking such studies;
- only very limited information is available on the consumer perception of the e-purse. Although various studies have been carried out on consumer reactions, very little material is publicly available.

The following section contains an excerpt of a study carried out by De La Rue and Datamonitor, together with a summary of discussions with a major European consumer organisation. It provides an overview on the conditions of e-purse acceptance by consumers.

Opinions and surveys on e-purse use

The Institut Européen Interrégional de la Consommation (IEIC) is one of the four major consumer organisations in Europe. IEIC have forty-two members in different countries and work closely with the European Commission on consumer affairs.

The main concerns for the consumer, seen from IEIC perspective are:

Interoperability. The e-purse must be usable abroad and on the various schemes at a national level;

Information. The user must be able to see the amount remaining on the card at any time;

Safety. There should be a maximum amount of cash stored on an e-purse (fixed by legislation) and the responsibility for lost amounts on a lost/stolen e-purse should be clarified;

Confidentiality/privacy. The confidentiality for the user should be guaranteed (personal data). It should also not be possible to download new services, offers, etc. on the card without the user's (cardholder) agreement.

Cost. The handling of physical cash is a costly business for the banks - production, logistics, circulation management etc - from which they make very little profit, with the exception of currency exchange. However, there is no cost for the user when paying with real cash. To become a pervasive and acceptable commodity, users should have some control over the evolution of transaction charges on e-purses. Without this level of control, the banks could attempt to maximise their profits in this domain.

Factors conditioning e-purse acceptance

The following gives an overview on the factors that condition e-purse acceptance by consumers. The data was compiled from a study carried out by De La Rue with input from Datamonitor.

Consumer Attitudes

Attitudes to technology:	▪ Capability of magnetic stripe is often over-estimated ▪ Strong concern around data security ▪ Relaxed attitude towards chipcards - they will come anyway ▪ Technology should make life easier not more complicated
Attitudes to money and e-cash:	▪ Consumers do not think that e-cash will replace cash ▪ Consumers are quite reluctant to have two forms of cash to carry ("not yet another card") ▪ Cross-border travel (work and personal) is continuously increasing. Implication - demand for multi-currency payment card ▪ Demand for 24-hour access to funds (and purchasing) ▪ Many consumers worry about credit and the temptation to over-spend ▪ Consumers want to get full benefits of rewards being offered (loyalty scheme, incentive to use cards...) ▪ Even if risks are comparable, loss/theft of an e-purse card is perceived as a major inconvenience

Consumer Expectations	▪ Consumers want to know that their means of payment will be accepted ▪ Consumers want to be able to use their cards from one country to another ▪ Consumers do not want to carry more cards ▪ Consumers want the card to be widely accepted ▪ Consumers do not want to have to memorise yet more PIN numbers ▪ Consumers want greater security (photograph etc.) Consumers are surprised that issuers don't make use of the security methods available ▪ E-purse has to add value to cash ▪ For multi-applications, consumers want to be able to decide which application is on the card (Open Platform)

Main Drivers and Barriers to e-purse acceptance

Drivers:	▪ More security is required (fraud, cash handling/policing, card lost or stolen...) ▪ Too many cards. Consumers want multi-application cards ▪ Considering that e-purse will be more & more often issued on multi-application cards, banks are seen as trusted and natural issuers of this type of cards. ▪ Acceptance of e-purse for unattended-POS; payphone, transport, (strong added-value to cash) ▪ Cash is perceived as being free. Therefore, e-purses should be free ▪ E-purse has to be as convenient as cash - fast & anonymous (no signature, no PIN) ▪ Multi-currency capability is a key advantage over cash until the introduction of the Euro. By 2002, if the Euro is not available on the e-purses in Europe it could become a key barrier to acceptance. ▪ Needs for means of making small payments adapted to Information Society. Home banking, telephone banking, e-commerce, mobile commerce, Web TV, mass transit... ▪ Balance reader and statements
Barriers:	▪ Concerns about security in remote-POS transactions ▪ Resistance to separate payment card ▪ Resistance to have 2 different forms of cash (electronic & classic) ▪ Resistance to card fees ▪ Lack on interoperability : consumers want to be able to use their wherever they are (national & international) ▪ Some consumers dislike concept of pre-payment ▪ In some countries users might object to audited e-purse schemes ▪ Monetary and fiscal authorities might object to non-audited schemes because of money laundering and tax implications

Conclusions and recommendations

Initiatives promoting e-purse interoperability

CEPS are currently the only open standard with a potential to federate existing e-purse schemes on an e-purse interoperability solution. It has gained the support of the large majority of the industry and should be considered by all players concerned as the common basis for the definition of interoperability migration strategies.

Learn from previous experiences

The implementation of a global framework for the migration towards e-purse interoperability should take into account previous experiences. One should in particular take advantage of the lessons learnt in the migration to EMV with regards to type approval, compliance verification and encourage establishing decentralised institutions to take care of these tasks in the different countries, these institutions being subject to accreditation and audits.

EMV and ISO compliance

Since CEPS relies on EMV level 1, the implementation of EMV on the existing infrastructure should be planned as a preparatory step for the migration to CEPS.

With regards to card accepting devices, one must determine whether they will support multiple applications and therefore must be prepared to introduce some after the initial installation. One must further be aware of the divergences between ISO and EMV in case some of the applications originate from a non-financial sector and require ISO compliance.

Industry participation in CEPSCo

A higher level of co-operation between CEPSCo and industry would be beneficial to all. It has not been an easy task to obtain clear technical and marketing information and documentation on CEPS. CEPSCo should take into account the domain knowledge of the supplier industry as well as the requirements of the players concerned with the e-purse and its interoperability aspects, especially the card acceptors.

Current technology limitations

There are now two important trends in card based payment solutions:

- the trend towards interoperability of e-payment transactions;
- the trend towards multi-application cards.

These trends will push the currently available card technology to its limits. It will be very difficult to implement on existing and soon to be available smartcard chips the required memory capacity and hardware (crypto co-processors, memory management unit) for multi-application cards with a CEPS compliant e-purse function. More sophisticated operating systems and application environments could provide a solution by supporting on-demand downloading of applications.

Local differences

There can be no single migration strategy for all European countries. The definition of local migration strategies must deal with the specifics of the local differences; such as different infrastructures; possible EMV introduction programmes; existence or not of existing domestic e-purses; current business practices and commercial agreements; market segments that need to be covered and the impact of specific application requirements; habits of consumers and card acceptors, etc.

Issuers of CEPS compliant e-purses will have to define products according to their perception of the needs of different markets. Possible alternatives to be considered for new programmes include:

- domestic e-purse based on CEPS if performance is deemed acceptable;
- using CEPS specifications under domestic commercial agreements;
- domestic CEPS with international payment system brands under commercial terms governed by the brands
- a combination of a domestic purse using fast symmetric cryptography with a CEPS engine to handle cross-border payments,
- CEPS on a single application card i.e. a mono-service product (although the business case might be difficult)
- CEPS on a multi-application card i.e. one of multiple services on a product.

Requirements for new infrastructures

The cost of interoperability depends on the timing of its implementation. It is obviously easier and cheaper to build it into the initial system design than to re-engineer an already deployed system.

To achieve maximum flexibility, new installations should ensure that the devices possess the necessary technical characteristics to handle evolution after the installation of the device. Evolution means both enhancing existing products and introducing new products.

Examples of terminal hardware requirements include sufficient memory, processing power, SAM slots, memory management, open architectures, secure software downloading capability, etc. With such facilities, the flexibility to introduce or amend applications after device installation will be available, enabling the issuers of products to decide what they will do or introduce and when, as required by their domestic environment.

Cost of migration

The question of the cost level has no answer yet, nor the question of whom will pay. The investments to implement interoperability seem to be high compared to the generated business, not to mention the revenue potential.

E-purse interoperability would seem to present a difficult business case, which would benefit from being studied in detail, including an assessment of various options.

European Electronic Central Bank

The issue of clearing and settlement must be clarified, likewise the relationship between possible national organisations and the European Central Bank. It is important that the ECB determines its role in the overall handling of e-money, in particular how the flow of e-money will

If ECB chooses not to play a role in this domain, then the establishment of a European Electronic Central Bank should be considered.

In either the case, the responsibility for the control of the certification processes should be left exclusively to the private sector.

The Euro as a domestic e-cash currency

The strategy of the international payment networks is to offer CEPS interoperability as an additional cross-border payment brand mark to domestic e-purses. Domestic payments would hence be made with the existing domestic e-purses and cross-border payments with the CEPS compliant (CLIP, VISA Cash) e-purse. Payment transactions would be settled over the existing infrastructure of the international payment networks.

This raises a question concerning Euro payments. Should the Euro be considered as the 'domestic' e-cash payment currency within EMU, or as an exchange currency for e-cash payments between EMU states? For example, should a transaction payment in France with an e-purse issued in Belgium be considered as a cross-border payment?

The SmartEuro partners believe that the Euro should be considered as a domestic currency in the Euroland. In line with this, a settlement infrastructure is needed at the EMU level for CEPS based Euro payments.

Card acceptors

Merchants have (or had) high expectations for e-purse solutions in the context of the introduction of the Euro. Important issues for them are the cost of equipment (and use) and the durability of their investments. Interoperability standards play a major role in this context.

It can be assumed that recently delivered terminal products are EMV compliant. It can also be assumed that future terminal products will be CEPS compliant. However the installed base of terminals can be estimated to over one million units that will need to be upgraded (if this is possible) or replaced. In view of the existing timing constraints and the complexity of implementing CEPS based interoperability, it is almost impossible to envisage more than a very small fraction of the technical infrastructure converted to CEPS compatibility when the Euro as a cash currency is implemented in EMU states - i.e. by 2002.

Consumers

Little information is available on consumer expectations, payment habits and the conditions for achieving a market acceptance for e-purses in general. Similarly, for their expectations concerning e-purse interoperability and cross-border.

More effort should be spent on the preparation of dedicated publicly available market studies, the implementation of pilots, the assessment of the results of e-purse trials and their publication, as well as awareness campaigns towards consumers, merchants and the industry. The European Commission should play a leading role in this context.

Key user requirements are obviously, besides low usage cost, ease of use and widespread acceptance of e-purses. Technical complexity of e-purse interoperability implementation should be made as transparent as possible to the user. The consumer should have a unified view of his e-purse, be it for domestic or cross-border use and for payments in the real world or the virtual world.

Transport applications

The combination of e-purse functions with transport applications is considered important for its potential of accelerating e-purse deployment and the general improvement of the e-purse business case.

Transport applications require contactless operations to achieve the transactions speed needed.

To date, technology has not reconciled the requirements of CEPS compliant e-purses (public key infrastructure, transaction complexity) with the requirements of transport applications (contactless operation, fast transaction speed). The constraints of the contactless operation in terms of energy management and operating time do not at present allow the implementation of CEPS compliant transactions.

Alternative solutions must be found to enable the integration of both transport and e-purse applications on a single card.

European and national authorities

The deployment and use of e-purse payment could be significantly accelerated in Europe if the governments of the different countries would promote e-payment of various public fees. Whilst requesting more effort for the deployment of e-payment solutions from the industry, the governments are often latecomers for implementing such solutions for their own use. The European Commission should provide incentives for the Member States to adopt and promote e-purse payment solutions.

The Internet

E-purse features should be considered within the perspective of the potential of the Internet. The Internet and the mobile networks should be considered as major opportunities to develop e-purse based payment solutions. They have the potential to increase the usability and added value for the user by supporting options such as remote e-purse loading features.

Internet based payment requires interoperability standards. The implementation of CEPS based interoperability should be considered in light of the migration of payment infrastructures in both the real and virtual worlds.

CEPS pilots

Pilot projects based on CEPS should be set-up as soon as possible in view of the approaching introduction of the Euro as a cash currency.

Pilot objectives and approaches should bear in mind previous similar pilot projects, learning from both successes and failures. They should also take into account the work currently underway on PKI in various EU initiatives.

In view of the complexity of the underlying technology and the required type approvals, the pilots should be organised in two phases, starting with a stand-alone CEPS e-purse in the first phase, before implementing a multi-application environment in a second phase.

The pilot location and users to be involved should be carefully chosen. Since interoperability will be mainly perceived as beneficial in cross-border payment operation, the pilot should be set-up in suitable and relevant environments, such as airports, trans-European trains, popular tourist regions, etc. Euroepan Institutions themselves would represent suitable locations as well, with their various centres in Brussels, Luxembourg, Strasbourg etc.

The choice of regions in which the implementation of EMV has already well progressed would simplify the required upgrades to the infrastructure. In the same way, it’s important to think about CEPS functionality when migrating to EMV. For example, terminals should include optional multi SAMs slots.

The pilots should take into account the added-value services enabled through the Internet and mobile networks (e-commerce and m-commerce). Furthermore the use of these networks could simplify the implementation of complex operations, such as e-purse load operations. It should also be borne in mind that the use of mobile phones would avoid the necessity to go through all the current acquirer networks associated to the terminal.

Appendices:

Glossary of terms and definitions

Acronyms

ACH	Automated Clearing House
ANEC	European Association for the Co-ordination of Consumer Representation in Standardisation
API	Application Programming Interface
ATM	Automated Teller Machine
C/D	Credit / Debit (banking cards)
CEPS	Common Electronic Purse Specifications
DES	Data Encryption Standard
DS	Digital Signature
ECBS	European Committee for Banking Standards
EDI	Electronic Data Interchange
EFT	Electronic Funds Transfer
EFT - POS	Electronic Funds Transfer at the Point Of Sale
EITO	European Information Technology Observatory
EMV	Europay - MasterCard – VISA (Standard issued for C/D cards)
EP	Electronic Purse (e-purse)
ETSI	European Telecommunication Standard Institute
EVA	European Vending machines Association
GSM	Groupe Systemes Mobiles or Global System for Mobile communications
HSM	Hardware Security Module
ICC	Integrated Circuit Card
ISO	International Standards Organisation
LSAM	Load Secure Access Module
MAC	Message Authentication Code
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point Of Sales (terminal)
PSAM	Purchase Secure Access Module
SAM	Security Access Module
SET	Secure Electronic Transaction
SIM	Subscriber Identification Module

Definitions

Term	Description
Application Programming Interface (API)	An interface between the operating system and application programs, which includes the way the application programs communicate with the operating system, and the services the operating system makes available to the programs.
Asymmetric Cryptosystem	Synonym for Public Key Cryptosystem
Authentication	The process whereby a card or a terminal verifies that the other party is genuine.
Automated Teller Machine (ATM)	A machine which can handle many of the functions of a bank teller, including the dispensing of cash.
Card issuer	The entity responsible for issuing cards and obliged to pay or redeem transactions or balances presented to it. Issuer is usually, but not necessarily, a financial institution or a group of financial institutions.
Card reader	Equipment that can electronically read the information from one or many types of cards.
Cardholder	Generally the person to whom a nominative card is issued. For financial transaction cards, the cardholder is usually the customer associated with the primary account number recorded on the card.
Certification Authority	A body able to certify the identity of one or more parties in an exchange (an essential function in Public Key Cryptosystems).
Chip card	Also known as an integrated circuit (IC) card. A card containing one or more computer hips or integrated circuits for identification, data storage or special-purpose processing used to validate personal identification numbers (PINs), authorise purchases, verify account balances and store transaction and/or personal data.
Clearing	The process of transmitting, reconciling and, in some cases, confirming financial transactions between financial institutions prior to settlement, possibly including netting of instructions and the establishment of final positions of settlement. Sometimes the term is used (imprecisely) to include settlement.
Closed prepaid system	A system where the Issuer and Acquirer of the card are the same party. The card is issued by the party that provides those services that can be accessed by the card.
Closed systems	A system whose use is limited to the original application issuer(s). Common closed systems include campus cards, corporate badges, etc.
Common Electronic Purse Specifications (CEPS)	Specifications established by a number of payment organisations for smartcard-based electronic purses.
Contact	A point of electrical connection between an integrated circuit card and its external interface device. ISO standard IC cards have eight contacts (the contact plate is commonly called a module).
Contact Smartcard	A smartcard that operates by physical contact between the reader and the smartcard's different contacts (in comparison to Contactless smartcards).
Contactless Smartcard	A smartcard with no visible module that communicates by means of a radio frequency signal. There is no need of physical contact between the card and a reader (in comparison to Contact smartcards)
Credit Authorisation Terminal (CAT)	A device placed in a merchant location which is designed to verify by electronic means whether the customer (cardholder) is authorised to complete the transaction requested.
Credit card	A card whose the cardholder has been granted a line of credit with the

	cash up to a prearranged ceiling; the credit granted can be settled in full by the end of a specified period or can be settled in part, with the balance taken as extended credit. Interest is charged on the amount of any extended of any extended credit and the holder is sometimes charged an annual fee.
Cryptography	The science of transforming confidential information to make it unreadable to non-authorised parties (see also Public Key, Private Key, DES, RSA).
Data Encryption Standard (DES)	DES is a private key encryption algorithm, where the same key is used for encryption and decryption. The key must be kept secret and distributed securely in order to maintain system security. DES has been adopted by the US National Bureau of Standards and is used extensively in the banking world. Smartcards are available which can encrypt and decrypt DES messages internally. A strengthened version of DES called triple DES (or 3-DES) is commonly used in bankcards. See also Private Key Cryptosystems.
Debit card	A card where purchases and/or cash withdrawals are charged directly to the account of the cardholder and credited to the merchant.
Electronic cash (e-cash)	Sometimes referred to as "digital cash". A system seeking to emulate cash over the Internet to pay for goods and services. The key feature of e-cash is anonymity, which implies that money circulates as an electronic token. E-cash systems require sophisticated security.
Electronic commerce (e-commerce)	Doing business electronically. E-commerce often refers to business that is conducted (up to and including payment) over electronic networks (especially the Internet).
Electronic Data Interchange (EDI)	Standard format for exchanging business data. An EDI message contains a string of data elements, each of which represents a singular fact, such as a price, product model number, and so forth, separated by delimiters. The entire string is called a data segment. One or more data segments framed by a header and trailer form a transaction set, which is the EDI unit of transmission (equivalent to a message). A transaction set often consists of what would usually be contained in a typical business document or form. The parties who exchange EDI transmissions are referred to as trading partners. EDI messages can be encrypted. There are two EDI standards: the first one is ANSI X12 and it was developed by the Data Interchange Standards Association in the United States. The second one is EDIFACT, which is more international.
Electronic Funds Transfer (EFT)	A system that transfers funds through electronic messages instead of by physical means, such as cash or cheques. A generic term describing any transfer of funds between parties or depository institutions via electronic data systems.
Electronic Funds Transfer at the Point Of Sale (EFT - POS)	A data network linking banks, debit cardholders, and merchants that permits a consumer to make direct electronic payment at the place of purchase, via electronic terminal, and a merchant to be credited without physical intervention.
Electronic money (e-money)	The term is used loosely to refer to a wide variety of payment mechanisms, based on transfer of value via data networks. E-money products can thus be defined as "stored-value" or "prepaid" products in which a record of the funds or "value" available to a consumer is stored on an electronic device in the consumer's possession. The electronic value is purchased by the consumer (for example, in the way that other prepaid instruments such as travellers' cheques might be purchased) and is reduced whenever the consumer uses the device to make purchases. In contrast to the single-purpose prepaid card schemes (such as those offered by telephone companies), e-money products are intended to be used as a general, multipurpose means of payment. This definition covers both prepaid cards (see electronic purse) and prepaid software products that use computer networks such as the Internet. E-money also refers to schemes where currency issuer is not a financial institution, supervised by central banks. Both the definition and the regulatory implications of e-money are

	subject of intensive but so far inconclusive discussions among academics, regulators and financial institutions.
Electronic Purse (e-purse)	A small portable device which contains electronic money. The smartcard is the ideal device to implement an electronic purse. It is sometimes called the electronic wallet or stored value card. An e-purse can de disposable or reloadable.
EMV	Set of specifications defining the main structures for an international Debit/Credit smartcard. (EMV: Europay - MasterCard - VISA)
Encryption	A means of scrambling data so that it can only be understood by the party that has the key to changing it back to its original format. In the plastic card world, the encryption of data is performed using either a private key cryptographic system such as DES or a public key cryptographic system such as RSA.
European Telecommunication Standard Institute (ETSI)	The EU organisation in charge of defining European telecommunications standards. The most well known European telecom standard is GSM. ETSI has been very active in the Smartcard field in building European standards where there are holes in the ISO standards. All ETSI card standards work is based on ISO standards where published.
Float	The value arising from the delay between the time a payment instrument is used and the time when it is actually debited or credited. For a financial institution, float can be positive (in case of banks using value date to debit an account before the payment is made) or negative (in case of debit card account with an end-of-month debit date).
Global System for Mobile communications (GSM)	Global System for Mobile Communications, a European standard for digital cellular telephones that has now been widely adopted throughout the world. Under the ETSI standard, GSM telephones contain a SIM smartcard that identifies the individual subscriber.
Home Banking	Retail banking operations conducted by customers using electronic payment terminals in their own homes.
Hot list	A compilation of lost, stolen over limit or counterfeit cads, which is used to verify the legitimacy of the transaction during authorisation process.
International Standards Organisation (ISO)	ISO has published standards for a variety of cards and work continues on smartcards (contact and contactless), optical memory cards and others. For smartcards, the central standard is ISO 7816. ISO 7816-1 Physical Characteristics of IC cards ISO 7816-2 Position of Module and Contacts on IC cards ISO 7816-3 Exchange protocol with IC cards (i.e., communication between readers and cards) ISO 7816-4 Command set for microprocessor cards
Interoperability	The ability of products manufactured by different companies to operate correctly with one another.
Java	An object oriented programming language developed by Sun Microsystems. Java is a machine independent language and offers considerable protection between applications.
JavaCard	A set of specifications for running a subset of Java on a smartcard.
Key	A value that is used with a cryptographic algorithm to encrypt, decrypt or sign data. Secret Key Cryptosystems use only one secret key. Public Key Cryptosystems used a public key to encrypt data and a private key to decrypt it.
Key Length	The number of bits forming a key. The longer the key, the more secure the encryption. Government regulations limit the length of cryptographic keys in a number of countries.
Key Management	Generation, transmission and storage of keys in a Cryptosystem.
Mask	The software routines contained in a smartcard, including OS and application software.
Memory Card	A smartcard containing a memory chip with read / write capability and in some cases hardwired security functions (some people do not consider memory cards as smartcards).

	and a contact plate, connected by fine wires and encapsulated in a drop of epoxy resin. The mircomodule is inserted into a cavity in the card body to form a finished card.
Multi-application card	A smartcard that can accommodate several applications (from different owners) while maintaining separate security conditions.
Multi-function card	A smartcard that can accommodate several applications from the same owner.
Multos	A programming language developed by Mondex for systems using MAOS (multi-application operating systems) for smartcards.
Off-line	In the card area, the term off-line refers only to the authorising of a transaction or an entry to a building and requires that such operations are carried out without referral to any other part of the network. Most off-line transaction systems, however, are not completely off-line in this sense either since a proportion of transactions will be authorised on-line as an additional check against fraud and bad debt.
On line	This refers to any system where individual components are connected via telecommunications lines either directly to each or indirectly via a switching centre. In the card area, it is used to refer to a system where both the cards and the operations which are carried out with them are authorised by a central processor.
Payment system	A set of instruments, procedures and transfer systems among several financial institutions that facilitate the circulation of monetary value and settlement of transactions.
Personal Identification Number (PIN)	Secret code entered into a terminal (ATM, POS) to identify the cardholder.
Point of Sale Terminal (POS)	An electronic device at a retail location that allows merchants to accept a debit card. The same device may also be use to accept credit cards. These terminals can be online or offline.
Prepaid card	A card on which value is stored, and for which the holder has paid the issuer in advance. (See also store-value card and electronic purse)
Private Key Cryptosystem (or Secret Key Cryptosystem)	A cryptographic system that uses a single key for encrypting data. The most well-know private key algorithm is DES. Synonym: Symmetric Cryptosystem. See also Public Key Cryptosystem.
Protocol	A set of rules and procedures governing interchange of information between a smartcard and a reader. The ISO defines several protocols, including T=0, T=1 and T=14
Public Key (PK)	Public key Cryptosystem are based on trapdoor one way functions. Forward direction: encryption, Inverse direction: decryption.
Public Key cryptography	Cryptosystem invented by Whitfield Diffie and Martin Hellman in 1976 to solve the key management problem: each person gets a set of 2 keys: the public key is used to encrypt messages and the private (secret) key to decrypt messages. The most well-know public key algorithm is RSA.
RSA	Rivest, Shamir, Adleman. An important and very secure public key cryptography system already able to be performed internally by certain smartcards. Named after its three inventors.
Secret Key	Value used in an algorithm to enable authentication or communication ciphering.
Secret key cryptography	Sender and receiver of an encrypted message use the same (secret) key to encrypt and decrypt the message.
Secure Electronic Transaction (SET)	Security protocol developed by VISA and MasterCard for authentication of credit card transactions over the Internet.
Security Access Module (SAM)	A dedicated microprocessor unit that enables active authentication with appropriate memory or microprocessor card.
SET	Secure Electronic Transaction. A technology developed by a group of companies including IBM and VISA for e-commerce.
Settlement	An act that discharges obligations in respect of funds or securities transfers between two or more parties.

Settlement system	A system used to facilitate the settlement of transfers of funds.
Smartcard	This term is used in CCITT for cards that covered by the patents of Roland Moreno; i.e. a plastic card by the patents of ISO standard dimensions with a chip embedded towards the middle of the left-hand side. It should maybe be noted that a vast majority of such cards in circulation today are not "smart" in the true sense at all, but are simple prepaid cards without a microprocessor. Under this definition, there are three basic types of smartcards. These are prepaid or stored value cards either of the throwaway or reloadable type, simple wired logic cards able to handle multiple functions and microprocessor equipped cards able to perform functions on the information stored in them. The latter contain a CPU for data processing and security functions, RAM for storing interim calculations, ROM for storing programs and operating instructions and either EPROM or EEPROM for storing specific information about the individual card. Smartcards of all three types may be of the contact or contactless variety.
Stored-value card	A prepaid card in which the record of funds can be increased as well as reduced. (See also electronic purse.)
Subscriber Identification Module (SIM)	A specific type of smartcard for GSM systems holding the subscriber's ID number, thus allowing him to call from any GSM device.
Symmetric Cryptosystem	Cryptosystem with a single key for encryption and decryption.

Bibliography

Sources of information used for this study in addition to the information provided by the participating organisations:

- Ctt, October 1998
- Card Forum International, 5-6/97, "Electronic Purses - who will take the lead?"
- ECBS study TR102, March 1997, version 2 "Overview on European electronic purse projects"
- European Card Review Sept/Oct. 98, "Balance of power"

Other Sources

Card Technology, January 2000

Card Technology, November 1999

Card technology, October 1998

Banque & Informatique, November 1999

Le Monde de l'Informatique, 16 April 1999.

Le Monde de l’Informatique, 12 November 99

'The Unmaking of Mondex', ComputerWorld, 12 May 1997

European Central Bank, Report on Electronic Money, August 1998

Financial Times - 29 November 1999

01 Informatique, 10 September 1999

Les Echos, 27 September 1999,

Card Forum International, Nov./Dec. 1999

Leo Van Hove, Free University of Brussels'Proton, the Belgian intersector electronic purse' (http://cfec.vub.ac.be/cfec/leo.htm) (http://cfec.vub.ac.be/cfec/purses.htm)

ACTS-FAIR working paper no 35, 'Electronic Cash and the Innovation Process: A User Paradigm'.

ACTS-FAIR Constructing the European Information Society'

Le Monde, 7 July 1999, 'Le Monde Interactif'

European Committee for Banking Standards (ECBS), Interoperability of European Electronic Purse systems, October 1997

01 Informatique, 10 September 1999Excerpt of a study from De La Rue

Report 'Smart Card 1998' from David Jones and Carolane Mearns

Public Websites (in particular Gemplus' and FIWG's)

ARTTIC s.a., Paris

Related information sources on the WEB