



Centrum voor Wiskunde en Informatica

REPORTRAPPORT

MAS

Modelling, Analysis and Simulation



Modelling, Analysis and Simulation

CAFE project – Final report volume I
Trials and surveys

Edited by R. Carter, C.J. Stanford, A. Weber

REPORT MAS-E0302 FEBRUARY 28, 2003

CWI is the National Research Institute for Mathematics and Computer Science. It is sponsored by the Netherlands Organization for Scientific Research (NWO).

CWI is a founding member of ERCIM, the European Research Consortium for Informatics and Mathematics.

CWI's research has a theme-oriented structure and is grouped into four clusters. Listed below are the names of the clusters and in parentheses their acronyms.

Probability, Networks and Algorithms (PNA)

Software Engineering (SEN)

Modelling, Analysis and Simulation (MAS)

Information Systems (INS)

Copyright © 2001, Stichting Centrum voor Wiskunde en Informatica

P.O. Box 94079, 1090 GB Amsterdam (NL)

Kruislaan 413, 1098 SJ Amsterdam (NL)

Telephone +31 20 592 9333

Telefax +31 20 592 4199

ISSN 1386-3703

CAFE Project – Final Report Volume I

Trials and Surveys

Edited by R. Carter, C.J. Stanford, A. Weber

Published by CWI, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands

ABSTRACT

This is the final public report of the CAFE project (ESPRIT 7023). CAFE developed a secure conditional access architecture and implemented a multi-currency electronic purse system based on smart cards and infrared wallets. The electronic purse was tested in user trials at the European Commission premises in Brussels. Part I of the report covers background surveys, a simplified functional description of the system, and the operation and results of the user trials. Part II describes in detail the security architecture and the technical protocols developed by the project.

2000 Mathematics Subject Classification: 69C30, 69D56, 69E30, 69M34, 69M55

1998 ACM Computing Classification System: C.3.0, D.4.6, E.3.0, K.4.4, K.6.5

Keywords and Phrases: Conditional access, electronic purse, electronic wallet, smart cards, e-commerce, digital cash, consumer payments, multi-currency

Note: Many CAFE project participants contributed to the writing of this report, and it would be impossible to accurately list its authors. The editors listed are those who were involved in the final preparation and editing of the document.



Final report Volume I

Bob Carter	(CardWare)
Chris Stanford	(CardWare)
Arnd Weber	(IFS)

Preface

This report summarises the experiences gained in implementation of the CAFE architecture for secure privacy protecting electronic payments. The CAFE project culminated in a trial of the technology at the premises of the European Commission in Brussels. Indeed the trial of the CAFE technology has subsequently been further extended, by commercial sponsors, to other countries.

It is the final report of the Trials and Surveys workpackage of the CAFE project and the authors acknowledge the work of the following people who have during the project contributed to establishing the requirements for helping in the operation of the most technically advanced payment card demonstration so far in operation.

Gerd Paul, Franco Furger:

Dale Whinnett, Susanne Schaper, Hilde Vandooren:

Gerry Farmer, Ann Vanderborght:

IFS.

trial survey's

trial operations Brussels

The demonstration focused on off-line operation of a multi-currency electronic purse, it should be stressed that this is only one possible way to use the CAFE architecture. Commercial users of CAFE's basic protocols would be able to apply them to most forms of payment instrument or securely signed documents such as drivers licence's, passports and medical data.

Contents

1	Introduction.....	5
2	Background surveys	6
2.1	Summary of the investigation of existing systems.....	6
2.1.1	Market issues	6
2.1.2	Commercial issues.....	7
2.1.3	Economic and legal framework	8
2.1.4	Privacy requirement.....	8
2.1.5	Operational Issues	9
2.1.6	Technical considerations.....	10
2.2	Summary of the survey of experts	11
2.3	Consumer Survey Results	13
2.3.1	Stored Value Cards and Devices	13
2.3.1.1	The Electronic Purse in General.....	14
2.3.1.2	Infrared Handheld Wallets.....	14
2.3.1.3	Differences Between Traditional and Electronic Cash.....	14
2.3.1.4	Specific Characteristics	16
2.3.1.5	Electronic ECU	18
3	Simplified guide to the CAFE protocols	20
3.1	The signature transporting principle	21
3.2	How does the merchant gets paid.....	23
3.3	Summarising the loading and payment cycle for purses	25
4	Demonstration organisation	26
4.1	Commercial constraints.....	26
4.2	User help desk and loading point	26
4.3	Equipment installed in the Beaulieu building.....	27
4.4	Summary of equipment for the Beaulieu building.....	28
4.5	Partners responsible for the provision of equipment	29
4.6	Planned expansion of the demonstration.....	29
4.6.1	Nerviens Building	29
4.6.2	Breydel building	29
4.6.3	Breydel building summary	30
4.7	Project management	30
4.8	User documentation.....	31
4.9	The Exchange logo.....	40
5	Demonstration equipment functionality	41
5.1	Structure of demonstration:	41
5.2	Key technical points of the demonstration:	41
5.3	Scope of trial:	41
5.4	The Consumer Perspective	42
5.4.1	Joining the Scheme and obtaining the cards / wallets.....	42
5.4.2	Loading with value (Withdrawal).....	42
5.4.3	Changing the PIN (Change PIN)	43
5.4.4	Depositing value	43
5.4.5	Reviewing the balance (Show balance).....	43
5.4.6	Spending value at an attended point of sale.....	44
5.4.7	Spending value at vending machines.....	45

5.4.8 Multi-currency operation	45
5.4.9 Fault and loss tolerance.....	47
5.4.10 Leaving the scheme.....	47
5.4.11 Incentive programme.....	47
5.5 The acceptors perspective.....	47
5.5.1 The canteen and coffee shop service provider (DGIX)	48
5.5.2 The vending machine service provider (Sportschuur)	49
5.5.3 Transaction collection.....	50
5.5.4 Multi-currencies and guaranteed exchange rates	51
5.6 The Issuers perspective	51
5.7 The acquirers perspective	52
5.8 The Clearers perspective	52
5.9 The help desk perspective.....	53
5.10 Detail of operations from the consumer perspective.....	55
5.11 Transaction terminal operations from the service providers perspective	60
6 Running the demonstration	61
6.1 Background	61
6.2 System integration.....	61
6.2.1 Technical issues.....	62
6.2.2 System acceptance test specification.....	65
6.3 Initial running	72
6.4 Xchange Card Survey results	73
6.4.1 Present Card Usage	73
6.4.2 Integration Into a Bank Card.....	75
7 Technology cost assessment.....	77
7.1 Assessment of technical achievements against objective	77
7.2 Current and estimated mass production costs.....	78
Appendix 1 Semi-Standardized Questionnaire for the Xchange Card	83

1 Introduction

This volume of the final report of the CAFE project describes the background research and principle findings before outlining in simple terms the CAFE principles. The operation of the CAFE demonstration, from organisational, functional, operational and user view points is then described and finally an assessments of the cost of the technology for potential users is included.

When the CAFE project was first conceived there were no bank issued pre-paid schemes in operation although it was known that several banks were investigating this potential market. One aspect however was very clear, whilst no bank had revealed its pre-pay technology, it was extremely certain that whatever technology was adopted they would not be compatible. Although this attitude was acknowledged, our initial research with central bankers indicated a desire for the emerging pre-pay technology to incorporate a secure architecture for a banker controlled payment system for multi-issuers that would operate across borders.

A framework that not only provides for a national low cost cash alternative, but that can be enhanced to cover legally irrefutable cross border payments of both low and high value as well as include the optional attributes of anonymity, loss tolerance, multi-currency operation and limited transferability, was seen by many to be desirable.

Based on this principle and using the bankers draft analogy CAFE concentrated on developing a highly secure approach for electronic payments. The “signature transporting” principle became the cornerstone of the architecture.

2 Background surveys

During the first year of the project research was carried out to determine the market requirements for advanced payment devices. The surveys were split into three target areas namely, to learn from existing systems, to gain from the opinion of experts in the payment industry and to capture the requirements of the consumer. The results obtained in these surveys are summarised in this section.

2.1 Summary of the investigation of existing systems

The existing systems survey covered a variety of mainly payment related schemes as this was the aspect of the project emphasised in the EC remit for CAFE. There are many innovations in the payment system market place as can be seen from the large number of relatively small schemes covered. However, in order to provide the background into which any innovative device must fit, the major payment schemes, both national and international, were also surveyed.

To assist in the overall analysis of the information gathered this summary covers the major points resulting from those surveyed under the following headings:

- Market issues
- Commercial issues
- Economic and legal framework
- Privacy requirement
- Operational issues
- Technical considerations

2.1.1 Market issues

The major international payment scheme providers have all stated that they are aggressively marketing into Europe. Most are broadening their product range and bringing new products into Europe, significantly the debit cards Maestro and Delta from MasterCard and Visa respectively.

With the move into new products the originally strong brand identity of the major players does raise issues. Visa cards are no longer just credit cards and a particular product (Visa electron for example) may not be accepted at locations displaying the Visa decal. This causes confusion for both merchants and consumers and may cause friction at the POS if a customer payment is refused. Also exemplified by the Lufthansa Airplus card which carries 9 logos, who does the consumer complain to if there is a problem? In general there are many other instances of confusion of brands.

All the major scheme providers state their intention to expand their merchant base, by implication the acquiring of transactions will become more open.

Whereas the major payment scheme providers, with their emphasis for on-line operation have so far concentrated on high value transactions, the market being addressed by many of the new schemes surveyed is the low value purse transaction. Most of the schemes surveyed can be described as closed (one issuer, single or multi-applications) although some are emerging as multi-issuer multi-application national schemes. It is interesting to note the number of non-financial institutions involved in this market.

The pre-pay throw-away-when-empty card brings with it new opportunities for promotional advertising as seen on most telephone cards and taken to extremes in Japan. Indeed pre-pay cards in general create

opportunities for other forms of promotion such as discounts (i.e. pay 5,000 Yen and get 5,700 Yen encoded on the card) or other incentives.

Cross marketing of applications is based on the principle that the development of a card scheme is expensive. If the cards can be used for new functions outside of payment the costs can be shared among a number of commercial organisations. Some of the new card technology applications have concentrated on this route not always successfully, since in the case of card schemes it is not the technology that drives the market. Use of technology to provide new services or reduce the costs of existing services makes sense as highlighted in the transport market where novel variable discount schemes are embedded in the card and in the case of British Gas where the card is used not only as a payment device but also to collect data from consumer's homes.

A narrow market can also be a problem: This was seen in the UBS scheme where consumers were disappointed that the homebanking system could only access one bank, whereas the targeted UBS customers maintain accounts at several banks.

2.1.2 Commercial issues

Pre-pay schemes

The basic business case is to take cash off the streets. Unattended coin operated machines are open to abuse were money is stolen from the machines and the machines left inoperable. The collection of the cash from the machines additionally involves the use of expensive security procedures. Card operations solve these problems and saves the costs of cash collection and repair of damaged equipment. The pre-pay funds generate a positive cash flow and the use of cards usually increases the revenue taken (e.g. France Telecom, customers spend 30% more time per call using cards than coins).

There are two main scenarios based on the type of card used:

Low cost decrementing cards, thrown-away-when-empty.

Higher cost rechargeable "smart" cards

The first scenario is almost exclusively that chosen for closed schemes (like payphones) where there is a high number of outlets and no existing infrastructure of payment terminals available to the consumer to allow them to recharge their cards.

The cards tend to be less secure and the associated risk has to be taken into account by the scheme (normally single issuer / service provider). Offset against this is the low cost of the card, the opportunities for card advertising revenue, the opportunity to accumulate an unused card balance and the complete absence of a clearing system.

The second scenario is that chosen for interoperable schemes where the card is more secure and hence costly. An interoperable system may even encourage larger amounts to be carried on pre-pay cards. Already in Japan and St Moritz cards charged with a value equivalent to ECU 1,000 are being used. Extra security is needed to convince the multiple partners to trust the electronic value. The more expensive cards cannot be thrown away and recharging terminals have to be available conveniently sited for the consumers, add to this the cost of the clearing system and the infrastructure development becomes significant.

For the above, combined banking sector initiatives seem most promising, as in general they have the required infrastructure and merchant network which could be generally available to all.

To encourage greater acceptance of pre-pay transactions by merchants the settlement process for pre-pay should not be slower than cash.

Debit / credit schemes

The use of the smart card has its roots in France where fraud prevention was one of the main reasons for its introduction. Other countries have been slow to adopt the same strategy. Indeed in one case, Norway, the banks decided against the chip card in spite of a successful technical test in Lillestrom: (the cost of the system could not be justified for roll out, especially as the card was used solely as a magnetic card replacement and in use performed one basic function only).

Fraud prevention is now high on the agenda of most European Banks and national / international payment scheme operators. Studies into alternative card authentication and indeed personal verification techniques are underway. Current indications point the way to broader introductions of smart cards for use in the credit/debit card market outside of France, however for the international schemes it must be recognised that a global solution must be established. This may in turn allow local areas, such as Europe, freedom to introduce both the global standard which could be a magnetic solution and a regional solution which could be a smart card.

2.1.3 Economic and legal framework

The question of the liquidity of the issuers of pre-pay cards becomes more important as the services covered and the number of issuers and cards in circulation multiply. Considerable sums can be involved. For example, the Japanese model of depositing 50% of the float balances with the central bank may be adopted by European authorities. Consumers will need the re-assurance that their card is as trustworthy as cash. However this will create a conflict with issuers who view the float as an important part of their business case. Are the cards another type of money in the legal sense? What happens when an issuer leaves a scheme or goes bankrupt? Some form of bond or lifeboat fund might be considered necessary in order to protect the consumer. Do pre-pay cards carry an expiry date, or is the issuer liable for ever? Again no clear consensus has yet been identified.

In many cases, where there is a legal requirement to offer a receipt of purchase (VAT or Reg E in the USA among others) would an electronically stored receipt be acceptable?

2.1.4 Privacy requirement

Whilst most people will accept that an account based debit / credit card scheme is not anonymous, it is a different issue when cash replacement products are considered.

Most schemes surveyed consider that small value transactions should and could be made anonymously. Past history has shown that there can be considerable public backlash against schemes that are considered to be an invasion of privacy for example

In the 1983 Dancard trial, when the Personal Registration Number, which each citizen received from the government, was recorded on the card.

Hong Kong road pricing, with electronic number plates, is reported to have been scrapped because of the privacy issue (Heusch et al. 1991, Financial Times of 27.7.1990).

There is, however, a conflict of requirements within pre-pay card schemes. The issuer wants to be able to protect his system against organised or individual attack from forged cards and dummy terminals, so most build in a means to identify individual or groups of cards. Scheme providers assured us that they would only use this information to block fraudulent cards or transactions and not track an individual customer. Identified examples of where the privacy issues are considered important are:

Some providers of pre-pay card schemes are considering deleting most of the records e.g. Swiss PTT in Biel, transport in Germany and possibly, the French La Poste. This is, at least in part, a result of the perceived privacy issue.

The UK department of transport considers that road pricing schemes should protect the motorists' privacy.

For cellular phones, consumers perceive an invasion of privacy resulting from the use of radio scanners in North America (Beatty 1992). GSM in addition to providing better voice quality, is designed to reduce this threat.

2.1.5 Operational Issues

Usage

Off-line capability for pre-pay card processing is seen as essential for cardholders, card issuers and retailers for small value transactions. It may be that for higher value transactions the cardholder is verified and for extremely high transactions an on-line connection is made.

Where user verification is needed, (recharging a pre-pay card from the user's bank account for example), then if a PIN is used it should be customer-alterable. For small value transactions users find it quite acceptable not to use a PIN (Loughborough, PTT's worldwide).

Usage is said to increase when consumers are given the opportunity to use a signature, in place of a PIN (MasterCard trials, Peek & Cloppenburg [Germany], UK experience). This suggests that some of the biometric techniques which are currently being tested, (e.g. the fingerprint based system at Schiphol airport and the hand geometry approach at Newark and JFK airports in the USA) might be more appropriate in the future.

The man-machine interface for a multi-application card can be very complex. In a number of applications these functions are implemented by using different attributes of the card (i.e. chip, magnetic stripe or indeed embossing). This maybe alright if the application can only use one of the alternatives, but what, if there is a choice (for example a payphone that takes pre-pay off the chip and credit calls off the magstripe). Inevitably different service providers indicate options in different ways. In situations where operator assistance is available (at the POS for example), then the retailer can lead the consumer through the options. Where no assistance is available then the customer interface needs to be explicit and unambiguous, a tall order especially if the user is in a foreign country. There are good examples of ATM's especially in Spain and Switzerland, which display the operating instructions in the language of the cardholder.

Contactless operation is becoming increasingly popular for "people moving" applications. In the extreme case of vehicle to roadside communications (e.g. for tolls and road pricing), it is of course mandatory. Where individuals are making payment then the preferred approach is to adopt close proximity operation, whereby the user has to indicate their commitment to pay by placing the card close to the reader or pressing a button. Using longer range cards for payment raises other issues. Even if a button is provided on the reader, how does another user in the queue know if the funds have not been taken from their card by mistake? Using longer range cards to operate metro barriers after the payment has taken place elsewhere is felt acceptable (e.g. Dutch rail trial).

Initial observations indicate that facilities for customers to check their remaining balance are perceived as useful.

The ability to refund (at least the last transaction), back into an individual's pre-pay purse was mentioned as a requirement in some schemes. It does raise issues as to the security of the system to allow this "undo function". In at least one case the card and transaction have to be matched before the undo can take place. Whether this is practical in a busy shop is debateable; it certainly seems to imply traceability. How long can a busy terminal store all the transactions? As an alternative and certainly after a long time has elapsed, another method of refunding would have to be used, perhaps because there would be two different methods making refunds this would be confusing to the consumer.

2.1.6 Technical considerations

There appears to be no clear policy by card issuers on the refunding of funds on pre-pay cards due to customers moving, equipment malfunctioning, lost or theft of cards. Most suggest that each situation is judged individually on its merits. This issue need not only be confined to the card holder, but can also be important for the merchant accepting the value from pre-pay cards.

It is generally recognised that a pre-pay scheme must have some fall-back mode of operation in the event of network faults or device unreliability. This could be achieved by the use of another attribute of the card (magstripe, embossing ...), or by the sections of the system or the card that may remain active, offering to the cardholder or merchant limited facilities only.

Pre-pay cards should aim to be as reliable as cash. In general, card reliability does not in many cases appear to be as good as should be. It is apparent that the smaller the chip in the card and the longer it has been in production, the more reliable is the finished product.

Manufacturers of existing pre-pay systems rely, at least in part, on having system secrets stored in a tamper resistant way in terminals. The management of these secrets is a complex task and the trend is towards removable Security Access Modules (SAM's), so that at least the logistics of terminal maintenance and replacement are simplified.

Device form factors identified in the survey ranged from ISO sized contact chip cards (the majority after magstripe cards) to a key fob shaped Contactless tag (Ajax, Canada) and watches. Other Contactless cards thicker than ISO have been used in a trial in Helsinki and on the London underground. Obviously by freeing the device from the constraints of a slot (Contactless operation), any shaped object may be constructed as long as the nature and function of the interface is the same.

In general the success of a new system is very dependant on the first impressions. It is therefore imperative that any trial should be thoroughly planned, tested, resourced and proven before launching it

on the public.

2.2 Summary of the survey of experts

International and domestic payment systems are owned and operated by a variety of different organisations, ranging from the vertically integrated to the open membership schemes. The product range offered is diverse and is designed to meet the particular needs of their cardholders. The major card payment schemes are openly seeking to expand their operations within Europe. However, expansion to other market areas such as pre-pay raises important issues:

- How to protect their brands?
- How will they maintain control?
- What new revenue will the service generate?
- Will members be able to co-operate whilst offering competitive products?

The CAFE wallet proposal additionally raises issues such as:

- How will the product be branded?
- Will customers purchase their own wallet?

However, there is general agreement that public key cryptography offers the best solution for the future. The use of an asymmetric key signature provides benefits over existing procedures in that it allows the key management issue to be simplified, enhances the scheme security and would ensure that cross border pre-pay payments become a feasibility.

To ensure backwards compatibility with existing smart card schemes it was agreed that the CAFE device contains the ability to interface with or contains a "generic" smart card. It was also recognised that to achieve the CAFE objectives it would be necessary for the device to contain all existing card payment functions.

Existing debit and credit payment cards remain the property of the issuer at all times. However, if a device was obtained by the purchaser: Who would own the card? Would the card issuer still retain ownership or would the card issuer only own the applications they had securely placed within the wallet? If ownership was split, who would be responsible for the transactions?
Will payments be anonymous, will loss tolerance be offered?

Will asymmetric signatures achieve legal status as reported from Sweden and USA? Will a verification system be incorporated within the card?

Additionally, operators of the payment schemes are concerned about the financial benefits that a pre-pay product can generate. Whilst it has to date proved difficult to discover the exact cost of cash, it is estimated that the cost of handling cash for a merchant is in the range 3% to 5% of face value. The business case for a pre-pay product can therefore capitalise on the potential savings in overheads.

It is recognised that the CAFE device can offer other services apart from the pre-pay market. VAT payments for foreign travellers do present a problem. It has been suggested that a CAFE type concept could be introduced to allow visitors to either avoid the domestic payment of VAT, or use the device to reclaim the VAT paid as they leave a country.

However, there are other issues. Can the device comply with international standards? Here members of the CAFE consortium have been working with success to ensure that the use of public key cryptography is included on the work schedules. The physical characteristics of the interface are also important.

Whilst the payment system experts appear to find favour with the CAFE concept, the real success will only follow if the products receive the support of the buying public.

A major area of interest has therefore centred on seeking the views of consumer representatives. Not unsurprisingly they have expressed strong views.

In general they do not like the idea of a cashless society. However there is a strong view that consumers be given a choice of payment options. Cash is perceived as providing value. Payment by card is not perceived in the same light. A card payment is not as real and hence can lead to overspending. Overspending by card is seen to be a real fear. This is certainly true for a certain percentage of the population with conventional payment cards. However, with a pre-pay option, this danger would be removed as card holders would only be able to spend what they had pre-loaded.

When moving to payment by card it was conceived that there should be little change in the operating procedures for the consumers. For example, if a receipt was currently expected, then paying with the CAFE device would not change this procedure. However, if the CAFE device could contain the receipt in an electronically readable form and was legally acceptable, then this option should be given. Consumer representatives like the option of being able to check how much value remains within the device. Again this option has to be provided.

The privacy issue needs to be addressed. Whilst in general pre-pay transactions will be anonymous, there may be occasions when scheme operators will wish to trace transactions for marketing or security reasons. The consumer will need the re-assurance that if a product is sold as being anonymous, that this is true.

Consumers were also concerned that by using a card in place of cash they would be expected to pay for the privilege. Costs involved in transferring items between countries have been perceived as high. Consumers would not like the same scenario to occur with a pre-pay device.

It was also expected that a pre-pay product must be universally acceptable. If the intention is to replace cash, which can be accepted almost everywhere, then the CAFE device should aim to achieve the same status. This, however, raises issues on the trust placed in a cash replacement scheme. Will the issuer always honour transactions? What happens in the event of bankruptcy of an issuer?

Whilst it was acknowledged that pre-pay cards like cash can be lost or stolen, experts believed that card holders should be given the opportunity to advise the scheme provider when this occurs.

Consumer representatives also expressed the view that there should be a facility to cancel a transaction. This option, however, would have to comply with certain procedural rules and in general could only occur at the time the mistake was noticed.

Verification of the card holder is seen as important. The existing pre-pay schemes for low value transactions generally do not require any form of verification other than possession of the device. However, should higher value transactions be contemplated, then card holder verification is important.

The PIN was viewed by the experts as being particularly weak as it offered no real proof that the genuine user had entered the number. A biometric option was considered as the best possible alternative.

Biometrics have reached a level of maturity; however, very few are in commercial usage. The options being seriously considered by the payment systems include fingerprint and signature. It would be possible to include a suitable biometric within the CAFE device, either contained totally on the device, or as a carrier for the biometric template. Should the device be telephone based the voice biometric would offer a natural and easily integrated solution.

Main points

- The consumers are becoming accustomed to paying by card.
- The proposed technology to provide secure devices and secure transfer is realisable.
- The ability to automatically verify an individual is reaching maturity.
- The expert views would suggest that the market is seeking a solution for open pre-pay.
- Any pre-pay device should be capable of cross border operation.
- The architecture must allow for multi-issuers to securely co-exist.
- The pre-pay card market is viewed as the next major market to be tackled by the banks.
- Universality of usage is important for pre-pay products.

2.3 Consumer Survey Results

We were interested in how existing prepaid cards are viewed and used and asked debit and credit card users their opinions about a hypothetical electronic purse. We wanted to learn about characteristics, risks, and usages of other means of payment such as credit and debit cards, and about money handling in general. We interviewed more than 300 consumers from all over Europe. We focused on users of existing chip card payment systems including the French Carte Bleue system, the Italian Carta Moneta and the Swiss PTT's Postcard Biel. The latter is not only a debit card, but also a prepaid card. With regard to prepaid cards, we interviewed users of the Dallington Country Club. We also interviewed users of the Lufthansa AirPlus travel cards, a multifunctional card that can be used with different service providers. It also offers an optional chip for telephone use. Many users of the above mentioned cards also owned other payment cards such as Visa, MasterCard, Eurocheque, Switch, Connect, or telephone cards, such as the prepay or postpay cards used in the different European countries.

2.3.1 Stored Value Cards and Devices

In our consumer surveys we showed those we interviewed prototypes, discussing the future activities our concept makes possible. It should be kept in mind that we interviewed frequent card users, not the general public. We expected frequent card users to readily imagine consequences of our approach and to be able to detect problematic areas. We also expected them to be the first ones to use these new devices. With this approach we discovered a number of challenges. Before we discuss these, we present the general feedback to our approach.

2.3.1.1 The Electronic Purse in General

Among card users, the general acceptance of an electronic purse was encouraging. Approximately six of ten would use it for daily shopping and in vending machines. Frequent travellers might even be inclined to stop using cash altogether.

2.3.1.2 Infrared Handheld Wallets

Our surveys of the new devices were done with the help of a simulation and with mockups of the devices. We suggested that the devices can be reloaded with value at home at some special phone or home-ATM. We had even more positive feedback on the infrared handheld wallets than on the purse. Nine of the ten respondents said they would like to use such a device. Two-thirds were prepared to pay ECU 15 to 100 for such devices, which can cover the cost of manufacturing them. Spontaneous responses were quite encouraging:

E.g. in the UK: "That's quite snazzy".

For some of the French it was an expression of "modernisme" and they expressed "enthousiasme".

Or a German lady: "Wenn ich so ein Superding in der Hand habe, würde ich es natürlich vielseitig einsetzen."

Another respondent: "It's obvious that something like this is going to come eventually."

A German businessman: "Could be something like a Swatch, the latest trend to have."

A Finnish frequent traveller: "That's the future, this kind of thing."

Consumers liked the secure feeling of not having to give their wallets to someone else such as a store clerk, for example. They also liked to enter their PIN in their handheld device and would like to be able to reload the wallet at home.

We identified two groups of users: those who would like a prepay and postpay facility, and those who want only the prepay facility. Among the first group are those we called the *sophisticated credit users* above. This group is willing to pay ECU 25 to 100 for a device with prepay and postpay facilities and a keyboard. The second group, who want to *know where they stand*, prefer the prepay approach. They would like upper amounts for loading in the range of ECU 200 to ECU 1,500, or have no limit at all. They are prepared to pay around ECU 15 for such a device.

Of course, such devices would only be used if they work perfectly and if there is a sufficient number of terminals. These are issues which should be solvable. Nevertheless, two of the ten would prefer their standard postpay card. From accompanying comments, we would judge that they would like to avoid the risks of a new technical system (risk of non-functioning, insufficient availability of terminals). What is a bit more difficult to solve is that a large minority of men had problems concerning how they should carry it on their person. Accordingly, it should either have a very compact shape or be very thin so that it could easily go into a wallet or a shirt pocket. The thickness of a standard PCMCIA-card might be the upper limit (3 to 4 mm). So the question is not whether wallets are feasible, it rather is how thin they can be made. Judging from the consumer remarks, the most appropriate size and layout of a wallet would be credit card outline.

Other consumers remarked that as long as such devices do not really replace a wallet of today, we should not call them wallets.

2.3.1.3 Differences Between Traditional and Electronic Cash

In order to learn what exactly our research paradigm of building an electronic equivalent of cash means, and in order to detect limits or problems of our approach, we asked respondents if they regarded

existing cash, and electronic cash in stored value cards, as equivalent. We asked both users of prepaid cards and users of other cards. To the latter, we explained how such an “electronic purse” would work. We found differences between traditional cash and value in prepaid cards in the following areas:

1) Gifts and Tips

Respondents mentioned situations in which they use the physical tangibility of cash in order to hand money personally to someone else, e.g. as a gift, as charity, or as a tip. It was believed that this could not be done with prepaid cards. Only under rare circumstances would it be possible to hand over a whole card, as is done in Japan.

With regard to tips, it is important for waiters, for example, to have some means to supplement low pay. It is not certain that procedures such as rounding up the bill, or leaving some coins on the table will occur when cards are used.

Gifts and tips can relatively easily be made if you can transfer value from one device to another person's device in a simple way. This does not mean that all gifts and tips will be made with electronic means in the future. Habits might be against it, and the tangibility of cash is lacking. Still, transferability would ease the situation. In our consumer surveys transferability also occurred in other areas as in the issue of:

2) Other Person-to-Person Payments

Other person-to-person payments (as opposed to person-to-merchant payments) for which only cash was regarded appropriate, were payments to children, friends, colleagues, or neighbours. Retailers also mentioned that they would like to pay another merchant. Again, electronic cash transferability might be a solution: if it were technically feasible or secure enough.

3) Cash for Small Sums

Situations mentioned were also those of paying small sums, e.g. for “une baguette” or “ein Glas Bier”. Whereas some consumers may get used to paying such amounts with cards in the future, others apparently viewed these as old, robust habits.

4) Cash as a Tradition

Some insisted that not everything be computerised. Habits were viewed as important components of an individual's way of life. An attempt to modify or replace them by more “efficient” means was perceived as an unacceptable intrusion in the private lives of individuals. Therefore, it must be expected that not all cash transactions can be substituted in the future.

5) Cash as a Tangible and Visible Form of Money

Respondents stated that only cash can be touched and seen easily. The importance of the physical character was shown by an English worker (the U.K. being a country in which it was common until recently to have wages paid in cash):

“I don't think there's anything better than on a Friday afternoon, get a big wage and sticking it in your wallet as it makes you feel good.”

Respondents also mentioned that only with cash is it possible for a child to learn about the value of money. Accordingly, handheld readers that display balances might be of help, but will probably not be fully equivalent to the look and feel or the symbolic meaning of cash.

6) Cash in Deals With Unknown Partners

Bank notes are the only trusted method of payment in certain situations such as the selling of a car to a stranger. In the long run, a perception of security might evolve which attributes the same feeling of security to electronic cash, but this perception probably will not be present immediately.

7) Briberies

Some businessmen we interviewed mentioned briberies as a strong case for cash. Briberies (or the black market) are perhaps not a very respectable reason to introduce privacy. If electronic cash will indeed be untraceable, then it may replace cash in black markets. If not, existing cash will continue to be used for briberies or black market payments.

2.3.1.4 Specific Characteristics

So far, we have been discussing the differences that the respondents saw between existing cash and electronic cash. We will now discuss some of these issues in more detail and make a proposal for the characteristics a payment architecture should provide.

Transferability

General transferability of funds may be required if an issuer intends to replace cash completely. It is not necessary to have this type of transferability if one thinks of payment situations such as in supermarkets, or with vending machines. General transferability makes it difficult, however, to monitor the system's security. With blind signatures for transferable money, memory requirements increase. Therefore, we decided not to implement general transferability in the basic protocols designed so far. What we actually added can be called "limited transferability". Money can be transferred from a wallet to, for example, a child's card belonging to the same account. It could also be considered to give a retailer the possibility to make a traceable payment to another retailer who then gives the money back to the bank. Thus, limited transferability could fulfil a number of needs. Full transferability can be reconsidered in the future.

Privacy

The enhanced form of asymmetric digital signature, developed by the CAFE team, allows transactions to be anonymous. This important feature gives both the user and service provider the option to offer total privacy for money transfers when required. For instance, government transportation departments, in many parts of the world, are mandating that electronic road pricing schemes be able to accept a form of payment that makes it impossible to track a user's movements through his payment history. Cash is anonymous, therefore, for an electronic equivalent to have any chance of major success in the market place, it has to retain this characteristic. We asked our respondents if they believe privacy, such as with coins, to be important. Our question was:

Personal data arising from card transactions is currently stored in data banks. With our system this

would no longer be the case. You would have so-called electronic coins and bills in your purse. Would it be important for you that electronic transactions be kept anonymous, just as cash transactions are now?

Half of the respondents found it important or even very important. It should be noted that our respondents were frequent users of postpay cards and thus often pass their identity at the point of sale. Some were not interested in something like anonymous electronic coins because they felt that they would then have less means to solve errors or disputes. Their problem can, of course, be solved by providing both electronic money and undeniable receipts, as with cash payments now. In order to make clear to the reader what the respondents' remarks were, examples are shown in the box below.

Germans emphasised the importance of privacy the most. Around one-fourth to one-third of all card users interviewed were even willing to pay ECU 10 to 25 annually for privacy. This is interesting, as the annual cost of a cryptographic co-processor used for blinding the signatures are far below these amounts. Some French, who were not willing to pay for privacy, were not indifferent toward the privacy issue. On the contrary, they considered privacy a service that must be included in the basic price of the Carte Bleue. The French respondents often argued in political terms. Privacy was considered an individual right that should be enforced by the state.

Privacy As With Coins	
Austrian man, aged 28:	“Geht niemanden was an, soll schließlich Bargeld ersetzen.”
German man, aged 36:	“Monetäre Angelegenheiten sind primär Privatangelegenheiten.”
German woman, aged 27:	“Weil ich entscheiden will, wer wann was von mir erfährt.”
British man, aged 42:	“to minimize ‘Big Brother’s’ surveillance of my expenditures”
British woman, aged 46:	“It is my business how I spend my money, which organizations I support, etc.”
French man, aged 37:	“Confidentialité”
French man, aged 23:	“Liberté personelle”
Swiss woman, aged 25:	“Persönlichkeitsschutz”
US-American woman, aged 37:	“I feel entitled to the option of being anonymous when I choose to be.”
Italian man, aged 32:	“Tutela della privacy”

Even when the privacy option is implemented, the CAFE system can, if required by the user, trace previous transactions. This option can be offered as a service to the user who finds himself in dispute over a transaction with a particular merchant. With appropriate receipts, paper receipts of today, or electronic receipts in the future, it is possible to maintain a personal relationship with the salesperson or waiter. Identification is also required when one reloads one's wallet with money from one's bank account.

Postpay Function

An additional postpay function on a card, or preferably, on a wallet, would give users a means to pay unexpected or larger sums; in other words they have access to their account without carrying all their money around. It may happen, however, that consumers insist that the postpay function be used, while the retailer or the issuer may prefer the prepay function. In any case, we feel that if you want to attract most of today's card users, there is no way around a postpay function.

Loss Tolerance

According to our respondents, protection against loss and theft is one of the main advantages of existing cards as compared to cash. We learned that protection is even expected when consumers see a bank or credit card logo on a device. Therefore, we decided to build into our system a loss tolerance scheme, as described above. In case of a loss one easily gets one's money back. In case of theft, however, the thief can spend the money. Therefore it is required that the value can either be blocked by using a PIN, or, in the future, by biometric verification of the owner. Thus, one could have a flexible electronic equivalent of a traveller's cheque.

A practical implication of loss tolerance is that it insures the security of relatively high amounts of money in one's device. In other words, one could have one's bank account in one's pocket. Another implication of running a loss tolerance scheme is that it offers a perfect audit trail to handle disputes about non-functioning devices, broken chips, etc.

Some issuers might be reluctant, at first, to offer loss tolerance because it requires processing all transactions. However, it must be emphasised that this can take place off-line in batches. In the future, with the shrinking cost of telecommunication, more issuers might be willing to process all transactions.

2.3.1.5 Electronic ECU

When undertaking our original consumer research in 1993 we included the concept of the electronic ECU (European Currency Unit). The reason for doing so is as follows:

Pre-paid card scheme operators, in most European countries, are currently developing an infrastructure of systems and terminal equipment, capable of handling electronic money. The introduction of a pan European electronic currency could capitalize on these developments. Appropriate encouragement from the European Union can ensure that new and existing systems have "gateways" prepared for the electronic ECU.

By considering the ECU as an "alternative" currency for Europe, consumer acceptance can at first be encouraged for EU cross border payment applications. The numbers of low value, cross border payments are predicted to rise sharply during the next few years. Additional convenience for both consumer and retailer (understandable and simplified currency exchange rates) makes the alternative currency initially attractive, and avoids a direct confrontation with national currencies.

Introducing the ECU as an "electronic only currency" could avoid the high initial start up costs associated with the minting of coins and the printing of banknotes and the distribution of these to more than 300 million people. There would still be the costs associated with setting up and running additional ECU bank accounts, but this would also be the case if new notes and coins were issued.

As an “electronic only currency” the ECU would never have to bear any of the on-going costs associated with notes and coinage and would thus, always have the advantage over other national currencies, even if they migrated towards electronic versions. The same long-term advantage applies to the use of the electronic ECU outside of the EU, thereby creating a strong, worldwide influence. During the change over period the electronic ECU could play a role in easing the national sensitivities that will arise when existing currencies are replaced.

Therefore, we added questions on the ECU in our surveys:

Imagine that throughout Europe a unified currency were implemented in electronic form. You would, so to speak, have ECU in your card. Would you use it?

Electronic ECU	
Would you use it? (use it ... not use it; scale 5 to 1)	
166 of 245 ticked “5” or “4” (48 ticked “3”, 31 ticked “2” or “1”)	
British man, aged 35:	“Would make life easier for all of us.”
British man, aged 26:	“... wouldn't have to think about exchange rates in Europe.”
Australian woman, aged 25:	“If value of ECU known by everyone, less money would be lost on converting money.”
French woman, aged 19:	“Pratique et européen”
French woman, aged 23:	“Monnaie unique simple”
French man, aged 36 :	“Facilité, simplicité”
Swiss man, aged 31:	“Nur eine Währung... kein Geldumtausch mehr... keine Rechenprobleme mehr.”
Swiss woman, aged 25:	“Herumreisen ohne viele Währungen möglich.”
Austrian man, aged 28:	“Kein Umtausch mehr, Vereinfachung der Zahlungsmodalitäten.”
German man, aged 39:	“Große Vereinfachung bei den häufigen Auslandsreisen.”
German woman, aged 24:	“Es kommt drauf an, was akzeptiert wird. Solange es DM gibt mit DM zahlen, weil Abrechnung einfacher, und im Ausland mit ECU.”
Italian woman, aged 28:	“Mi sentirei più europea. È un passo avanti verso soluzioni tecnologiche più sofisticate.”
Italian man, aged 29:	“Praticità”

A majority of card users said they would use it because they expect the electronic ECU to be simpler, more transparent, and cheaper than the existing means of transborder payments, as our box shows. Frequent travellers and persons living in border regions were, of course, particularly interested in the improvements they expect. The French were also quite enthusiastic. The UK regarded it as inevitable. There were a few Germans who disliked the proposal for political and economic reasons. In general, we were surprised by the positive feedback as in the months before we conducted our survey (in late 1993), there were many political discussions and some referendums in Europe concerning the Maastricht treaty, some of which revealed critical attitudes towards certain European unification issues. Apparently, people respond positively when they think about the advantages and benefits the system would bring to them personally.

3 Simplified guide to the CAFE protocols

Security of any pre-pay instrument is always a big issue, but in attempting to provide a platform that can be accepted in many countries by many different service providers it assumes an even higher profile. Most of the experts interviewed agree that the technical approach put forward by the CAFE project in the use of asymmetric cryptography to digitally sign electronic money is the best way to achieve these desired objectives.



**Universal unforgeable instrument
used as the basis for electronic money**

The instrument is an electronic "form" for carrying all types of value transfer instruction signed and guaranteed by a financial institution.

The method of payment uses the same instrument filled in different ways and can be:

Pre-pay	(Cash)
Pay now	(Debit)
Pay later	(Credit)

One instrument many forms of money.

The CAFE architecture gives the flexibility to incorporate many forms of money within one simple set of protocols. There are huge potential benefits to the issuers and service providers in the use of one infrastructure that has the ability to accept a range of payment instruments based on a common open architecture. The user benefits by being able to carry all the necessary capability for each type of payment method within one device

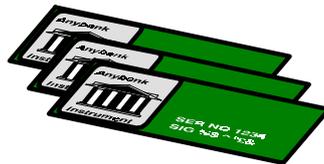
The following series of figures is intended to highlight the main features of a signature transporting pre-paid instrument on a step by step journey around the payment cycle from loading to clearing

3.1 The signature transporting principle

Electronic cheques are issued by the bank and signed by using secret keys that only the bank knows with a digital signature that has the property of remaining valid when the cheque is filled out at the point of payment. Acceptors of the cheque can authenticate the cheque is genuine by using the public key of the issuing bank. Knowledge of the banks public key does not give away any information about the secret key used by the bank and does not need to be kept secret in the accepting terminal. Indeed the public key of the bank can, if certified by a scheme key, be presented to the point of payment along with the cheque. By this means cheques from any issuer who is a member of the scheme can be authenticated by any point of payment operated within the scheme without prior knowledge of the issuers public key. The use of public key digital signatures and the dynamic system of key distribution produces a scheme that is open, highly secure, simple to manage and does not require the use of special tamper resistant hardware in the point of payment terminal.

The signature transporting principle *the basic instrument*

The electronic Cheque blank



Each electronic cheque has:

- An expiry date
- Can be filled out up to a maximum value
- Carries the issuers "unforgeable" digital signature

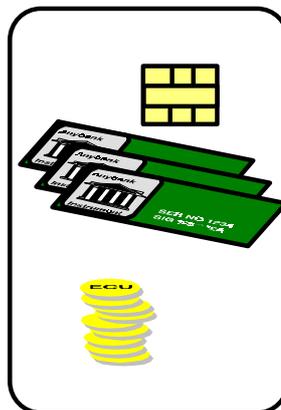
All of which are generated and set by the issuing bank

The digital signature uses asymmetric cryptography so that the bank does not have to share its secrets with anyone else

At this stage the cheques hold no value

The bank generates blank cheques using their secret key, each cheque contains a unique serial number. If the user has chosen unconditional anonymity the cheques can be "blinded" in such a way that the issuing bank cannot relate a given cheque to its user unless the user chooses to reveal a secret! Value is also loaded into the purse. The value is held as part of a cryptographically protected table of values which may contain any number of currencies, in the current implementation the table can hold up to five. It is worth stressing here that the value and the cheques are separate entities and you cannot make a transaction unless you have both.

The signature transporting principle *loading the purse*



The issuing bank loads the purse with a number of certified "cheque blanks"

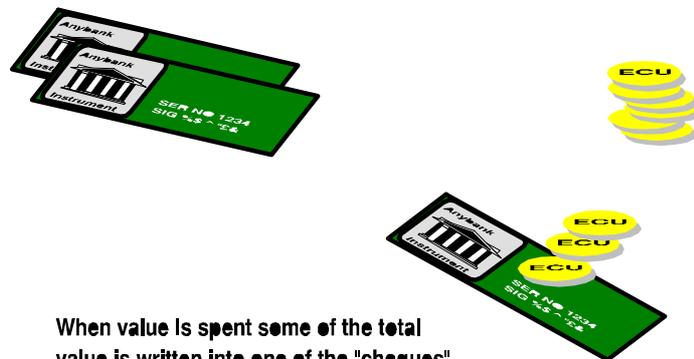
It also loads the purse with a value paid for by the user

A challenge / response: card / terminal authentication mechanism ensures that value transfer messages are always unique and the card is genuine.

Transaction information from the merchants terminal along with the date and the merchant identity is written into the cheque blank by the card¹. Value can also be written into a single cheque in small increments or "ticks" this is particularly important when the purse is used with payphones, using one cheque for each unit of a phone call would be extremely inefficient.

Also as cheques are made out in favour of the merchant they cannot be "cashed" by anyone else.

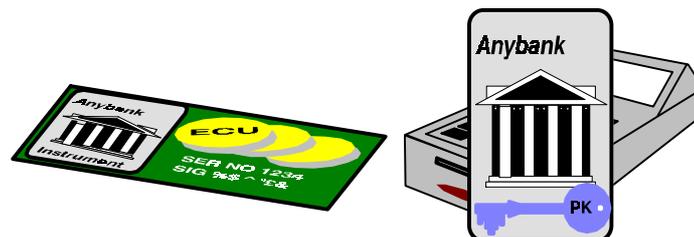
The signature transporting principle *spending value*



When value is spent some of the total value is written into one of the "cheques" which is then passed to the merchant

Merchant terminals need the ability to authenticate the cheque being used for payment. In order to do this the terminal uses the public key of the issuing bank and computes the validity of the banks signature on the cheque. Should this prove correct then the merchant can be guaranteed payment by the issuer.

The signature transporting principle *authentication by merchant*



By using the public key of the issuing bank to check its digital signature

The merchant terminal can verify if the presented cheque is authentic

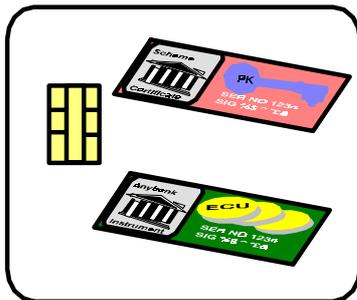
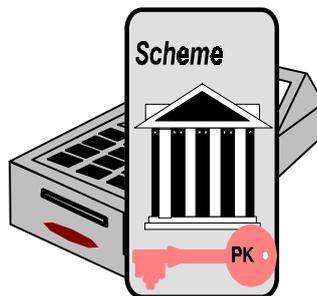
How does the merchant obtain the public key (PKb) of the bank? It can either be sent to the terminal from the acquirer (a reliable source) or be presented to the terminal by the purse itself.

¹ Every card uses its own key to encrypt balances and write information into cheques in such a way that even if a single card could be compromised others are still safe.

The PKb must be known to be the genuine key for that particular bank, just in case someone makes up a pair of keys (secret and public) and creates their own cheques! Since the key is public a directory of keys can be held in the terminal for reference, the process of keeping this directory up to date, especially when keys expire or are changed, is complex. Also if banks from all over the world are to be accepted the directory will be very large. If the purse carries the key we simplify management of terminal key distribution significantly but how do we know the PKb presented by the purse really belongs to the issuing bank claiming it? The way to ensure this can be verified by a terminal that may have never seen cheques from this bank before is to certify the banks PKb with a digital signature from

The signature transporting principle *key certification*

If the purse brings the key how does the merchant terminal know the banks



The banks public key is certified by a scheme provider (Europay, Mastercard or Visa for example) and can be checked prior to use by the scheme public key

a higher "authority". The terminal would hold the public key of this "authority" and verify the certificate accordingly before accepting PKb. In this scenario a hierarchy of authorities is envisaged

For example the terminal may carry an international Public Key, which is used to certify a national Public Key, which is used to certify a regional Public Key, which finally certifies PKb. In this case 3 levels of certification are needed if a terminal only knows the international Public Key. This process presents an overhead on the transaction process, each certificate checked requires Public Key verification computations. In practice the terminal can

accumulate commonly used keys and avoid, in the majority of cases, the full process. Again the commercial arrangements made for the acquiring process may reduce the requirement to only two levels as illustrated in the diagram opposite.

3.2 How does the merchant gets paid.

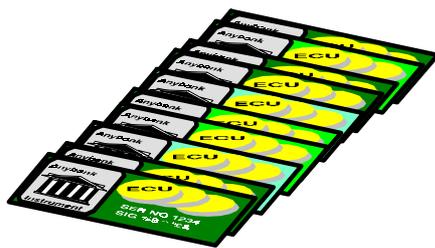
At this point it is stressed that the CAFE architecture is a technology that can be applied by payment schemes and not a payment scheme in its own right. There have been a number of erroneous reports that CAFE is a payment scheme, it is not and never will be! The CAFE architecture is open to all who wish to use it in their own schemes.

Acquiring

The signature transporting principle *acquirer options summary*

Acquirers may collect

individual transactions or aggregated totals per issuer



 = 300 ECU
 = 550 ECU
 = 1,325 ECU

The exact choice may be determined by a combination of the economics of comms, transaction processing, possible

Once the cheques have been collected by the merchant terminal how should they be presented for acquiring? There are a number of options that may be used.

Firstly store every cheque and forward this when needed to the acquirer.

Secondly accumulate the cheques presented per issuer then forward the total to the acquirer.

Alternatively store every cheque and the accumulated totals per issuer but only forward the totals to the acquirer unless a request is made for the complete file of cheques.

Each method has its own merits. Depending on the cost benefit analysis of the risk exposure the acquirer may choose the most appropriate method. For example where communication is low cost, collecting all cheques may be a viable option (most current electronic purse schemes collect individual transactions). Where communications costs are prohibitive then collecting aggregated totals may be the only option, the issuer has the choice! Currently communications costs tend to be reducing, what is too expensive today may be cost effective tomorrow. Flexibility to operate either way leaves the issuer in control.

There are other issues to consider. If totals per issuer are aggregated, without a complete trail of all transactions, then the, detection of double spending if the system is hacked or the operation of card fault and loss tolerant systems, becomes impractical.

Issuers can evaluate the services they wish to offer in conjunction with the risk exposure, in a given area or business sector and set the rules for aggregation or not. For example for customers who pay for recovery of their unspent value in the event of lost or stolen purses all their transactions will be collected individually. Other customers transactions may be aggregated.

Alternatively where the issuer thinks that there is a higher than normal security risk all transactions may be collected, otherwise aggregation may take place.

Verification of cheques

Each merchant terminal can verify whether a cheque is genuine or not and this should be sufficient for issuers to guarantee payment when the cheques are presented. The acquirers and issuing banks also

need to be sure that the cheques presented to them are:

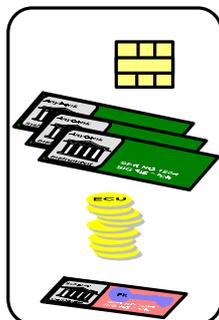
- * issued by them and valid forgery detection
- * have not been presented for payment before merchant malpractice detection
- * have not been used twice by card holders hacked or cloned card detection

Prior to the settlement of value the above control checks are made and conveniently can form part of the overall clearing and settlement process. For example where an acquirer is also an issuer then they can carry out all the above checks on their own transactions themselves and pass any "not on us" transactions through a clearing function to the appropriate issuing bank.

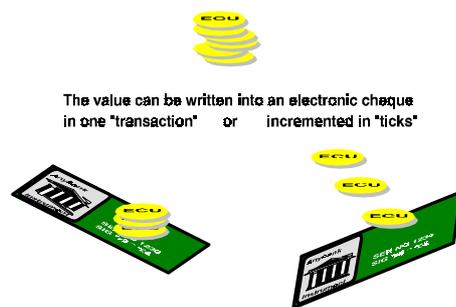
3.3 Summarising the loading and payment cycle for purses

- * value and cheques signed by the issuing bank are loaded into the purse
- * cheques are drawn with value from the purse at the point of payment and passed to the merchant
- * the merchant can, without a secure terminal, authenticate cheques from any bank
- * purses can hold many different currencies
- * key distribution may be, direct from acquirers, or from the issuer via the purse
- * maximum protection against systemic risk

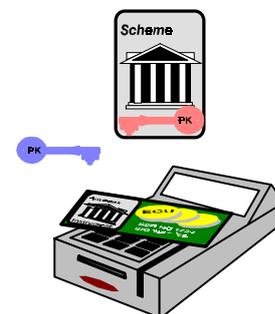
A purse is loaded with cheques value and the certified public key of the issuing bank



Value is written into the cheque by merchant terminal and card together



The merchant terminal authenticates the cheque using the banks public key which itself is verified using the scheme key, then stores the cheque for later deposit



4 Demonstration organisation

The objective of the ongoing demonstration was to validate a multi-currency interoperable pre-payment scheme initially using cards and later using electronic wallets, for use by CEC staff at the canteens, coffee shops, vending machines in premises of the EC / EU

The CAFE project team installed and supported a small demonstration of cards and wallets within the commission building at Beaulieu in Brussels. This first demonstration uses the CAFE architecture to implement a pre-paid financial application in the staff canteen(s), coffee shop(s) and vending machines. Staff are able to pay for food and drink using "smart" cards and electronic wallets that use a new "point and pay" principle. The cards and wallets may be loaded with more than one currency and in this demonstration the ECU in addition to the customers local currency is used. It is possible to load value onto the card or wallet in return for cash.

4.1 Commercial constraints

The EC officially advised the E.M.I. of the scheme and confirmed that the demonstration would comply with E.M.I. recommendations. This means that after the initial proving period where for convenience the card issuer was the European Commission Restaurant Economat a bank will become the issuer. The Commercial Bank of Greece have agreed to take on this role as the trial proceeds.

Settlement is required on transaction day plus one. This is achieved by opening the float account at the same Bank and branch that maintains the EC canteen account.

Participation to users and operators in the demonstration is free.

Loyalty incentives are to be encouraged, by the Commercial Bank of Greece.

Vending machines are operated by a separate company. Initially CAFE would be required to settle direct with this company for purchases passing a copy of the payment advice to EC.

The user "application form" has been kept as simple as possible, only calling for a name, possibly staff number and internal address:

4.2 User help desk and loading point.

The ideal location for the loading station and help desk proved to be in the main foyer of the Building. Adequate security is available and power and communication links were installed. It was also felt unnecessary for the loading station to be operational all day and it was decided that between 10.00 - 2.00 would be adequate. During promotional periods the station would stay open for longer, but in the longer term it was felt that only one reload station would be necessary.

The CEC agreed to make available support resource for the manning and operation of the help desk and loading station.

4.3 Equipment installed in the Beaulieu building

The following equipment highlighted in italics was supplied by the CAFE project for the Beaulieu building.

In the Coffee Shop Operated by CEC

One Financial Transaction terminal (FTT) interfaced to a Fuji cash register

In the Staff Canteen Operated by CEC

Two FTT's interfaced to Fuji cash registers and connected via the internal telephone system to the site service host

For the Vending Machines Operated by Sportschuur

1 Hot	SEEA/Model ZC6	France 372 51818
1 Snacks	Snackmart III 4000	Model 3022

Three Vending machine interfaces (VMI) interfaced to the above machines.

The site service host

The site service host computer is part of the operational control centre for the CAFE demonstration intended for any of the largest sites. Operated by dedicated staff it is used for control of the distribution and collection of cards, creation of issuers value and the signature transporting cheques and collection of transactions at sites taking part in the demonstration.

The site service host replicates the functions of a card issuer and acquirer and provides access to the user and merchant data bases used for reconciliation and in support of "Help desk" enquiries. Its main functions can be categorised as follows:

- * Personalisation and distribution of cards and wallets
- * Collect transactions from local POS and vending machines
- * Control of re-loading station, reviewing device and issuing CAE value
- * Act as workstation for clearing centre and help desk.
- * In addition and for trial purposes only a user data base of remaining card balances is also maintained.

The Re-loading station

The re-load station is the user interface for loading and re-loading user cards and wallets with CAFE value and spendable cheques. In the demonstration CAFE value is created in the site service host and paid for in cash or cheque, by the user. In the early stages of the demonstration the EC is considered to be an Issuer and thus the float for the CAFE value is held by them. The reload facility was operated on

behalf of the Issuer by the CAFE project and a commercial agreement was produced to this effect. The re-loading of user devices is (initially at least) manually assisted, the CAFE RLS is connected to the site service host.

Hand held device (HHD)

Since the vending machines are not connected on-line to the site service host the hand held device (in fact a notepad computer) allows information to be transferred manually between vending machines and the site service host.

The clearing computer

The clearing computer (CC) processes all the transaction information and initiates the transfer of funds from Issuer to service provider.

The CC receives the transaction data acquired by any SSH on a regular basis, it checks the validity of the transactions and updates the data base of CAFE value issued. By this means the centre is able to detect any double spending of value (i.e. breaking of the tamper resistance in the card) as well as implement the fault tolerance and lost value recovery schemes. The CC maintains a data base of issuers, and service providers as well as the location of all terminals in the system.

Cards

The CAFE project supplied all the employees that volunteered to take part in the early stages of the demonstration with cards.

Much more significant quantities (>2,000) of cards are anticipated for use once the Commercial Bank of Greece takes over the role of Issuer.

Wallets

Only a small number of two button wallets are currently available for limited use in the demonstration.

4.4 Summary of equipment for the Beaulieu building

	Clearing computer (CC)	Site host (SSH)	Reload station (RLS)	Hand held device	Transaction term (FTT)	Vending interfaces (VMI)	wallets	Cards
Coffee Shop					1			
Canteen					3			
Vending						2		
Help desk	1	1	1	1				
Total	1	1	1	1	4	2	25	400

4.5 Partners responsible for the provision of equipment

As a matter of record the following partners were responsible for the development of the equipment provide for the demonstration

ITEM	Responsible partner
Financial transaction terminals	Ingenico
Vending machine interfaces	Digicash
Reload stations	SEPT
Hand held devices	Digicash
Site service hosts	SEPT
Clearing Computer	SEPT
Cards	Gemplus
Two button Wallets	Gemplus
Full Wallets	Gemplus

4.6 Planned expansion of the demonstration

Continuation of the operation at Beaulieu and expansion of the demonstration site to further buildings is planned under a separate initiative run by the Open Payment European Research Association. This association (OPERA) is made up of five major banking organisations who intend to use the CAFE architecture in trials of their own and have also jointly committed to support the extension of the trial at the CEC premises.

The extension of the current demonstration to two further buildings is planned by OPERA as follows;

4.6.1 Nerviens Building

An additional EC building housing many card holding employees that have recently moved from Beaulieu. This site has a small canteen operated by the CEC and an additional FTT interfaced to a Fuji cash register will be supplied.

The FTT shall be connected to the CEC telephone system and its contents will be polled from the site service host at the Beaulieu building.

Card users from this site will be serviced by the Beaulieu help desk.

4.6.2 Breydel building

An additional building of similar size to Beaulieu that will house a further site service host and help desk facility. The equipment description and functions are the same as for Beaulieu and a summary of equipment to be provided follows:

4.6.3 Breydel building summary

	Site host (SSH)	Reload station (RLS)	Hand held device	Merc-hant term	Transaction term (FTT)	Vending interface (VMI)	Wallets	Cards
Coffee Shop					1			
Canteen					2			
Vending						3		
Help Desk	1	1	1	1	1			
Total	1	1	1	1	4	3	50	1,200

4.7 Project management

In addition to the resource allocated earlier in the project to the technical management of CAFE the need for a full time demonstration co-ordinator was identified. The co-ordinator resided in Brussels for the duration of the CAFE project.

The co-ordinator's responsibilities included:

Carrying out the trial set up activities.

Liaise with the CEC with regard to the day to day running of the demonstration.

Manage the help desk, card personalisation and data base management function.

Ensure the smooth operation of the clearing and settlement procedures.

The following charts are extracted from the project plan drawn up at the time to help manage the trial operation and list some of the detailed activities involved in the trial operation.

Task Name	Task Name
Trial Set up Activities	Operational support
Survey	Locate trial office
Detail interfaces	Help and enquiry point procedures
Comms lines	Recruit support staff
Canteen Procedures	Produce user instructions
Placement of equipment	Produce operator manuals
Accounting	Hanging by demo group
Accounts relationships	Simulated acquirer files available
Audit methods	First cards available
Exchange rate handling	Card tests
Marketing plan	FTT,VMI,RLS tests
Card Design (surface print)	SSH Tests
Card Design (laminated)	CC tests
Plan incentives	Installation
Scheme publicity	Training
User recruitment aids	Help desk and SSH staff
Application forms	Merchant awareness
Exit strategy for Girovend cards	

4.8 User documentation

A comprehensive user guide was produced (in four languages) to help users of the demonstration to become familiar with the operation of the system. The guide went into greater detail than would normally be expected since the single guide covered not only use of the card but details of the use of all the terminal equipment. The user guide which was designed to fit into a jacket pocket is reproduced in the following pages for information.



Card User Guide

Safety First!

The Xchange Card Reloading Station

Changing your PIN

Loading your Card with Electronic Cash

Checking the Balance on your Card

Changing the Language of your Card

Transferring Electronic Cash from your Xchange Card to your CAFE Account

Paying for Purchases in the Coffee-shop or Self-Service Restaurant...

Check your Receipt!

Using the Vending Machines

Multi-Currency Operation

Looking after your Card

If your Xchange Card Fails in Service...

Lost or Stolen Card?

Need some Help?

For Holders of CAFE Wallets.

Contents

About the CAFE Trial

Participating in the CAFE Trial

About the CAFE Trial...

CAFE (Conditional Access For Europe) was conceived as Project 7023 under the ESPRIT III research programme. Essentially a trial of electronic payment technology in the premises of the European Commission in Brussels, it seeks to demonstrate the feasibility of the electronic purse as a vehicle for cross-border financial transactions in a multi-currency environment with the ECU as a base currency.

The trial is the result of close collaboration between commercial companies and research organisations from seven European countries over a three-year period.

Extensive market research was used to elicit from members of the general public a list of features considered to be desirable in an electronic payment system of this type and, wherever possible, these have been implemented.

The system has been designed to be fully interoperable, that is, to allow for multiple card issuers and service providers.

Participants will be issued with a smart card - the Xchange Card. A limited number of them will also receive one of two types of electronic wallet. The latter use a contactless infra-red interface to effect payment from a distance, the customer merely having to point his wallet at the cash register and press a button.

Among other innovations featured are:

- the first use of advanced public key cryptography in an electronic payment system for maximum security.
- multi-currency operation - the electronic purse may be used to make payment in local currency or ECU.
- fault and loss tolerance provision - to allow fraudulent (cryptographically flawed) or erroneous transactions to be detected and ignored.
- the ability to preserve the anonymity of the person making payment unless that person chooses to reveal his identity, for example, in the event of card theft or loss.

At the end of the trial, the reaction of participants will again be sought to determine the acceptability of the features tested.

Participating in the CAFE Trial

The CAFE trial has been designed as a conventional banking system in miniature to make it as realistic as possible. Thus, when you apply to participate in the trial, a personal account will be opened for you in the CAFE 'bank' and you will receive an Xchange Card electronic purse.

You may deposit cash, cheques drawn on a Belgian bank or Eurocheques at the CAFE help desks. All cheques must be made out to "DG IX /C/7 Restaurants-Economat", crossed and supported by a current cheque card and must not exceed the 7,000 BEF guaranteed limit.

You may then withdraw funds from your CAFE account and load them onto your Xchange Card as electronic cash.

Whenever you spend electronic cash, each transaction will be encapsulated in an electronic 'payment envelope' to render it unique for security reasons, so, whenever you withdraw electronic cash, a number of 'payment envelopes' will also be transferred to your card.

- During the CAFE Trial, you may store both BEF and ECU in separate balances on your Xchange Card.
- All purchases of electronic cash must be made in BEF.
- Until further notice, the exchange rates for buying and selling ECU will be set at: 1 ECU = 40 BEF.
- A maximum of 4,000 Belgian francs or 100 ECU (both currencies combined) may be stored on the card.
- All purchases from participating outlets or vending machines will be charged to the Xchange Card either in Belgian francs or in ECU converted to Belgian francs. During the initial phase of the CAFE trial, all purchase must be made *wholly* in BEF or in ECU. It is not currently possible to aggregate the two currencies to complete a transaction.
- You may use your Xchange Card to make purchases in Beaulieu 5 and Breydel buildings at the following locations:
 - self-service restaurant
 - coffee-shop

- vending machine area

Safety First!

Your Personal Number ensures that only *you* can transfer funds from your CAFE account to your Xchange Card. It protects your account if your card falls into the wrong hands.

Remembering your Personal Number isn't always easy... By allowing you to choose your own, we believe we've made the task that much easier.

What's more, you can change your personal number as often as you like... a useful precaution if you suspect somebody else may have discovered it.

All Xchange Cards are issued with the same temporary PIN.

So, when you receive your card: **first, change the PIN.**

Remember...

- never tell anybody else your Personal Number
- try to memorise it
- if you *must* write your PIN down, please disguise it
- don't write your PIN on your card
- don't write it on anything you keep with your card

The Xchange Card Reloading Station

Xchange Card Reloading Stations are situated at the CAFE help desks. They are available for use during the opening hours detailed at the end of this user guide. They enable you to perform all the operations described on the following pages. You may change your PIN or the language of your card or check your balance at any CAFE help desk, but you should always go to the help desk where your card was issued to reload your card with electronic cash or to return electronic cash from your card to your CAFE account.

To use the reloading station...

- Check that the message **XCHANGE** is displayed. If not, seek help.

- To ensure correct orientation, keep your thumb uppermost on the Xchange 'button' printed on the front of the card.
- Insert the card in the slot located at the front of the reloading station. Make sure you push it home.
- The main menu will be displayed, as follows:

WITHDRAWAL	A
DEPOSIT	B
CARD BALANCE	C
OTHER	D

The Reloading Station is fitted with a time-out facility: if you wait too long before selecting an option, a persistent beeping will sound. You will be prompted to remove your card:

*Insert your card again when you see the **XCHANGE** Message re-appear on the display.*

Changing your PIN

- Select the **OTHER** option from the main menu by pressing button **D**.
- The **OTHER** sub-menu will be displayed:

OTHER	
CHANGE LANGUAGE	A
CHANGE PIN	B

- Select the **CHANGE PIN** option by pressing button **B**.
- The first time you use your card, type in the Personal Number **0000** and then press the **OK** button.

*(On subsequent occasions, if you are changing your PIN, type in your current PIN + **OK**.)*

- To change your PIN, type in a new 4 digit PIN and then press the **OK** button.

*(Do not use combinations of the same number, such as **4444** or easily deduced sequences like **1234** or your year of birth.)*

- To confirm your choice, re-type the new 4 digit PIN and then press the **OK** button.

- Remove your card *only* when instructed to do so.

*If you make a mistake when typing in or confirming the PIN and discover it before striking the **OK** key, use the ← key to erase the wrong number(s). Then type in the correct number(s).*

*Alternatively, press the red **C** key, remove your card and start again from the beginning.*

*If you make a mistake when typing in your old PIN and press the **OK** key, you will be granted two more attempts at entering the correct PIN before the card is locked. If this happens, seek help.*

Loading your Card with Electronic Cash

- Select the **WITHDRAWAL** option from the main menu by pressing button **A**.

- Enter your 4 digit PIN and then press the **OK** button.

*If you make a mistake when entering your PIN and discover it before striking the **OK** key, use the ← key to erase the wrong number(s). Then type in the correct number(s).*

*Alternatively, press the red **C** key, remove your card and start again from the beginning.*

*If you make a mistake when entering your PIN and press the **OK** key, you will be granted two more attempts at entering the correct PIN before the card is locked. If this happens, seek help.*

- Press button **B** (BEF) or button **C** (ECU), depending on which currency you wish to load onto your card.

- Type in the amount you require, then press **OK**.

(The maximum sum you may load onto your card is limited to 4,000 BEF or 100 ECU. If you want to have both BEF and ECU on your card, the sum of the two currencies should not exceed 4,000 BEF.)

*The message **AMOUNT TOO HIGH** will appear if:*

- * *the amount exceeds your CAFE account balance*
- * *the amount exceeds 4,000 BEF (BEF + ECU)*
- * *the amount entered + the card balance (BEF + ECU) exceeds 4,000 BEF (BEF + ECU).*

The reloading station will then display the maximum amount which may be loaded onto the card without exceeding the 4,000 BEF limit. The transaction will be aborted and you will be prompted to remove your card.

- *Insert your card and start again at the beginning.*
- *Enter a lower amount and press the **OK** button.*
- **Remove your card only** when instructed to do so.

Checking the Balance on your Card

- Select the **CARD BALANCE** option from the main menu by pressing button **C**.

- ☐ The balance(s) on the card will be displayed, together with the number of electronic payment envelopes left.

(If there is no money - or no longer any money - on the card, you will not see any entry - even a zero balance - but the number of payments left will be displayed.)

- ☐ The display will then revert to the main menu.

Changing the Language of your Card

- Select the **OTHER** option from the main menu by pressing button **D**.

- ☐ The **OTHER** sub-menu will be displayed:

OTHER	
CHANGE LANGUAGE	A
CHANGE PIN	B

➤ Press button **A** to select **CHANGE LANGUAGE**.

The following sub-menu will be displayed:

ENGLISH	A
FRENCH	B
DUTCH	C
GERMAN	D

- Press **A**, **B**, **C** or **D** followed by the **OK** key to select the language you require.
- Type in your PIN when requested to do so, then press the **OK** key.
- Remove your card *only* when instructed to do so.

Transferring Electronic Cash from your Xchange Card to your CAFE Account

(You are unlikely to perform this operation, unless you decide to cease to participate in the CAFE trial.)

- Select the **DEPOSIT** option from the main menu by pressing button **B**.
- Enter your 4 digit PIN and press the **OK** button.

*If you make a mistake when entering your PIN and discover it before striking the **OK** key, use the ←*

key to erase the wrong number(s). Then type in the correct number(s).

*Alternatively, press the red **C** key, remove your card and start again from the beginning.*

*If you make a mistake when entering your PIN and press the **OK** key, you will be granted two more attempts at entering the correct PIN before the card is locked. If this happens, seek help.*

- Press button **B** (BEF) or button **C** (ECU), depending on which currency you wish to transfer from your card to your CAFE account.
- Type in the amount you wish to deposit, then press the **OK** button.

*The message **AMOUNT TOO HIGH** is displayed if you try to deposit more than you have on your card. The message **OPERATION CANCELLED** will appear, the transaction will be aborted and you will have to re-insert your card and start again from the beginning.*

- *Type in a smaller amount and press the **OK** button.*
- Remove your card *only* when instructed to do so.

Paying for Purchases in the Coffee Shop or Self-Service Restaurant...

- The cashier will ring up your purchases as usual.
- The price to pay will be displayed on the cash register.
- The cashier will ask if you wish to pay by Xchange Card.
- Hand over your card.
- The cashier will insert your card into the card terminal.
- The value of the bill will be deducted from your card.

*For an explanation of how the system functions when the card is loaded with ECU as well as BEF, please see '**Multi-Currency Operation**' .*

- The cashier will hand your card back, together with the receipts printed by the card transaction terminal and the cash register.
- Please *keep* your two most recent receipts in case of queries.

XCHANGE		
①, ②	06/09/95	12h35
③	BU5-DGIX-Self Service-001	
④	Card # 000628	
⑤	Start bal.:	3226 BEF
	File # 3	Record # 2
⑥	Payee:	50 BEF
⑦	Customer:	50 BEF
KEEP RECEIPT		

Check your Receipt!

- ① Date
- ② Time
- ③ Site/retailer/terminal identification
- ④ Card serial no.
- ⑤ Initial balance of currency debited to card
- ⑥ Amount & currency received by retailer
- ⑦ Amount and currency debited to cardholder
- ⑧ Exchange rate for currencies if applicable

XCHANGE		
①	03/09/95	13h05
②	BREY-Coffee Shop-002	
③	Card # 000342	
④	Start bal.:	47 XEU
⑤	File # 4	Record # 9
⑥	Payee:	120 BEF
⑦	Customer:	3 XEU
⑧	Exchange Rate:	1 XEU = 40 BEF
KEEP RECEIPT		

Using the Vending Machines

- Check that the card reader display shows **XCHANGE**.
- To ensure correct orientation, hold the card vertically, your thumb on the Xchange 'button' and towards you.
- Insert the card, chip first, vertically upwards in the slot in the base of the card reader.
- The card reader display will show **WAIT...** If you have any funds on the card, the card reader display will show a balance in BEF or ECU. (See 'Multi-Currency Operation'.) The vending machine display will show the price of the most expensive item.

*If you have no electronic cash in any currency on the card, the message **CANT PAY** will be displayed.*

*If you have electronic cash, but no payment envelopes, the message **GO TO RLS** will be displayed.*

If you see either of the above messages, you should return to the help desk where your card was issued to reload your card.

- Press the buttons on the vending machine keypad to make your selection.
- First the item code, then the item price, will appear on the vending-machine display. The item will be vended..
- *If you have insufficient funds for the chosen item, the vending machine will bleep three times. The price of the item will briefly appear on the lower display, which will then again show the card balance (if only one currency is present) or the larger balance (if more than one currency is present). You should then either choose a less expensive item or return to the CAFE help desk where your card was issued to reload it.*
- The card reader display will show the remaining balance.

Multi-Currency Operation

When you use your card to make a purchase in the self-service restaurant or coffee-shop or from a vending machine, the system will automatically determine from which balance to deduct payment according to logical and arbitrary rules.

In the self-service restaurant or coffee-shop...

- if there is sufficient local currency on the card, the Belgian franc balance will be debited.
- if there is *insufficient* local currency, the system will determine whether there is an ECU balance on the card. If so, and if that balance contains sufficient ECU to permit settlement of the transaction when converted at the prevailing rate, the ECU balance will be debited.
- A receipt will be printed by the card transaction terminal showing the price paid in local currency and, where appropriate, the exchange rate and the corresponding amount deducted in ECU.

At a vending machine...

- If there are BEF but no ECU present on the card, the BEF balance will be displayed, even if it is insufficient to permit the purchase of any of the items on offer. Provided the cost of the item selected does not exceed the displayed value, the transaction will be permitted.
- Otherwise, the vending machine will bleep three times to warn you that you have insufficient funds. You should either choose a less expensive item or return to the help desk where your card was issued to reload it.*
- The new card balance will be displayed.
- If the card carries BEF and there are ECU present:
 - if there is sufficient local currency to pay for the *most* expensive item, the BEF balance will be displayed (even if there are more ECU on the card) and will be debited to pay for the transaction

- if there are *sufficient* ECU but *insufficient* BEF to pay for the *most* expensive item, the ECU balance will be displayed and will be debited to pay for the transaction.
- if there are *neither* sufficient BEF *nor* sufficient ECU to pay for the *most* expensive item, the larger of the two balances will be displayed. Provided sufficient funds remain to permit the transaction, the displayed balance will be debited.
- *Otherwise, when you make your selection, the vending machine will bleep three times to warn you that you have insufficient funds. You should either choose a less expensive item or return to the help desk where your card was issued to reload it.*

Looking after your Card...

Since your Xchange Card contains cash, you should look after it as carefully as you would your conventional purse.

If you lose your card or if it is stolen, you may well lose some or all of your electronic cash, if somebody else finds and uses the card before you notify us of your loss or before we can take appropriate action.

Your Xchange Card is robust, but it should not be abused.

Please observe these simple precautions:

- *do not bend your card, or it will eventually snap*
- *do not expose your card to extreme heat*
- *keep your card free from grease and chocolate*
- *do not use solvents to clean your card*
- *if cleaning is necessary, wipe with a dry cloth*
- *do not exert intense pressure on the microchip*

If your Xchange Card Fails in Service...

Please don't throw it away! Take it instead to any CAFE help desk.

You will be issued with a replacement card free of charge the next working day, credited with the card balance remaining at the point where the previous card failed. Replacements are subject to availability.

Alternatively, you may choose not to participate any longer in the CAFE trial. In that case, a refund of the above balance will be made on the next working day following the day you return your card. Any money remaining in your CAFE account will also be refunded. Either way, we *must* receive your card first!

Please note that we may offer a refund instead of a replacement card at our discretion.

Lost or Stolen Card?

If you lose your card or think it may have been stolen, please inform one of the CAFE help desks as soon as possible.

You may notify us in person during our office opening hours (see below) or leave a message on the CAFE 24 hour Card Loss Answering Machine, *tel.: 91564. (All messages are automatically time- and date-stamped.)*

Please leave your full name (to be repeated, slowly), your daytime telephone number, the number of your card (*not* your PIN) and brief details of your problem.

Similarly, if you find a lost card, please return it as soon as possible to one of the CAFE help desks.

If notification is received *before* 1700 hrs., we shall take immediate steps to prevent any further funds being downloaded from your CAFE account onto your Xchange Card - even if somebody else has discovered your PIN. We shall also take action (at midnight, or sooner if possible) to prevent any further purchases being made with it.

If your message is left *after* 1700 hrs., we shall take the above precautions as soon as possible after 0900 hrs. the next working day.

Need some Help?

If you are experiencing difficulty in using your Xchange Card, please contact the CAFE help desks for advice and practical assistance.

Beaulieu 0/133 *tel.: 93411*

Breydel 5/186 *tel.: 90533*

Opening Hours: Monday-Friday: 1000 - 1115 hrs.
1145 - 1400 hrs.

Except for European Commission and public holidays.

For Holders of CAFE Wallets

The attention of holders of CAFE Two-Button Wallets and Full-Function Wallets is drawn to the fact that supplementary user guides for these devices are available on request from the CAFE help desks.

4.9 The Exchange logo

It was decided to give the card used in the demonstration a “scheme identity” independent of any particular issuer, this emulated the normal practice of branding cards in such a manner that the user can easily identify a logo on the card that is reproduced at the points of use. Although the project was called CAFE the name was not considered suitable since the main use of the card was indeed in canteens and it was felt that the generic nature of the electronic purse function would be lost if the name CAFE was chosen.

The new name Xchange was chosen because of the connection between the use of the card for multi-currency operation (where Exchange rates are involved) and as a purse holding loose change.

The Logo design was commissioned with the brief to present the name on a background of a coins of different sizes, and the chosen stylistic representation of this appears above. All cards used in the demonstration carry this logo as does the promotional literature and decals indicating where the card may be used.



5 Demonstration equipment functionality

This section describes the principles and operation of the CAFE trial in the premises of the European Commission. The CAFE consortium have developed an architecture for payment transactions that is both highly secure and suitable for cross border payments of all kinds between any number of issuing banks and service providers. In the demonstration one type of payment, commonly known as the electronic purse, is demonstrated. The purse may either be a smart card or an electronic wallet that is used with contactless communications. Consumers load their purse with electronic value denominated in currency provided by the issuer, the value can then be spent in canteens, coffee shops and for drinks and snacks from automats in the Commission. A prime feature of the multi-currency operation is the use of the ECU as a common currency for use across borders².

5.1 Structure of demonstration:

The demonstration is structured to emulate as closely as possible the roles found in commercial payment schemes. These roles are:

- The **consumers** (cardholders)
- The **acceptors** (service providers)
- The **issuers** of value
- The **acquirers** of value
- The **clearing** of value
- The **help desk**

5.2 Key technical points of the demonstration:

- * Use of smart cards carrying advanced cryptographic processors.
- * Multi-currency operation with the ECU as the base.
- * Clearing of signature transporting transactions between multi-issuers and multi-service providers.
- * Handling of loss and fault tolerant processes.
- * Use of electronic wallets with contactless infra-red point and pay features.

5.3 Scope of trial:

The trial takes place using a small number of cards at first, in one building of the European Commission in Brussels, namely Beaulieu. Shortly afterwards it will be expanded to a second building, Breydel. The card will be accepted as payment for canteen meals, coffee shop purchases and snacks/drinks from vending machines located in the two buildings. It will be possible to load the cards at the CAFE project help desk in each building. The help desks will be manned throughout the trial

² For example a consumer may load their purse with their own country's currency (home currency) and some ECU. When away from home points of payment will automatically select the ECU as the currency to be used for payment. When at home, home currency or ECU may be used.

during lunch periods and enquiries may be made by telephone during normal working hours. As the trial progresses electronic wallets will be introduced as "point and pay" devices in addition to the cards.

The trial will last for at least six months and during this period the reaction of the users, service providers and operators will be surveyed. Further commercial sponsorship has been obtained from a number of financial issuers (members of the Special Interest Group for Multi-currency Electronic Wallets - SIGMEW). It is the intention of the trial sponsors to provide funding for additional cards, wallets and promotion to expand the trial in these two buildings. Further proposals are in hand to extend the trial beyond six months and into other EC and Non EC premises. In the trial the card will carry the Xchange logo plus any sponsoring issuer identification.

This part of the document describes the operation of the demonstration from the perspective of the different players in the demonstration system.

5.4 The Consumer Perspective

5.4.1 Joining the Scheme and obtaining the cards / wallets

Employees of the EC will be invited to fill out simple application forms for cards. Cards and later wallets will be issued "free of charge" from the Xchange help desks. Each cardholder will receive instructions for use of the cards at all points of sale and the re-loading station. The reloading station acts like a "cashless" ATM for loading and re-loading the card.

For at least the start of trial period the use of consumers cards will be tracked by a mirror account held in the SSH computer this feature is intended to be used in the resolution of consumer queries during the initial stages of the trial.

Application forms will be held in confidence by the trial operator and will be used to facilitate the monitoring of trial usage with consumer survey questionnaires and interviews.

5.4.2 Loading with value (Withdrawal)

Cardholders will be invited to load funds, assisted where required by help desk personnel, onto the card in return for cash, cheques, or later in the trial debit card authorisations. Any Girovend cardholders will also be able to transfer their remaining Girovend balances onto the Xchange card.

Loading can be carried out at the reload station located at the help desk where the card was issued as follows:

- * The cashiers at the help desk will accept payment from the cardholder. They will enter this amount into the computer that controls the reload station (RLS) against a cardholder suspense account that relates to the serial number of the card.
- * The cardholder will be encouraged to load all the payment onto their card by using the (RLS). The first time this is done help desk staff will be available to assist them through the operation.
- * Only cards can be loaded at the RLS. The wallets used early in the trial can only be used for payment when they carry a card with value.

Details of consumer operations for withdrawals are included in section 5.10

5.4.3 Changing the PIN (Change PIN)

The Cardholders PIN (personal identification number) is held secretly on the card and is only used during the withdrawal, deposit and change PIN functions. All transactions at POS or vending machines do not require PIN entry.

- * The cashiers at the help desk will encourage users to change their PIN the first time they use the RLS³ to withdraw funds and warn users that if they forget their PIN then they will be unable to withdraw or deposit funds at the RLS. The help desk does not keep records of any user PIN's and cannot be responsible for their use. Indeed once a card is locked⁴ it can only be unlocked by special procedures.

Details of how PIN's may be changed are included in section 5.10

5.4.4 Depositing value

Cardholders may at any time return funds to their suspense accounts, for example to obtain a refund of their balance should they wish to leave the scheme.

- * The suspense account acts like a pseudo bank account for the purpose of this trial.

Details of how Deposits may be made are included in section 5.10

5.4.5 Reviewing the balance (Show balance)

Cardholders may review the balances held on their card at any time by using the RLS.

- * The values of all the different currencies held in the card and the maximum number of payments the card can still make are displayed⁵

Details of how balances may be reviewed are included in section 5.10

5.4.6 Spending value at an attended point of sale

³ For the trial the first time a card is used the PIN will be set to the default value 0000, consumers will be encouraged to change this to another number they will easily remember.

⁴ Three incorrect PIN entries in succession will render the card locked. If a locked card still has value then it is possible to use it up, but cannot be re-loaded

⁵ The value carried by the card is not the only limiting factor on spending. Value can only be spent if there are cheque blanks (authorised by the issuer) available, the current card can carry up to 70 cheque blanks. If there are none left then any value remaining on the card cannot be spent until further cheques are loaded into the card. The next withdrawal will again fill the card with cheque blanks even if zero value is withdrawn.

Cardholders may use their cards to purchase goods from the canteens and coffee shops the procedure is the same at both points of sale. However there are differences when using the card alone or the card with wallet.

In the event that a refund is to be given this will be made in cash as it is impossible to add value to cards at the Point of sale.

Using the card

- * The card holder selects the goods to purchase in the same way as for any other means of payment. The cashier will enter amounts on the cash register as normal and ask for the method of payment.
- * By handing over the Xchange card to the cashier the cardholder implies a card payment. The cashier will select an Xchange payment on the cash register and insert the card into the transaction terminal, the amount to be paid will be deducted from the card.⁶
- * The cardholder will be given a receipt showing the opening card balance, the purchase value and currency. During the trial they will also be given the normal cash register receipt. It is recommended that cardholders keep their receipts.

Using the (point and pay) wallet

- * The wallet holder selects the goods to purchase in the same way as for any other means of payment. The cashier will enter amounts on the cash register as normal and ask for the method of payment.
- * The point and pay link facing the wallet holder will activate (this is indicated by the illumination of a red light on its panel).
- * To make a payment the wallet is turned on and pointed at the link. The amount to pay will be shown on the wallet, pressing the pay button on the wallet confirms the payment and the amount is deducted from the card in the wallet.
- * The wallet holder will be given a receipt showing the opening card balance, the purchase value and currency. During the trial they will also be given the normal cash register receipt. It is recommended that wallet holders keep their receipts.

⁶ If there are insufficient funds on the card then no transaction takes place and the cashier asks the cardholder to pay by another method.

5.4.7 Spending value at vending machines

Currently only cards can be used to purchase goods from the vending machines.

Using the card

- * The card holder inserts the card in the vending machine reader which displays the cards balance. The required goods are then selected, if sufficient funds are available on the card then the transaction proceeds and goods are delivered⁷. The cards closing balance is shown on the display.
- * Further vends can then be made if sufficient funds are available until the card is finally removed.

Details of the vending operation are included in section 5.10

Using the wallet

- * At present wallets cannot be used with the type of vending machines installed. Later in the trial a new vending machine is scheduled for introduction that operates in such a way as to make wallet payments practical.
- * If use of the wallet is attempted at the currently installed machines then the display use card will be shown.

5.4.8 Multi-currency operation

The trial has been set up to allow operation in multiple currencies. The explanation of how this operation is simplified by using the following descriptions:

Home currency:	The national currency of the user.
Local currency:	The national currency of the sales outlet.
ECU:	The European Currency

Unit.

for example in the case of the trial sites at Beaulieu & Breydel the local currency of the sales outlet is Belgian Francs and the cardholders home currency will be Belgian Francs.

During the early phase of the trial the help desks will only be able to accept Belgian Francs in payment for value loaded onto the cards. In order to test the multi-currency option a number of users will be encouraged to load some Belgian Francs and ECU onto their card. The exchange rate used at the point of sale and for loading will be identical so that there is no financial risk to users or the trial operators during this phase⁸.

⁷ If there are insufficient funds on the card then no vend takes place

⁸ Later in the trial when a sponsoring bank becomes an issuer the buying and selling rates may be different replicating the true commercial situation.

Multi-currency operation is implemented in the trial as follows.

The user presents their card in the normal way at the points of sale or vending machines.

Where the home currency equals the local currency and there is sufficient value on the card the sales point will complete the transaction in the local currency.

If there is not sufficient home currency or the home currency does not equal the local currency of the sales point, the sales point will automatically look for ECU in the card and providing there are sufficient ECU then the transaction will be performed in ECU. The rate used to determine the ECU value will be that stored in the point of sale or vending machine for conversion from local currency to ECU.

If neither currency is sufficient then the transaction will be terminated even if the combined value of both currencies would have been enough.

Cards at the point of sale using ECU

- * The cash register will display the amount to pay in the local currency. If (in accordance with the above rules) ECU is used for payment the transaction terminal receipt will show the value taken from the card in ECU and the payment to the service provider in local currency.

Wallets at the point of sale using ECU

- * The cash register will display the amount to pay in the local currency. If (in accordance with the above rules) ECU is used for payment the wallet will display the amount to be paid in ECU.
- * Once the "Pay" button on the wallet is pressed the transaction will proceed and the transaction terminal receipt will show the value taken from the card in ECU and the payment to the service provider in local currency.

Cards used at the vending machines

- * If (in accordance with the above rules) and the ECU balance is greater than the local currency balance ECU will be used for payment and vending machine will display the cards ECU balance.⁹

⁹ After a vend the rules are checked again and it may be that the next vend is in local currency

5.4.9 Fault and loss tolerance

The trial uses the capability, built into the CAFE payment architecture, that allows recovery from the anonymous transactions those made by a particular card. In the trial the seed key used by the card to provide unconditional anonymity will be held, on the cardholders behalf, in the acquiring computer at the help desk where the card was issued.

- * Cardholders whose cards become faulty (unreadable) during the trial will be able to obtain a refund of the remaining value from the help desk the working day after they return the card to the help desk.
- * Cardholders who lose their cards must identify themselves and report the loss to the help desk. Cards so reported will be listed as lost and entered onto a negative file which will be transferred into each point of sale. It will be possible to give refunds one full working day after the loss has been notified¹⁰. Should the card holder subsequently recover the card the listing in the negative file will be removed from the file within one working day after the help desk has been notified.

5.4.10 Leaving the scheme

Should a cardholder wish to leave the scheme they can recover the remaining card value at the help desk where the card was issued.

- * To recover their card balance they must deposit all the value from their card into their suspense account, return the card at the help desk along with any outstanding questionnaires they may have and they will then immediately receive a refund of the value held in their suspense account.

5.4.11 Incentive programme

From time to time during the trial the sponsoring issuer(s) may wish to offer incentives to encourage usage of the card by various means. Details of potential schemes are still being produced by the sponsoring organisations and will be subject to the agreement of the EC and DGIX in particular.

5.5 The acceptors perspective

In the trial two independent commercial organisations (service providers) will accept the Xchange card. Each organisation will collect Xchange value and be reimbursed as a result of the daily clearing and settlement process by credit transfer from the issuer(s) into the bank account of the service providers¹¹.

¹⁰ This feature is only possible because the right to unconditional anonymity has vested in the issuer of the value for the early phase of the trial. If unconditional anonymity is retained by the cardholder then lost cards are equivalent to lost cash and the value cannot be refunded.

Loss tolerance can be implemented, in a global scheme for example, without the overhead of a negative file providing the card holder gives up the right to unconditional privacy when a loss is discovered and waits until all the cheque blanks held in their card are date expired (could be some months later). At this time the issuer may refund any remaining value without exposure to further payments by the missing card.

¹¹ In practice for the early phase of the trial Restaurants Economat will act as the issuer of value as well as one

5.5.1 The canteen and coffee shop service provider (DGIX)

At these attended points of sale, the operation of the CAFE trial is designed to have the minimum effect on the current operating procedures. The points of sale will be able to accept all the current methods of payment except that the Girovend card scheme, that only operates in the Canteen, will be progressively replaced by the Xchange card.

In the event that the Cardholder has insufficient Xchange funds they will have to make payment by alternative means.

Any refunds made at the point of sale, to customers that have paid with Xchange value, have to be made in cash as it is not possible to add value back onto cards at the point of sale.

Transactions made with the Xchange card are held individually in the transaction terminal and also logged in the cash register as card payments. The settlement for the Xchange card payments may subsequently be reconciled with the cash register daily log.

Cash register operation with the Xchange card

- * The cashier will ring up purchase in the normal way and the price to pay will be displayed on the cash register.
- * The cashier will ask how the customer wishes to pay and if offered an Xchange card will take the card and press the Xchange card payment button on the cash register. At this time the transaction value is automatically sent to the transaction terminal.
- * The cashier then inserts the card into the transaction terminal alongside the cash register, payment is taken from the card and a receipt issued by the transaction terminal and the cash register.
- * The cashier then hands the receipts to the customer.

For details of operation of the transaction terminal by the cashier see section 5.11.

Cash register operation with the wallet

- * The cashier will ring up purchase in the normal way and the price to pay will be displayed on the cash register.
- * The cashier will ask how the customer wishes to pay and if told by wallet will press the Xchange card payment button on the cash register. At this time the transaction value is automatically sent to the transaction terminal.
- * The customer now points and pays.

of the service providers

- * The cashier then hands the card and receipts to the customer.

For details of operation of the transaction terminal by the cashier see section 5.11.

5.5.2 The vending machine service provider (Sportschuur)

- * The vending machines (by nature unattended) accept cash as well as the Xchange card
- * In the event that the customer has insufficient Xchange funds they will have to make the whole payment in cash. Part payment by card and the remainder in cash is not supported in this trial.
- * Any refunds, to customers that have paid with Xchange value, will have to be made in cash in accordance with current procedures
- * Removal of the card at any time before value has been removed from the card will result in termination of the vend.
- * Transactions made with the Xchange card are held individually in the card reader built into the vending machine. They are also logged as a card total elsewhere in the vending machine. The settlement for the Xchange card payments may subsequently be reconciled with the vending machine totals¹².

Vending machine operation with the Xchange card

There are two generic types of vending machine commonly used, select after payment, and pay after selection. The first type is at present installed in the trial sites at the EC. Select after payment is cumbersome to operate with wallets and this option is precluded from the trial at this stage. It is the intention of the vending machine service provider to replace at least one machine with a pay after selection type during the trial if this occurs then use of the wallet with this type of machine will be implemented.

Card operation for "select after payment" machines

- * After the cardholder has inserted their card providing there are sufficient funds to purchase the highest cost item then the vending machines escrow (as if coins had been inserted) will be opened to that value¹³. Assuming there are sufficient funds the card holder may then select an item to vend.

Card operation for "pay after selection" machines

¹² Care must be exercised to ensure that any periodic reading of vending machine totals matches the same period as settlements made for Xchange value. Additionally since the card transaction totals held by the vending machine are held in volatile storage overall reconciliation may only be possible by referring to mechanical totalisers in the machine and subtracting the cash value collected

¹³ If the card contains less value than the highest cost item but more than the lowest then the escrow is opened to the remaining card value. If insufficient funds are available then the card is rejected

- * After the cardholder has selected an item to vend the vending machine display will show the value to be paid.
- * Inserting the card indicates the method of payment and if sufficient funds are available the vend will proceed.

5.5.3 Transaction collection

Before the service provider can be paid for Xchange card transactions the transaction data must be collected by the acquiring computer. In the trial two methods are used to retrieve transactions.

Automatically by polling of the transaction terminals.

Manually (using a hand held computer) by visiting each vending machine.

In both the above cases Xchange transactions are held in non-volatile storage and the same principle applies to transactions collected automatically or manually as follows:

- * All transaction data held in the transaction terminals and vending machines are delivered to the acquiring computer. In return a certificated file of previously collected and successfully cleared transactions is returned to the points of payment. Upon successful receipt of this certified file earlier transaction data may be deleted. By this means data not collected one day remains available for collection the following day and so on.
- * The certified return file also contains an update of the negative file, and the latest currency conversion rates.

For points of sale

- * The transaction terminals are polled via the internal telephone system at each site by the acquiring computer for that site. The polling takes place overnight, each terminal is polled in turn and if connection cannot be made the next terminal is polled. After all terminals have been polled then those where connections could not be established are polled again. Each terminal is polled up to a maximum of three times before the attempt to retrieve data from that particular terminal is abandoned.
- * Successfully polled terminals issue a paper receipt indicating that data has been sent to the acquiring computer.

For vending machines

- * The help desk personal will load, via floppy disc transfer from acquiring computer, the portable computer with certified return files destined for individual vending machines.
- * By visiting each vending machine in turn data is collected by using a collection card connected to the portable computer. The collection card is inserted into the card reader slot on the vending machine and the portable computer requests transfer of transaction data. In return it passes the appropriate certified return file to the vending machine.
- * The collected transaction files are then loaded into the acquiring computer, again via floppy

disc transfer.

5.5.4 Multi-currencies and guaranteed exchange rates

Where ECU are accepted for payment then during the trial settlement with the service provider will be made in their local currency. The rate guaranteed by the scheme¹⁴ to the cardholder shall be the rate specified for the day the transaction was made¹⁵. This rate is transferred from the acquiring computer to the transaction terminals and vending machine readers during the procedure for collection of transaction data.

5.6 The Issuers perspective

Xchange card value is withdrawn via the reload station (RLS) attached to the computers at each help desk. These computers are able to generate cheques and carry the suspense accounts for the cardholders and thus are emulating the role of a card issuer. For the trial there are two of these computers, one at Beaulieu and one at Breydel, they may later be configured so that each one represents a different issuer. The trial environment constrains the cardholder so that they can only load value at the site where the card was first issued (normally this would be where they work). Cards can of course be used for purchases at anywhere Xchange is accepted.

- * Multi-issuer operation can be implemented by allocating each site to a different issuer.

Issuers control the cheque generation process and the value loading.

- * By setting the maximum guarantee limit for each cheque.
- * By setting the expiry date for cheques
- * By means of the suspense account emulate access to a real bank account and control the value loading process.
- * By setting the purchase rate for different currencies
- * By setting the maximum total card balance allowed (The total card balance is the aggregation of all the different currencies held on the card)

Issuers control the guarantee to pay

- * Only valid cheques are accepted by the points of payment and or the issuer
- * Double presentation of the same cheque is detected and only honoured once.
- * In the unlikely event that a cards tamper resistance is compromised and cheques are spent twice

¹⁴ The term scheme is used here to signify that regardless of how many issuers of value there may be, at least for this trial, they will use common exchange rates.

¹⁵ In the case of the early stages of the trial the rate will be fixed and be the same as the rate used to withdraw value in ECU

anywhere in the system then this will be detected and the identity of the fraudster revealed. (the so called double spending check is fully implemented in the trial)

- * Secret Keys used in cheque generation may be changed during the trial and the public keys used in validation are distributed either directly or indirectly. For the transaction terminals the public keys are sent directly from the acquiring computer. For the vending machines the public keys are distributed by the cards themselves. In this case the issuers public key carried in the card is certified by the "scheme" and only the scheme public key need be previously known to the vending machine.

5.7 The acquirers perspective

The same computers that are used for the issuing of value are also configured to act as acquiring computers. Each site uses a separate computer to poll the transactions from the points of payment which are then passed on to the clearing computer for processing. Each computer collates the transactions from all the points of payment in its catchment area and produces a file (deposit table) for submission to the clearing centre which later returns a file to the acquiring computer of all cheques that should not be honoured (the reject table). Each acquiring computer holds a file (the settlement table) for all the service providers linked to it.

- * Whilst it is not envisaged for the early stages of the trial the responsibility for settlement could be delegated separately to each site.
- * The polling of transaction terminals is automatic via internal telephone lines and takes place overnight¹⁶.
- * Once collated the acquiring computer dials the clearing centre computer via the PSTN to send the deposit table for clearing.
- The acquiring computer then waits for a return call from the clearing computer to deliver the reject table, and any other essential information.

5.8 The Clearers perspective

A separate computer is allocated to this task and can in principle be sited anywhere. Currently this computer is sited in the Beaulieu help desk office. The clearing computer maintains a table of all cheques collected and compares newly received cheques against this table. As cheques expire they can be eliminated from the table.

The clearing system is based on the use of a standard database package (Paradox™). Different tables contain, system parameters, backup data, live data, settlement reports, and activity logs.

- * Overnight the clearing computer waits for the acquiring computers to dial in, transfer its files, and ring off.

¹⁶ Transaction terminals may share a line with a voice telephone. In this event the terminal can be programmed not to respond to incoming calls during normal office hours.

- * Once all acquiring computers have sent files (there is a window of expectancy which if exceeded then that particular acquiring computer will be assumed mute for that night). The clearing program then automatically runs.
- * After clearing the Clearing computer dials up the acquiring computers that sent data and sends the results of the clearing process.

The clearing centre checks the entire scheme for instances of:-

- * Double spending (card hacking)
- * Double presentation of the same cheque
- * Invalid cheques, (digital signature is not valid)

It also produces report files for the acquiring computers containing:-

- * The table of rejected cheques
- * Scheme wide currency exchange rates
- * An acquirer settlement table
- * The aggregated service provider settlement table

5.9 The help desk perspective

Operators of the help desks are the main customer interface for the trial. Their duties involve operational and financial responsibilities.

Operational Services

- * The collection of application forms for cards
- * Controlling the issue of cards and wallets
- * Offering assistance to card holders
- * Control and monitoring of the reloading process, refunds, lost cards, locked cards and scheme leavers.
- * Manual collection of data from the vending machines
- * Operating the acquiring and clearing computers, ensuring back up procedures are maintained
- * Monitoring the operation of and first line (replacement) maintenance where possible of transaction and vending terminals

Operations involving financial responsibility

- * Collecting payment from cardholders (a cash register will be used to form part of the audit trail along with the entries into the suspense accounts)
- * Banking the cash collected with the issuers bank
- * Providing settlement information instructing the issuer to pay the service provider
- * Refunds to cardholders

5.10 Detail of operations from the consumer perspective

Withdrawal Operation	Display
* When the (RLS) displays the word “Xchange” the card may be inserted into a slot on the front of the unit.	Xchange
* At this time the display will show an options menu in the language chosen by the cardholder on their application form. The four languages implemented in the trial are Dutch, English, French and German. Pressing the function key A selects the withdrawal function.	Withdrawal A Deposit B Card Balance C Other D
* Withdrawal is selected and entry of a 4 digit PIN will be requested. Enter the PIN then press The OK button	Withdrawal Enter PIN
* After successful PIN entry the currency desired may be selected from a choice of BEF, XEU or other ¹⁷ . by pressing one of the relevant function key (B - D)	Withdrawal BEF B XEU C Other D
* If for example BEF is selected The amount required is entered on the numeric key pad and then OK is pressed	Withdrawal BEF Amount
* Providing there is sufficient funds in the suspense account for that card and the total value (the sum of all the currencies) on the card will still be less than 100 ECU equivalent the card will have the new value added to its balance ¹⁸ .	Please wait verification
* At the same time the number of payments available on the card will be topped up to the maximum of 70 this activity is shown on the display as it happens	Payments left 01(02 etc)
* Once the operation is successful the display scrolls to	Operation succeeded
* Once completed removal of the card is requested. Should the card be removed at any other time the loading operation will terminate, depending on where in the transaction this occurs will leave the card working with new value or not.	Remove your card
* Card is removed	Xchange

¹⁷ If "other" is chosen the user may scroll through currencies by repeatedly pressing the function button until the correct currency is found.

¹⁸ If the amount requested exceeds the maximum card limit or there are insufficient funds in the suspense account then the display will show **Amount too high**

Change PIN Operation	Display
* When the (RLS) displays the word “Xchange” the card may be inserted into a slot on the front of the unit.	Xchange
* At this time the display will show an options menu in the language of the cardholder as indicated on their application form. The four languages implemented in the trial are Dutch, English, French and German. Pressing the function key marked D selects the Other function.	Withdrawal A Deposit B Card Balance C Other D
* The menu then changes to a sub menu	Other Change Language A Change PIN B
* Select Change PIN and enter the current 4 digit PIN.	Other Enter PIN
* After successful entry of the current PIN a new PIN may be entered. The PIN must be only 4 digits and is entered on the numeric key pad followed by pressing the OK button	Other Enter New PIN
* The new PIN must then be re-entered to ensure that the new PIN has been entered and stored correctly. If the re-entry does not confirm the previous entry then the changing of the PIN will not take place and the old PIN will remain valid	Other Confirm New PIN
* When confirmed correctly the PIN will be changed and PIN Changed will be shown	PIN Changed
* The display scrolls to	Operation succeeded
* Once completed removal of the card is requested. Should the card be removed at any other time the loading operation will terminate, depending on where in the transaction this occurs it will always leave the card operational with new value or not.	Remove your card
* The card is removed	Xchange

Deposit Operation	Display
* When the (RLS) displays the word ready the card may be inserted into a slot on the front of the unit.	Xchange
* At this time the display will show an options menu in the language chosen by the cardholder on their application form. The four languages implemented in the trial are Dutch, English, French and German. Pressing the function key B selects the deposit function.	Withdrawal A Deposit B Card Balance C Other D
* Deposit is selected and entry of the 4 digit PIN will be requested then press OK	Deposit Enter PIN
* After successful PIN entry the currency to be deposited is selected.	Deposit BEF B XEU C Other D
* If for example BEF is selected. Type in the amount then press OK	Deposit BEF Amount
* The display then scrolls through	Please wait verification
* and	Operation succeeded
* Once completed removal of the card is requested. Should the card be removed at any other time the operation will terminate, depending on where in the transaction this occurs will leave the card working with new value or not.	Remove your card
* Card is removed	Ready

Card Balance Operation

- * When the (RLS) displays the word ready the card may be inserted into a slot on the front of the unit.
- * At this time the display will show an options menu in the language chosen by the cardholder on their application form. The four languages implemented in the trial are Dutch, English, French and German. Pressing the function key C selects the card balance function.
- * Show balance is selected, the balances on the card and the number of payments still possible will be displayed
- * The terminal will then return to the main menu

Display

Xchange

Withdrawal	A
Deposit	B
Card Balance	C
Other	D

Card Balance	
BEF	XXX
XEU	XX,XX
Payments left	XX

Withdrawal	A
Deposit	B
Card Balance	C
Other	D

	Vending Operation in local currency Where the card carries sufficient funds for several items and no other currencies are present	Display	
*	When the vending machine reader scrolls through the displays shown. The card may be inserted into a slot under the unit.	Xchange	
*	At this time the reader display will show the local currency card balance	BEF	XXXX
*	Select an item to purchase. The vend will take place and the reader display shows the remaining card balance.	BEF	YYYY
*	A further item may then be selected the vend will take place ¹⁹ and the reader shows the remaining card balance providing there are sufficient local currency funds on the card for the lowest cost item	BEF	ZZZZ
*	Removal of the card sets the display back to the main scrolling menu	Xchange	
	Vending Operation Where the card carries sufficient funds for several items and ECU are present	Display	
*	When the vending machine reader scrolls through the displays shown. The card may be inserted into a slot under the unit.	Xchange	
*	If there is insufficient local currency for the highest cost item but sufficient ECU then reader display will show the ECU card balance	XEU	XX.XX
*	Select an item to purchase ¹⁹ . The vend will take place using ECU and the reader display shows the remaining card balance.	XEU	YY.YY
*	If there is now more local currency than ECU and it is sufficient for the lowest cost item. The balance will automatically switch to BEF. A further item may then be selected using BEF ¹⁹	BEF	ZZZZ
*	Removal of the card sets the display back to the main scrolling menu	Xchange	

¹⁹ If the item to purchase costs more than the card balance then the display will show **Cantpay** and the vend will not take place

5.11 Transaction terminal operations from the service providers perspective

	Payment in local currency	Display
*	When the card payment button is pressed on the cash register the transaction terminal is ready and the customers card may be inserted into a slot on the front of the unit.	CARD>>>>>>> AMNT= XX
*	The cashier inserts the card and if the card holds sufficient local currency the display switches to	BEF XX PLEASE WAIT
*	A receipt is now printed and the display prompts for removal of the card	PROCESSED REMOVE CARD
*	Card is removed	Xchange

	Payment in ECU	Display
*	When the card payment button is pressed on the cash register the transaction terminal is ready and the customers card may be inserted into a slot on the front of the unit.	CARD>>>>>>> AMNT= XX
*	The cashier inserts the card and if the card holds insufficient local currency but sufficient ECU the display switches to	XEU XX PLEASE WAIT
*	A receipt is now printed and the display prompts for removal of the card	PROCESSED REMOVE CARD
*	Card is removed	Xchange

6 Running the demonstration

This section describes the system integration, initial running and first reactions from users to the demonstration. It highlights the experiences encountered in co-ordinating the individual workpackage developments into each other and the issues surrounding the integration of the overall development with on site equipment not originally designed to cater for the CAFE enhancements.

6.1 Background

The original CAFE project was planned as a technical demonstrator to validate the use of advanced cryptography in portable consumer devices. During the life of the project the consortium was offered the opportunity by the CEC to extend this scope of the demonstration and to run it on their premises.

The additional development workload placed on the project proved to be more than expected and the very ambitious timescale to implement the trial proved to be too optimistic thus unfortunately the trial did not commence operation until some nine months later than originally planned.

The consortium agreed to support an extension to the project for a further three months until the end of February 1996. Furthermore the OPERA members now intend to run the demonstration until the end of 1996 thus giving an extended period of running similar to that originally planned.

During the period until the end of April 96 the trial has run at a low level of usage to ensure the maximum of confidence in the system prior to major promotion and expansion by our commercial sponsors.

6.2 System integration

The system was first installed in April 1995. It soon became apparent that there was much development work outstanding. The system integration work that took place prior to delivery proved inadequate and with hindsight the installation should have been further delayed. It must be remembered that the majority of the equipment, software and system design is brand new and developed only to prototype stage. As can be imagined the integration of leading edge technology was not without problems.

All aspects of the integration procedure experienced difficulties, ranging from the production of the smart card containing the large chip to interfacing with change giving vending machines and Fuji cash registers. The majority of the issues encountered required the consortium to re-develop certain aspects of their work in order to achieve total integration with each other and the on-site installed equipment. The process to resolve all the difficulties took longer than anticipated as development changes were predominantly made off site and in isolation. In hindsight it would have been more productive to have duplicate off-site test beds with examples of all on site equipment available to each partner. The costs of such were however deemed prohibitive.

6.2.1 Technical issues

Whilst it is not intended to highlight here every detail of the items resolved during the system testing it is appropriate to illustrate the area where most work was required and in relation to the various items of equipment. The following Equipment versus Technical issues chart whilst inevitably an oversimplification of the complexity of the issues summarises the major problems resolved by the partners

Some explanation is necessary in order to interpret the chart:

* **Status**

Each item of equipment has been given a status either prototype or production this gives an indication of the maturity (and hence operational ruggedness) of the equipment.

Problem areas have been separated into three categories for each equipment:

* **Hardware**

The physical build standard of the equipment had to be modified.

* **Firmware**

Low level software, Normally held in PROM that runs basic primitive code for such things as communications, cryptography, keypad and display control.

* **Application software**

High level software, normally held in down loadable Non volatile RAM, that runs the application.

Equipment vs Technical issues

	Card	Vending Interface	FTT	RLS	Wallets	Site service host	Clearing Computer
Status	Prototype	Prototype	Production + Prototype Infra Red and Co-processor	Prototype	Prototype	Prototype software	Prototype software
Hardware	Low yield at high frequency	Required new version to overcome interface problems with change giver	Problems with Infra red and co-processor	User interface improvements	Case not rugged	Standard PC	Standard PC
Firmware	Excellent	Excellent	Excellent	Comms to SS host not rugged	Excellent	Excellent (Win NT)	Excellent (Win NT)
Applies Software	Minor SW Patches	Minor SW Patches	Many Patches made major interface problem with Fuji till	Major user interface changes and patches on SSH	Minor Patches required	Mirror accounts User interface ?	Currency table re-write, key management enhancements

The following is a brief overview of the technical issues noted in the chart.

Cards:

The crypto chip chosen is one of the most advanced available to the project, problems have been encountered with cards failing to load cheques (a process that involves the card in significant cryptographic calculation) and then becoming unusable. It is believed that if the cards are run at a slower speed 3.5MHz instead of 7MHz the problem is unlikely to happen. The frequency of 7 MHz is within the specification for the chip and the problem is still under investigation.

Vending Machine Interface:

The interface exhibited a fault of an intermittent nature (several days of successful operation then a failure would occur). The vending machine is set to accept coins as well as cards and includes a change giving facility, periodically the interface would block the acceptance of coin. The complexity of the vending machines necessitated a new hardware and software configuration to solve the problem.

Financial Transaction Terminal:

Although this terminal is a production item the cryptographic processor and infra red interface is housed in prototype hardware. Implementation of the cryptographic software proved more difficult than envisaged but is now finalised and some of the firmware had to be changed to solve a problem whereby transaction records could be missed. Also interfacing to the Fuji cash register proved difficult and intermittently a transaction in progress will lock up. Cash registers that could be replaced with a new model do not exhibit this problem. But because the canteen cash registers are deeply embedded in the overall canteen system it was not possible to offer replacements for these. The age of the canteen registers also limits the options available in solving the problem, however, modifications have now been made which should solve the problem.

The Reload Station.

The initial user interface proved to be technically orientated rather than suited to the public, as a result many hardware and software changes were implemented. The ability to change the language coding on user cards was later added and SSH communications software enhanced.

Wallets:

The case design for the wallet should be improved by strengthening the method of holding the two halves of the plastic case together. It is possible for the case to separate if dropped on the floor. Any changes would require a new plastic moulding and associated tooling which could not be completed within the timescale of the project.

Site Service Host:

The mirror account functionality added for the purposes of tracking transactions during the demonstration had to be improved and a more operator friendly interface had to be designed.

Clearing system

Changes were made to the correct the currency table operation and several alterations to the initialisation setting and key management to allow for more than one issuer.

Current status

All the technical issues identified in the matrix are resolved and all equipment is now operational. There is one area of uncertainty that remains concerning the long term reliability of the connection to the Fuji Cash register in canteens. Every other part of the system has been running with confidence for several months.

Because the operational difficulties have been resolved we are now ready to increase the level of activity of the trial and will be introducing the commercial sponsor and greater promotion.

6.2.2 System acceptance test specification

It became apparent that more formal methods of testing the various parts of the system were required and a significant amount of effort was put into preparing test schedules that could be used to measure system performance.

The following text in italics outlines an example of the contents list, equipment list and two test schedules from the system acceptance tests.

Contents:

1	<i>Introduction.....</i>	1
	<i>1.2 Scope of trial:.....</i>	1
2	<i>Equipment required.....</i>	2
	<i>2.1 Test cards.....</i>	2
	<i>2.2 Wallets.....</i>	3
	<i>2.3 Other types of card.....</i>	3
	<i>2.4 Simulated deposit files.....</i>	3
3	<i>Assumptions and rules for carrying out the tests.....</i>	4
4	<i>Associated documentation.....</i>	4
5	<i>Language tests.....</i>	4
6	<i>The test schedules.....</i>	4
	<i>The financial transaction terminal.....</i>	5
	<i>1 Normal card operation at a point of sale.....</i>	6
	<i>2 Insufficient funds at a point of sale followed by cash payment.....</i>	7
	<i>3 Insufficient funds at a point of sale followed by card payment.....</i>	8
	<i>4 Insufficient BEF then swaps to ECU.....</i>	10
	<i>5 No card inserted annul transaction.....</i>	11
	<i>6 Card negative file.....</i>	12
	<i>7 FTT out of paper (FTT continues to operate).....</i>	14
	<i>8 FTT paper jam (FTT will continue to operate).....</i>	15
	<i>9 Cards inserted incorrectly before a transaction.....</i>	16
	<i>10 Cards inserted incorrectly.....</i>	18
	<i>11 Card with value but no cheques.....</i>	20
	<i>12 Card with expired cheques.....</i>	21
	<i>13 Card with incorrect cryptography.....</i>	22
	<i>14 Card removed early and replaced out of sequence.....</i>	23
	<i>15 FTT power interruption.....</i>	25
	<i>16 Normal operation at a POS wallet turned on whilst pointed at link.....</i>	27
	<i>17 Normal operation at POS wallet turned on prior to pointing at link.....</i>	29
	<i>18 Normal operation at a POS wallet turned on to view balance prior to pointing at link.....</i>	31
	<i>19 Insufficient funds with wallet at a point of sale followed by cash payment.....</i>	33
	<i>20 Insufficient BEF in wallet then swaps to ECU.....</i>	35
	<i>21 No Wallet payment annul transaction.....</i>	37
	<i>22 Card in wallet on negative file.....</i>	38
	<i>23 Interrupted wallet communications at a point of sale, sale continues.....</i>	40
	<i>24 Interrupted wallet communications at a point of sale, with card recovery.....</i>	42
	<i>25 Incorrect wallet use at a point of sale.....</i>	45
	<i>The reload station.....</i>	47
	<i>26 Card withdrawal of home currency at a reload station (RLS).....</i>	48
	<i>27 Card withdrawal of home currency at an RLS Insufficient funds available.....</i>	50
	<i>28 Card withdrawal of ECU at an (RLS).....</i>	52
	<i>29 Card withdrawal attempt for unavailable currency at an RLS.....</i>	54
	<i>31 PIN change operation at an RLS new PIN not confirmed.....</i>	58
	<i>32 Card Balance review at an (RLS).....</i>	61
	<i>33 Card deposit operation at an RLS.....</i>	62

34	Card deposit attempt with invalid cheques at an RLS.....	64
35	Card withdrawal zero value but cheques topped up at an RLS	66
36	Card removed during verification at an RLS.....	68
37	Card removed during cheque reload at an RLS	70
38	Cards inserted incorrectly at an RLS.....	72
39	Accidental misuse of buttons at an RLS	74
40	Power interrupt during verification at an RLS.....	75
41	Power interrupt during cheque reload at an RLS	77
42	Communications interrupt during verification at an RLS.....	79
43	Communications interrupt during cheque reload at an RLS.....	81
44	PIN change operation at an RLS Independent of the SSH	83
45	Card Balance review at an RLS independent of SSH.....	86
	The Two button wallet	87
46	Xchange card type A reading	88
47	Xchange card type B reading	88
48	Xchange card type C, D, E, F reading	89
49	Messages versus language coding on the card	90
50	Xchange card type G reading	91
51	No card inserted in the TB-wallet	91
52	Card errors in the TB-wallet.....	92
53	Low batteries testing	93
54	Card pulled out whilst balance reading	94
55	2 buttons pressed together.....	95
56	Blank card reading	95
	The Vending Machine interface	96
57	Simple card based purchase in BEF	97
58	3 successive purchases in BEF	98
59	Simple card based purchase in XEU.....	99
60	3 successive card based purchases in XEU.....	100
61	1st purchase in BEF and 2nd purchase in XEU	101
62	1st purchase in BEF and insufficient funds for 2nd purchase	102
63	1st purchase in XEU and insufficient funds for 2nd purchase	103
64	Simple payment rejected (insufficient funds)	104
65	Simple payment rejected (out of cheques).....	105
66	Simple payment rejected (cheques expired).....	106
67	Simple payment rejected (invalid signature).....	107
68	double payment rejected (double spending).....	108
69	Card on hot file	109
70	Card removed during payment	110
71	Card replaced during payment	111
72	card errors	112
73	Undefined currency rate on VM.....	113
74	Coins inserted whilst card present.....	114
75	Card inserted whilst coins present.....	115
	The Personalization station	116
76	Card personalization	117
77	Card re-personalization (PIN unblocking).....	118
78	Card pulled out early.....	119
79	Wrong card personalization.....	120
80	Connector unplugged during personalization	121
81	PC powered off during personalization	122
	Appendicies	123
A1	Messages versus language coding on the card.....	124
A2	Glossary of FTT display message translations	125

1 Introduction

This specification describes a series of acceptance tests to be performed on the Xchange card demonstration system at the CEC in Brussels. The tests shall be carried out and must be successfully completed prior to launching the system for general use by employees of the commission.

The tests shall be carried out by members of the CAFE project team in conjunction with members of the CEC.

The tests described in this document are designed to check for correct operation of the system under both normal and exceptional usage conditions and to emulate as closely as possible the situation likely to be found when the demonstration is available for general use.

It must be stressed that the phase 0 of the demonstration is a pilot phase to test the CAFE project technology and is the precursor to launching the demonstration on a broader base. It must be realised that there are substantial technical innovations being introduced in phase 0 of this demonstration and it is likely that as the trial progresses new problems and possible enhancements will be identified. As a consequence this schedule may have to be revised periodically.

1.1 Technical innovations being introduced

- * *The use of smart cards carrying advanced cryptographic processors.*
- * *A multi-currency electronic purse with the ECU as the base.*
- * *The Clearing of signature transporting transactions between multi-issuers and multi-service providers.*
- * *The handling of loss and fault tolerant processes for purse schemes.*
- * *The use of electronic wallets with contactless infra-red point and pay features.*

1.2 Scope of trial:

The trial takes place using a small number of cards at first, in one building of the European Commission in Brussels, namely Beaulieu. Shortly afterwards it will (subject to successful operation at Beaulieu) be expanded to a second building, Breydel. The card will be accepted as payment for canteen meals, coffee shop purchases and snacks/drinks from vending machines located in the two buildings. It will be possible to load the cards at the CAFE project help desk in each building. The help desks will be manned throughout the trial during lunch periods and enquiries may be made by telephone during normal working hours. As the trial progresses electronic wallets will be introduced as "point and pay" devices in addition to the cards.

1.3 Beaulieu Equipment Summary (the first site)

	Clearing computer (CC)	Site host (SSH)	Reload station (RLS)	Hand held device	Merc-hant term	Trans-action term (FTT)	Vending interfaces (VMI)	wal-lets	Cards
Coffee Shop						1			
Canteen						2			
Vending							2		
Project office	1	1	1	1	1				
Total	1	1	1	1	1	3	2	25	250

The above technical innovations, scope of trial and equipment summary sections highlight the core technologies, services and devices covered by this specification.

2 Equipment required

In order to carry out the test schedules described in this specification the following equipment is required:

2.1 Test cards

Test cards form the basis of many of the tests scheduled in section 4. Standard Xchange cards shall be used encoded in different groups as follows.

Five test cards type A	Cards coded with 1,000-2,000 Belgian Francs (BEF), and no other currency.
Five test cards type B	Cards coded with 0 BEF and no other currency
Five test cards type C	Cards coded with 100 BEF and 10-20 ECU
Two test cards type D	Cards coded as type C but loaded with incorrectly signed cheque blanks.
Two test cards type E	Cards coded as type C but loaded with expired cheques
Two test cards type F	Cards coded as type C but with no cheques left
Two test cards type G	Cards coded as type A but with "magic tape" covering 5v pin on card contact pad area.
Two test cards type H	Cards coded as type C set on negative card file at clearing computer
Two test cards type J	Cards coded as type C but with French as language code
Two test cards type K	Cards coded as type C but with Dutch as language code
Two test cards type L	Cards coded as type C but with French as language code
Two test cards type M	Cards personalised but containing no currencies

All Xchange cards carry a unique visual and electronic serial number which is noted when required in the test schedules. This data is used as part of the tests of the acquiring and clearing functions. In addition all cards are initially coded with PIN 1234 and all cards type A-H inclusive are language coded for English.

2.2 Wallets

The two button wallet is used extensively during the test as an aid to monitoring the state of each test card. When used as test equipment the wallet is assumed to be functioning correctly, if the information displayed is incorrect then double check this against a test card type C or another wallet or information provided by the reload station. When the wallet itself is under test then follow the test schedule for the wallet.

A minimum of two reference wallets shall be available for use during the tests.

2.3 Other types of card

The card interface to the FTT, VMI and reload stations in the demonstration conforms to ISO standards. But shall only accept Xchange cards and not cause damage to other cards or itself suffer from damage or lock up conditions if other types of card are inserted. In order to test this further test cards are needed.

Two test cards type 1	Magnetic stripe cards coded in accordance with the 7810, 7811 series of ISO standards (any VISA / MasterCard etc will suffice)
Two test cards type 2	Asynchronous smart cards coded in accordance with the 7816 series of ISO standards (A French bank (GCB) card will suffice).
Two test cards type 3	Synchronous chip cards coded in accordance with the 7816 series of ISO standards (A Dutch PTT card will suffice)

2.4 Simulated deposit files

Testing of the collection and processing of deposit files shall be carried out in conjunction with transaction data created during the scheduled tests. In addition a number of routine repetitive tests shall be carried out with known deposit files of the following characteristics.

File type A	A file containing fully compliant data simulating deposits from all POS and vending machines.
File type B	A file containing fully compliant data simulating deposits from all POS and vending machines but with additional valid files from merchant terminals not yet installed.
File type C	A file as in type A but where some deposits have invalid digital signatures.
File type D	A file as in type A but where some deposits are duplicated.
File type E	A file as in type A but where some deposits carry expired cheque blanks.

3 Assumptions and rules for carrying out the tests.

The structure of the test schedule described in section 4 is such that each group of tests that relate to a particular function are identified as a sub heading number (Z.N) under the main heading number for that function (Z) (ie 1.1 is a test carried out of the function described in test schedule heading No 1). Tests shall be carried out in the order they are listed (ie 1.1 before 1.2 etc) functions may be tested in any order (ie 3 before 1) unless pre conditions are stated in the main heading of the function.

Each sub heading line entry dictates an action and shows the expected response. Providing the test conditions have been

complied with fully and the response indicated is as expected then the tester shall mark a ✓ in the "✓/X" column of the schedule if not then mark a X.

Where values are requested then these shall be entered in the "Values" column of the test schedule. The values requested may or may not be relevant to the test being carried out but may be used as input data to other tests. Where the test schedule shows the ✓/X or values columns as shaded then no response is expected from the tester.

Each test is intended to be self contained and shall not, unless otherwise stated as pre conditions depend on the outcome of previous tests.

Whenever a failure is discovered then testing of that function shall be discontinued.

The tester responsible for the tests shall indicate their name and the date and time of the tests in the schedule.

4 Associated documentation

The documentation available during the running of the demonstration shall be as follows:

*User instructions, cards and wallets
Conditions of use of the card
Service provider operator instructions
Instructions for help desk personnel*

5 Language tests

The Xchange card carries a code that can be set during personalisation to one of four languages, English, French, Dutch and German. Test cards of type C are provided and may be substituted for English language test cards wherever type C cards are used in the test schedules.

Separate schedules are not included for each language but a glossary of display messages referenced to the English language messages used in the schedules is included as an appendix to this specification and may be used as appropriate in checking multilingual operation.

6 The test schedules

Details of each test are given in the tables in this section of this document.

for example for this report only the first two test for the financial transaction terminal are included as follows

CAFE PROJECT

1	Normal card operation at a point of sale	FTT displays in <i>Italics</i>	Comments	Values	✓ ✕
1.1	Use reference wallet to view opening balance of type A card and record serial number and balance	<i>XCHANGE DATE TIME</i>			
1.2	Cashier enters amount less than card balance on cash register as normal then presses Card Payment button. Record value of XXX	<i>XCHANGE AMNT= XXX</i>			
1.3	Insert the type A test card	<i>BEF YYY PLEASE WAIT</i>			
1.4	Record value of YYY	YYY should = XXX			
1.5		<i>PROCESSED REMOVE CARD</i>			
1.6		FTT and cash register receipt printed			
1.7	Remove test card A	<i>XCHANGE DATE TIME</i>			
1.8	View and retain FTT receipt record transaction value	Transaction value should = XXX			
1.9	View and retain Cash register receipt record transaction value	Transaction value should = XXX			
1.10	Use reference wallet to view closing card balance and record	Check closing balance + XXX = opening balance			

CAFE PROJECT

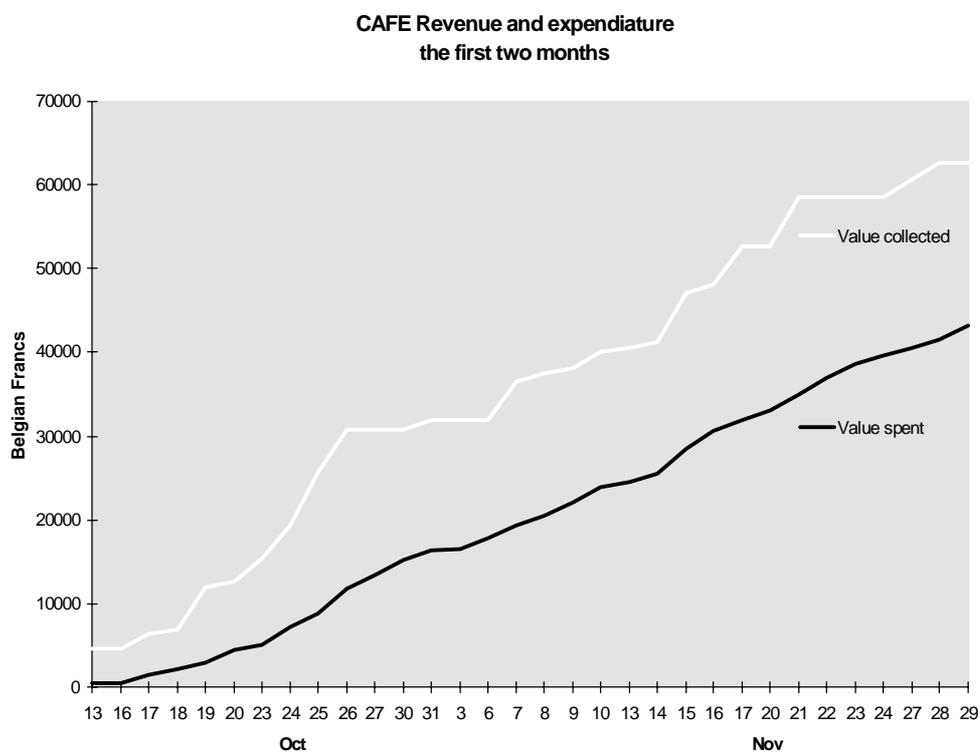
2	Insufficient funds at a point of sale followed by cash payment	Ftt displays in <i>italics</i>	Comments	Values	✓ ✗
2.1	Use reference wallet to view opening balance of type B card record serial number and balance (should be zero)	<i>XCHANGE DATE TIME</i>			
2.2	Cashier enters small amount on cash register as normal then presses Card Payment button Record value of XXX	<i>XCHANGE AMNT= XXX</i>			
2.3	Insert the type B test card	<i>EMPTY CURRENCY CANCELLED REMOVE CARD</i>			
2.4	Remove card	<i>XCHANGE DATE TIME</i>			
2.5		Cash register displays carte refusee			
2.6	Cashier then presses clear button on cash register	Cash register displays a pay XXX			
2.7	Cashier then presses cash button	Cash register clears and prints cash receipt			
2.8	View and retain cash register receipt record transaction value	Transaction value should = XXX			
2.9	Use reference wallet to view closing card balance	Check closing balance = 0			

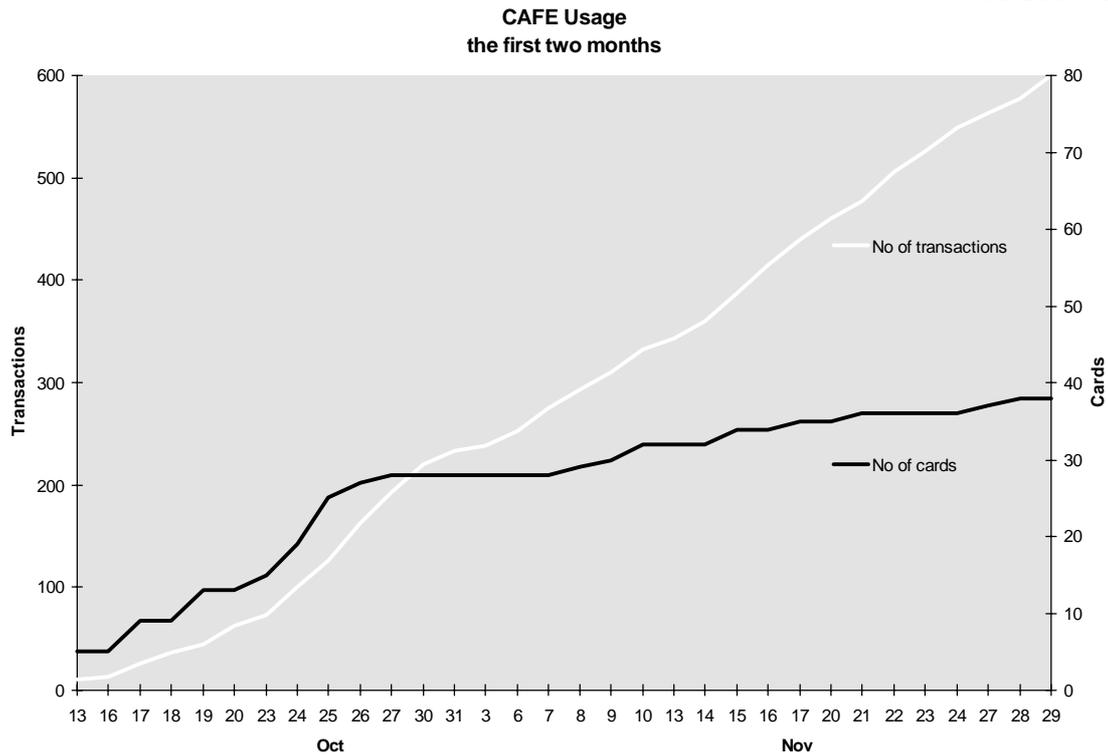
6.3 Initial running

During October the system went into operation for 20 - 30 selected card-holders. Initial reactions from the canteen service provider was that the system appeared to be slow. In fact when timed the CAFE transaction compared favourably with a cash purchase where change was involved.

The very nature of the coffee shop operation demands a rapid payment process which is not ideally suited to any slot based pre-pay device, further tests using the infra red wallets may prove to be suitable for speeding up the payment transaction.

The following charts show the initial take up and usage of the Xchange card.





It was during this initial period that the following user surveys were carried out.

6.4 Xchange Card Survey results

All interviews were recorded on tape using the questionnaire (see Appendix 1). Interviews were made by native Belgian interviewers who have a good knowledge of French, Flemish, German and English. All respondents work in the Beaulieu building of the CEC and were given an Xchange card. Two types of respondents were selected from the CAFE database:

- 1 Respondents who use the card relatively often and have, if possible, reloading experience.
- 2 Respondents who used the card and stopped using it. We refer to these persons as non-users.

We divided the questionnaire in two parts: the first part dealt with present card usage and technical issues, the second part was oriented towards possible acceptance and usage in the future. The interviews were made between Nov, 14th and December, 12th, 1995. We interviewed 12 people, 6 men and 6 women between the age from 25 until 55. The majority earn more than 100.000 BEF per month. Apart from one student all work full time. Two of them have stopped using the card. The following represents the most significant findings.

6.4.1 Present Card Usage

10 of the 12 respondents found their experience with the Xchange card positive. Two found it negative and stopped using their card. We refer to them as non-users. Most of the users (7) used their card at least once a day.

Electronic ECU

Of the 6 card users who loaded ECU 2 are professionally involved with European monetary

unification. The main reason for loading ECU was a positive attitude towards European unification. The 3 persons who loaded BEF from the beginning found it inconvenient to load ECU because the prices are always marked in BEF. Users had no special experiences with ECU. One person remarked that one still has to get used to counting in ECU. Another ECU-user mentioned the problem of converting BEF into ECU.

One of the non-users stated: "I don't see the point of this ECU dimension. ECU or BEF, it doesn't make any difference. It's actually more sensible to pay in BEF because all the prices are in BEF." Two respondents noticed the possible future usage of the Xchange card-system: "Een kaart voor alles en in ECU." ("One card for everything and in ECU.") "I would like to see it used internationally with ECU and for different purposes (tolls on the road)".

What Respondents Liked

"I don't have to carry around cash. I just put my card in my pocket. It's very easy, especially at the vending machines."

"My wallet is not as heavy as before."

"I do not have to use coins."

"You don't need to have change when the cafeteria is closed in the evening."

"I don't need my purse for purchases. It is easier to use the card, because you don't have to carry around your bag."

"Especially at the vending machines it's very practical. It's easier to invite people to drink a coffee."

"The convenience of knowing that I can always get food or drinks. Sometimes I forget my wallet but I leave my Xchange card at work, so I always have some money to get drinks with."

"It is safer than cash, you don't need to carry around so much cash."

According to the respondents, the main advantage is the convenience with regard to replacing coins.

What Respondents Disliked

Being asked for problems and what they do not like the card-users and non-users complained about the following issues:

Technical Problems

"The first two days that I went with my card to the restaurant, there were a few technical problems."

"Vending machines did not work (were blocked, didn't accept coins anymore)."

Not Enough Places to Use It

"It's not true that you don't need to carry a great deal of cash because the system is not widespread. You still need coins for other things, for example in the coca-cola machine." "There are not enough places where you can use the Xchange card in the building." "You can only use the card in few places, so you always have to handle the card and your purse (cash). In fact, it is more work now."

Reloading Office and Process

"It's not easy to load the money. You always have to go to the office. First you have to wait until it's loaded in the computer and then you still have to load your card." "Reloading station too slow." One non-user stated "not very practical, help desk not always available for charging card (opening hours). I

don't have much time, I want to have my card charged directly. In principle I have to go to my own bank first to get money, then I have to go to the CAFE-bank for to fill my account, then I have to charge my card, this is too time consuming."

"Recharging is time-consuming, especially when you have to deposit the money, you have to do that during special hours. You need to go there, when somebody is there."

Card Balance

"And it's very inconvenient if you go to lunch with some people and you have forgotten to reload your card ... I would like a warning if I'm under 300 francs."

"At the restaurant one cannot check the balance before using the card."

"Once I was standing in a queue and my card wasn't accepted because there was not enough money on it."

6.4.2 Integration Into a Bank Card

In this part we wanted to investigate the future acceptance of the Xchange card payment-system. For this purpose we asked the interviewees to imagine that the Xchange card had been integrated into their bank card and that they could pay with such a card in shops, restaurants, hotels, petrol-stations, etc. all over Europe. First we asked them about their card usage in everyday life: The cards that were used most frequently were Bancontact and Visa. Most of the users (8) withdraw cash at least 4 times per month with their bank card at a cash dispenser.

In respect of two main characteristics of the Xchange card payment-system, anonymity and electronic cash, the 10 card users stated the following:

Privacy

When asked how important they considered it to be that electronic transactions be kept anonymous most of the card-users (7) considered anonymity as an important matter, because they were afraid that information about a person could be collected for controlling-purposes, or that e.g. one could be bothered with advertisements which one does not want.

Loss Protection of Electronic Value

Respondents were asked what kind of protection against loss and theft of electronic value they would find convenient. Answers indicate that unlocking part of the money by using a PIN, as developed by the consortium, is the most promising way and should be explored further, as it was not tested in Beaulieu.

Electronic Value or Cash?

When asked if electronic value was just the same as cash for them, all users answered with yes. They want the card to substitute cash and prefer to live without cash. Most of the users (7) are convinced that payment systems with cards could replace payments with cash. Therefore, they couldn't imagine any situation where they would pay with cash. Nevertheless, three of the users are convinced that cash should not be replaced totally by cards and mentioned the following reasons: Cash should be kept as a kind of "back-up"-system, which one could use, when for some reason cards or terminals were out of order; another respondent felt that cash will always be necessary in life, e.g. money for beggars, flea-markets, payment between individuals, small purchases. One of them stated: "La carte est un progrès, mais elle ne justifie pas l'abolition de l'argent liquide" ("The card is progress but doesn't justify abolishing cash.")

Integration into Bank Card, Willingness to Pay

All of the users interviewed so far would like CAFE-money to be integrated into their bank card. Most were willing to pay 300 BEF for such a card, i.e. as much as they pay today. Only two were willing to pay 1,000 BEF.

Personal Data

Gender:	6 male	6 female
Age:	0/ 16 - 24 1/ 35 - 44 0/ 55 +	9/ 25 - 34 2/ 45 - 54 0 no answer
Marital status:	5 single	7 married/living as a couple
Number of children aged under 15 years in your household:	2 have one child	
Nationality:	1 Austrian, 3 Belgians, 2 British, 1 French, 4 Italians, 1 German.	

7 Technology cost assessment

This section summarises the following:

- Technical results against original objectives.
- Current item costs as for the CAFE project and estimated item costs if mass produced.

7.1 Assessment of technical achievements against objectives

DigiCash :

Objectives :

- A) Develop the mask (software) for the chip used in the Xchange cards
- B) Manufacture and install 3 Interfaces for Vending Machines with the Xchange cards

Results :

- A) Complete
- B) Complete

Gemplus :

Objectives :

- A) Manufacture 400 Xchange cards with the Siemens chips
- B) Develop, manufacture and install 25 Two-Button Wallets
- C) Develop, manufacture and install 30 Full-Wallets

Results :

- A) Complete
- B) Complete
- C) Complete

Ingenico :

Objectives :

- A) Develop, manufacture and install 10 POS terminal adaptation to the Xchange card
- B) Manufacture 10 Crypto modules for POS and 25 Infrared boards

Results :

- A) Developments complete
- B) Developments incomplete

Siemens :

Objectives :

Develop and manufacture the SLE44C200 chip for the Xchange card and the SLE44CP2 crypto coprocessor

Results : Complete

7.2 Current and estimated mass production costs

Card industrial manufacturing requires the mandatory following phases, some of them were skipped for CAFE, or were done in a simplified way.

Here are the main phases of an industrial card manufacturing process:

<u>Phase</u>	<u>Output Information</u>	<u>partner</u>	<u>Status for CAFE</u>
Card O/S development	mask code	DIGICASH	done
Mask generation		SIEMENS	done
Wafer manufacture	Product description : -Chip identification code, -Code location on the chip, -Bonding diagram	SIEMENS	Not 100% done
Wafer testing	Test flowchart : -Type of operations -State of the tested chip (virgin/altered) -Transport code -Outgoing specification	SIEMENS	Percentage of testing unknown
Wafers reception	Control report	GEMPLUS	done
Module assembling	Qualification of the SLE44C200 chip embedding	GEMPLUS	
Module testing (by sampling)	-Open/short test report -Yield obtained	GEMPLUS	done
Chip embedding		GEMPLUS	done
Card personalisation Software		GEMPLUS	cards personalised by tools used for samples
Qualification Test Software		GEMPLUS	Impossible : unknown Operating System and Chip
Card personalisation		GEMPLUS	Cards manually personalised as engineering samples
Card Qualification : - assembly checking - memory mapping test - Answer to Reset with transport code	- Functional test specification - Functional test report - Final yield obtained	GEMPLUS	Card basic testing manually done with unknown software provided by DIGICASH (OK / Not OK)

The non conformance to these phases may account for the weak yield obtained for these cards, that is about 80% of cards when loaded with payments.

However given the sharing of the project phase among several partners and the purpose of the project i.e. research rather than business, it was impossible to follow strictly the standard rules listed above.

Possible improvements for mass production :

Substantial improvements on the final production yield would be obtained following the mass production rules.

Therefore this means for the card embedder to receive test scenario from the chip programmer or to get sufficient technical elements from the chip programmer to build these test scenario.

Thus extra costs for new production and test tool developments must be taken into account.

Besides, the 400 Xchange cards were made of non-varnished surface printed ABS. For mass production, the more suitable surface is PVC which is more resistant than ABS for frequent insertions, and which allows embossing and a wider range of colours for surface printing. Inconvenient : PVC is more expensive.

Card mass production price :

Price for CAFE : XEU 18,00 card :

This price must take into account the fact that the cards were processed by GEMPLUS as engineering samples : People in charge of them were a staff of Engineers rather than Technicians.

For mass production : the cost would be identical to that of a GEMPLUS classical MPCOS card used in the purse applications, if the price of the SIEMENS chip lowers in the same proportions :

Mass production Price : around XEU 5,00 / card for many thousands of cards.

SLE44C200 mass production price :

Price for CAFE	Price for 10k.units	Price for 100 k.units	Price for 1M.units
DM 7.63	DM 7.04	DM 7.04	DM 5.93

Possible improvements for mass production

Siemens have announced a new chip the SLE44CR80S that is a smaller die size yet has more memory capacity.

Point Of Sale Terminals :

Technical status

After many difficulties, the POS terminals now run the cryptographic verifications.

Another difficult point was to handle the cash register interface with the FUJI cash register.

Finally the error message handling took a long time to be rugged.

The Get-certificate part of the transaction protocol is not implemented.

The crypto modules for the POS terminals are not 100% delivered.

Possible improvements for mass production :

The POS terminal as such cannot be mass produced given the restrictions on the availability of the SLE44CP2 Dual In Line package coprocessor used in their cryptographic module.

The SIEMENS SLE44CP2 coprocessor is not available in large scale because of restrictions from the German Authorities. This is a serious issue : no such powerful coprocessor circuit is available on the market in a single chip. However this coprocessor is integrated in the SLE44C200 chip used for the Xchange card. So one solution is to replace it with a plugged-in chip module dedicated to crypto-computations :

inconvenient : Computation and communication speed are limited to that of a card chip (around 5 MHz against 14 MHz for the SLE44CP2 coprocessor) Thus a redesign must be made, using another SLE44C200 chip instead, and the subsequent software adaptations.

The Infrared module must be modified to benefit from the latest chips available integrating the low layers of communications in a single chip. Reduction of cost and volume and gain in communication robustness.

The POS device cost will be strongly dependant on the desired payment storage capacity conditioned by the size of the flash EEPROMs used. The EEPROM chip price is significant.

The product must be qualified to be allowed to show the now mandatory “CE” label on its case :

Functional and endurance testing : normal operation and exceptional operation

ElectroMagnetic Compatibility (EMC) : conformance to the following standards :

Emission reduction	NF EN 5008X
Reception immunity	CEI 100-4-3
Conduction immunity	CEI 1000-4-X
Conducted emissions	EN 55022
Electrostatic discharges	CEI 801-2

Mass production price :

Price for CAFE XEU 685	Price for 5k.units N/A	Price for 10 k.units N/A	Price for 50k units N/A
---------------------------	---------------------------	-----------------------------	----------------------------

NB: N/A means not available at time of compiling this report.

Wallets :

Technical status

The full wallets were supposed to run two protocols of transactions :

Alpha + : operations secured by Xchange card inserted in the wallet

Gamma : operations secured by cryptography imbedded in the wallet thanks to the SLE44CP2 coprocessor, the plugged-in Security Module (Observer) and the Gamma protocol of transactions.

The applications software required to run the Gamma protocol is coded but not activated because it was not fully implemented and tested with the other transaction terminals. Thus these wallets will run the Alpha + protocol for any financial operation.

The Two-Button wallets were delivered on December 12 1995.

The full wallets were delivered later.

The following suggestions and remarks are regarding the Gemplus Two-Button and Full-Wallets. These wallets are demonstrator prototypes that obviously need a re-design for large quantity production. Here are some aspects that could be investigated :

Possible improvements for mass production :

Improve the Infrared link robustness with the use of dedicated chips now available

Reduce dimensions and weight and power consumption :

By using more surface mounted components

By integrating functions in a single chip now available (Card interface, Infrared interface)

By using a 3 volt technology more suited to hand held devices

Strengthen the package :

By reducing their weight

by a case re-design

The product must be qualified to be allowed to show the now mandatory “CE” label on its case :

Functional and endurance testing : normal operation and exceptional operation

ElectroMagnetic Compatibility (EMC) :

conformance to the following standards :

Emission reduction NF EN 50 081 and 50 082

Reception immunity CEI 100-4-3

Electrostatic discharges CEI 801-2 / CEI 1000-4-2

Full-wallets :

The following suggestions and remarks are regarding the Gemplus full-wallets only :

Replace the SIEMENS SLE44CP2 coprocessor not available in large scale with a plugged-in chip module dedicated to crypto-computations :

Computation and communication speed would then unfortunately be limited to that of a card chip (around 5 MHz against 14 MHz for the SLE44CP2 coprocessor) as a consequence the wallet will be slowed in its operations.

Mass production price:

Price for CAFE : The following prices do not include the hardware and software development processes submitted during the project, it is the hardware cost price of items produced for the trial.

(Price charged for the extra order for the D9 extension to the CAFE project)

Two-Button wallet : XEU 158,00

Full-wallets : XEU 193,00

These wallet prices should be multiplied by a factor 2 to obtain the selling price to the public. Now one can hardly imagine the users would agree now on buying such devices XEU 380,00:

An acceptable public price is nearly 20 times less, i.e. XEU 15,00 per device!

Mass production targeted cost with a redesigned hardware :

Re-designed CAFE full-wallet estimated quotation (in XEU) :

Component	Price / 10k units	Price / 100k units	Price / 1M units
8 bit microcontroller	7.2	6.95	6.66
Nonvolatile memory (500Kbytes*8)	8.4	7.56	6.8
RAM (32Kbytes*8)	2.4	2.15	1.93
LCD unit display + drivers	4.34	4.05	3.62
Keyboard	1.44	1.0	0.86
Card Interface driver + connector	1.15	1.0	0.86
2 SAM's driver + connector	2.3	2.0	1.72
2 * SLE44C200 Observer + crypto	7.6	7.6	6.4
Infra red interface	3.6	3.3	3.18
Printed Circuit Board	2.17	1.88	1.44
Plastic case	2.89	2.6	2.17
Transistors, resistors, capacitors...	2.0	1.8	1.6
Lithium batteries + connector	0.6	0.5	0.45
Total	46.09	42.39	37.69

These figures are not a GEMPLUS commitment for a new wallet production.

The purpose of the table above is to list the minimum hardware components required for a low cost mass production CAFE full-wallet and to estimate the price obtained.

The cost obtained here around XEU 38,00 is still incompatible with an acceptable public price.

As a conclusion the CAFE wallet is expensive because of the complexity of the transaction protocols.

Vending Machines :

Technical status

This item is provided by DIGICASH.

No technical specification is available about its functioning. For further details, please contact DIGICASH.

Price for CAFE
XEU 1085,00

Mass production price

N/A from DIGICASH

Appendix 1 Semi-Standardized Questionnaire for the Xchange Card

Interview No.:

Date:

Requirements:

1. *two pens (for interviewer and respondent)*
2. *tape recorder*
3. *tapes (new tape for each respondent, record each interview completely)*
4. *microphone*
5. *batteries*
6. *business cards, user manual, booklet, simulation*

I work for the Institute for Social Research in Frankfurt, Germany, which is participating in the ESPRIT PROJECT called CAFE. This scientific project is developing new payment technologies. We would like to ask you some questions about the use of the Xchange card. Your answers will be treated confidentially and will be evaluated anonymously in our institute in Frankfurt, Germany. First I would like to talk to you about the use of the Xchange card on the premises of the CEC.

1 Do you have an Xchange card ?

yes no

If no: Please tell us why not:

.....

If yes: How long do you have this card:

.....

2 Have you ever used your Xchange card at all since you initially received it?

- yes, very often
- only a few times, but I will continue to use it
- only a few times, I stopped using it
- no, not at all

If no, not at all: Why don't you use the Xchange card ?

.....

If no, not at all: please give non-users sheet with personal data.

With users or former users, next question:

3 On the whole, has your experience with the Xchange card been positive or negative?

rather positive rather negative

Why?

.....

4 How often did you use the Xchange card per week?

.... times per week

4.a. How often per week did you eat in the restaurant?

.... times per week

4.b. How often per week did you use the vending machines?

.... times per week

5 How satisfied were you with the type of information provided to you before you used your Xchange card ?

- very satisfied
- fairly satisfied
- dissatisfied
- fairly dissatisfied
- very dissatisfied

6 How many times have you reloaded your Xchange card ?

- every day
- 2-3 times per week
- once a week
- once every two weeks
- less often
- never
- don't know

Please hand next sheet to respondent

7 How easy did you find the process of reloading the Xchange card?

- very simple
- quite straightforward
- difficult in places
- hard to use
- too complicated

8 Have you ever used the Xchange card at the vending machine?

- yes
- no (*if no, skip next question*)
- don't know

9 How easy do you find the Xchange card to use for payments at the vending-machine?

- very simple
- quite straightforward
- difficult in places
- hard to use
- too complicated

10 Have you ever used the Xchange card at the restaurant?

- yes
- no (*if no, skip next question*)
- don't know

11 How easy do you find the Xchange card to use for payments at the restaurant?

- very simple
- quite straightforward
- difficult in places
- hard to use
- too complicated

12 Have you ever used the Xchange card at the coffee-shop?

- yes
- no (*if no, skip next question*)
- don't know

13 How easy do you find the Xchange card to use for payments at the coffee-shop?

- very simple
- quite straightforward
- difficult in places
- hard to use
- too complicated

Please give sheet back to interviewer

14 Have you experienced any problems at all in using the Xchange card-system?

yes no

If yes, please describe these problems and indicate how often they occurred.

	Once	Twice	3 or more
card became damaged by the?			
vending-machine	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
cashier	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
reloading station	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
card "locked" or retained by the?			
vending-machine	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
cashier	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
reloading station	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
difficulties changing PIN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
not enough money on my card (please explain).....	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
other:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

15 We would now like to talk to you about the currencies that could be loaded into the Xchange card. First please tell us, in which currency you get your salary?

Bfr. ECU Bfr. + ECU other

16 With which currency did you initially load your Xchange card?

Bfr. ECU both

17 Why did you load the above marked currency?

.....

18 If applicable: Have you ever loaded ECU since then?

.....

19 If ECU ever loaded: Which experiences have you made with it?

.....

How high is the balance on your Xchange card at the moment?

Bef:

ECU:

20 What do you like about the Xchange card?

please let the respondent answer spontaneously

.....

Then give him or her the next sheet:

What do you like about the Xchange card?

I like using the Xchange card because	yes, this is why I like it	no, this is not important for me
... I don't need to carry a great deal of cash around with me		
... I don't need to have the correct amount of coins		
... I don't have to wait for the correct change ...Payment with Xchange card is quicker than with cash		
Other reasons:		

Please give sheet back to interviewer

21 Is there anything you dislike about the Xchange card?

yes no

If yes, give him or her the next table to complete having answered.

If no, skip the table and go to 22.

Is there anything you dislike about the Xchange Card?

I do not like using the Xchange card because	yes, this is why I do not like it	no, this is not important for me
... there are not enough places where I can use it		
... terminals or vending machines were often out of order		
... the reloading station is not in a convenient location / too often closed		
... it is difficult to keep in mind the balance		
... I can't correct a wrong amount of money after having paid:		
... payment is too slow		
... loading is too slow		
because		

Please give sheet back to interviewer

22 Your "carte de service" could be integrated in the Xchange card. Do you consider this as desirable?

- yes no

23 Have you ever used a Girovend card?

- yes
 no

If respondent marks "yes" please hand him the section on the Girovend card

For Girovend-users only

How often have you used your Girovend-card ?

..... times per week

Have you had any problems with your Girovend-card ?

- yes no

If yes: Please tell us which ones:

.....

Which card-system do you prefer ?

- Girovend Xchange card

Why ?

.....

please give sheet back to interviewer

Now please imagine the Xchange card chip would be integrated into your favourite bank card. You would then have electronic money in it. We would now like to talk to you about, how exactly such a system should work and which characteristics the electronic money should have. When you tell us your opinion about certain issues, please imagine that you pay with electronic cash everywhere in Europe. All supermarkets, gasoline stations, hotels, vending machines etc. could be equipped with new terminals.

(Remark for interviewer: chip-card-readers are very simple and not expensive)

24 Now thinking about the different ways of paying for goods and services in shops, restaurants, etc. which if any of the following bank, credit, debit or telephone cards do you currently have?

Bank Cards:

- Bancontact
- Visa
- Eurocard/MasterCard
- Eurocheque
- American Express
- Diners Club
- Other bank or credit cards (please specify):

Telephone Cards:

- Belgacom
- Other telephone cards (please specify):

25 Which card do you use most frequently?

.....

26 How many times per month do you withdraw cash with it at a cash dispenser?

..... times per month

27 How many times per month do you pay with it at the point of sale, such as at a petrol station, in a supermarket or in a restaurant?

..... times per month

28 Where would you like to be able to reload your Xchange card ?

- bank cash dispenser
- cash points
- at home over the telephone
- at work over the telephone
- all the above
- don't know

29 Personal data arising from card transactions are currently stored in data banks. With our system this is no longer the case in the future. Would it be important for you that electronic transactions be kept anonymous, just as cash transactions now are?

- very important
- important
- less important
- unimportant

Why?

.....

30 Electronic money can be lost or stolen. A PIN-code would be a protection but it brings along also some inconveniences (e.g. payments could be slower). In the following PIN-code options you find descriptions of their advantages and disadvantages.

hand over next sheet to respondent

Imagine that you have to choose between the three following options for PIN-codes and protection against loss and theft of electronic money:

- (1) You would have to key in your PIN for every payment. This option protects the whole amount of money on your bank card against loss or theft. You could run the (very small) risk that someone could spot your PIN-code and steal your card at the same time.
- (2) You could lock and unlock all the electronic money in your card. This option requires you to relock the card after every release of money, if you want to have your money protected.
- (3) You could unlock a certain amount of money. For purchases you would not have to type in your PIN. The rest of the money would still be locked in your card.

Would you appreciate such a kind of protection or would you find it inconvenient?

appreciate

inconvenient

- option 1
- option 2
- option 3

- option 1
- option 2
- option 3

Please give sheet back to interviewer

Why?

.....

31 Electronic value is stored in your card: Is this value just the same as cash for you?

- yes
- no

If yes: Why is this electronic value the same as cash for you?

.....

If no: What makes it different from cash?

.....

32 With the above described card you could pay at all vending machines, shops, etc., as explained. In principle, this would make cash superfluous. Would you still want to pay with cash?

- yes
- no
- I don't know

Why?

.....

33 If yes: In which situations would you still want to use cash?

.....

34 Imagine that you had a card with all the above marked qualities, this is PIN-protection and privacy as you like it. Would you use such a card-system as we just discussed it?

- yes
- no

Why?

.....

35 How much would you be willing to pay for such a card annually?:

-
- nothing

If respondent says "nothing": Would you be prepared to pay 300 Bfrs. annually?

- yes
- no

hand over next sheet to respondent

Personal data

Gender: male female

Age: 16 - 24 25 - 34
 35 - 44 45 - 54
 55 + no answer

Marital status: single married/living as a couple
 widowed divorced
 separated no answer

Number of children aged under 15 years in your household

Nationality:

What is your highest educational qualification?

Which profession did you learn?

What is your actual job at the Commission?

Which of these best describes your employment at the moment: working full-time in paid job
 working part-time in a paid job
 self employed
 student
 other

Monthly personal income: 25.000 Bfr. - 50.000 Bfr.
 50.000 Bfr. - 75.000 Bfr.
 75.000 Bfr. - 100.000 Bfr.
 more than 100.000 Bfr.
 no answer

Would you allow us to have another interview with you in the next 3 months ?

yes no

If yes, please give us your name and telephone-number of your office:

Name:.....

Extension:

Thank you very much