

**A chip card architecture for
integrated retail systems**

MANAGEMENT SUMMARY

Objectives

This paper defines the requirements for multiple retailers seeking to integrate the processing of chip cards (smart cards) for payment and other applications into point of sale systems. It identifies a common architecture which allows integration of multiple smart card applications into retail systems, and which offers the flexibility required in this fast-moving field.

It is aimed at a broad cross section of readership, including:

- A broader spectrum of retail than that directly concerned in producing this paper;
- The banking community in general, including card schemes, APACS, acquirers and issuers;
- The supply industry: EPOS and EFT suppliers, the smart card and security industries.

The Opportunity

Smart cards are now becoming widely adopted in various industries and applications. Recent developments in card technology, including a 100% increase in bank card counterfeit fraud in 1996-97, have made it clear that smart cards will progressively during the next few years replace magnetic stripe cards for applications such as:

- bank credit/debit cards;
- electronic purses;
- building access control and computer system access.

In the UK, banks are engaged on several large-scale pilot projects and are now expected to start rolling these out during 1998. The cards also have advantages for applications such as customer loyalty and staff schemes, and some retailers are already using them to add value in other areas. Planning for smart card handling at the point of sale should not now be delayed, since external circumstances will in due course mandate the use of the chip.

The main standards for chip cards are now well-established and the most likely pattern for multi-application chip card acceptance is becoming clear. This allows investment in hardware and basic software, provided that the necessary interfaces to other systems are defined and that other functions can be provided in software.

Business and operational requirements

The paper considers retailers' underlying business and operational requirements for card acceptance, including both those which are carried over from current magstripe card handling and those which are introduced by the use of smart cards. A primary concern is to maintain the integrity and security of existing business processes and to maintain or improve the customer interface at the point of sale. Any new procedures introduced must be simple for both cardholders and staff.

For most retailers, acceptance of bank debit and credit cards will be the first requirement, but the architecture must allow seamless migration to other applications such as loyalty and electronic purse, using a single Card Accepting Device at each point of sale.

Structure and architecture

Sections 1-3 of this paper cover the current developments and the resulting retailer requirements in the introduction of smart cards. Section 4 outlines the Point of Sale architecture that is considered to be a requirement for major retailers. This section describes an architecture where all cards are accepted through a common Card Accepting Device which has a minimal “thin client” functionality for acceptance of all cards, with the other card application requirements “layered” across the retail system.

The architecture proposed divides the functions to be performed into a number of “services”. Each service can be implemented in any hardware or software form, although one of the advantages of the architecture is that only the lowest level functions need be performed in a separate Card Accepting Device; all the other functions can in principle be implemented in software, and at any point in the retailer’s network. This allows each retailer or supplier to map the smart card extensions onto existing retail systems.

There should be a defined interface between each of the services; although the definition of these interfaces is beyond the scope of this paper, some principles are proposed and a range of open standards and specifications which could be applied is given.

This model differs substantially from that envisaged by the card schemes and on offer from major EFT terminal manufacturers:

- It can be mapped on to any EPOS architecture
- Applications need not be resident in the Card Accepting Device
- Security Modules and Merchant Purses may be located at any point in the network, to match the retailer's infrastructure
- Type approval must be modular; approval of Card Accepting Devices must not be application-specific;
- The architecture will support the introduction of new applications, including non-banking applications.

The Future

The introduction of smart cards offers an opportunity to introduce more objective and accurate Cardholder Verification Methods, to replace the subjective signature inspection. The architecture and procedures should make provision for this change. Operators of unattended terminals, customer kiosks and unattended checkouts will be among the main beneficiaries of an objective CVM. It is considered that currently the only widely available technology is PIN but this paper calls for the banking industry to give a clear direction with a planned timescale.

Smart cards introduce several new functions to the EPOS system, and the requirement for flexibility demands that they and the existing functions be implemented in a modular way, using published “open” standards where possible. Any generalised solution must be applicable to older point of sale hardware as well as the current and future generations, and must allow migration from a single application (such as credit/debit or electronic purse) to multiple applications.

By the use of this architecture, retailers and suppliers may develop solutions which meet today’s requirements for chip card processing and which can be extended to meet all currently envisaged future developments.

Recommendations

The key recommendations are:

- Card reader and EFT terminal suppliers should consider making their architectures more modular and more suitable for network implementation. Software suppliers may have to provide additional interfaces.
- Card schemes should reconsider their type approval requirements to reflect the cross-industry nature of chip card applications.
- Retailers implementing chip card schemes or accepting card payments under current bank initiatives should support this architecture now in order to permit suppliers to develop products to meet their long term requirements.

LIST OF MEMBERS

Participants in the Joint Retailer-Supplier Forum were:

Peter Bone*	Dixons Group
Nick Bradshaw	Shell UK
Ian Chandler*	ICL Retail
Rod Ewing	Tesco
Paul Gillingwater*	IBM
Mike Hendry*	Consultant
David Martin*	J Sainsbury
Phil Mitchell	British Retail Consortium (Chairman)
John Owen*	Dixons Group
Simon Palinkas	Tesco
Nick Parpotta	Marks & Spencer
Simon Pressley	IBM
Simon Robinson	NCR
John Smith	J Sainsbury
Steve Turner	Retail Logic

* denotes member of drafting group.

TABLE OF CONTENTS

1.	Introduction	1
1.1	Background	1
1.2	Objective	1
1.3	Scope	2
2.	Market developments	2
2.1	Traditional technology	2
2.2	Current developments	2
2.2.1	Applications	2
2.2.2	Terminal developments	3
2.3	Anticipated developments	3
2.3.1	Technology	3
2.3.2	Applications	4
2.4	Critical assumptions	4
3.	Chip card handling requirements in multiple retailers	4
3.1	Business requirement	4
3.2	Operational requirements	5
3.2.1	General	5
3.2.2	Readers	5
3.2.3	Chip and magstripe on the same card	6
3.3	Functional requirements	6
3.3.1	Principles	6
3.3.2	New functions	7
3.3.3	Cardholder verification	7
3.3.4	Backwards compatibility	7
3.3.5	Security	8
4.	Architecture	9
4.1	Rationale	9
4.2	Framework	9
4.2.1	Card transport	10
4.2.2	Protocol conversion	10
4.2.3	CAD display / keypad handling	10
4.2.4	Card authentication and application selection	10
4.2.5	Application authentication	11
4.2.6	Application logic	11
4.2.7	Common functions	11
4.2.8	Point of service logic	11
4.2.9	Storage of value	12
4.2.10	Business logic	12
4.2.11	Logging and recovery	12
4.2.12	Host communications	13
4.2.13	Application control	13
4.3	Cards	13
4.4	Card accepting device	13
4.5	Point of service device	14
4.6	Back office / head office systems	15
4.7	Impact of other standards	15
4.8	Equipment certification and bank approvals	15

5. Interfaces	15
6. Summary	16
APPENDICES:	
A: Standards	16
B: Glossary.....	18
C: Details of current chip card schemes	19
D: Issues for resolution	21

1. Introduction

The production of this paper is the result of various activities by the British Retail Consortium, major retailers and their EPOS suppliers. The BRC has chaired a Joint Retailer Supplier Forum to identify the real requirements of large retailers with networked EPOS store environments in the implementation of multiple Integrated Circuit Card (ICC) applications at Point of Sale.

1.1 Background

Use of smart cards (ICCs) is now becoming widespread internationally in many different industries. In payment systems the international card schemes: Europay, MasterCard and Visa (EMV), have created specifications for the use of smart cards in credit and debit systems and in addition electronic purse (stored value) schemes are being implemented in many countries.

The UK banks are planning to introduce ICC both for debit and credit cards, via the APACS ICC Project initiative and for Electronic Purses, including Mondex and Visa Cash. (These developments are outlined in more detail in Appendix C).

The card schemes have defined the standards required for cards and for the interfaces into the acquiring systems. Because banks are purchasing cards and standalone EFT terminals the vendors of these have developed products meeting the requirements of the banks.

Acquirers are expecting major retailers to integrate the new functions into their systems as has been the case in various EFT developments over the years. However, the introduction of ICC raises significant issues which need to be addressed in order for this to happen on a widespread basis. Any system proposed must also handle non-payment applications and retailer-issued cards.

Further chip card projects around the world are making use of a wide variety of different standards and procedures. Only a minority of these is controlled by the banks.

UK retailers, via the BRC, have had various discussions with the banks (APACS) regarding the ICC trial but these discussions have been constrained by APACS to issues pertaining to the trial. There is a need for the retailer voice to be heard on the broader issues contained in this paper.

1.2 Objective

The objectives of the Joint Retailer Supplier Forum are:

- To address common issues to ensure retailers and suppliers can position their developments to capitalise on all relevant Smart Card opportunities.
- To identify common architectural and design approaches to hardware and software developments.
- To identify common interfaces between elements of the system which itself will vary from retailer to retailer and from supplier to supplier.
- To identify the factors which will permit future developments with a minimum of architectural or hardware changes.
- To identify key obstacles to the development of reasonably future proofed, generic Smart Card solutions

The objectives of this paper are to:

- Document a common approach to the above and the issues and architectures required in retail systems;
- Give this widespread circulation in all relevant industry groups in order to provoke discussion;
- Guide and influence the creation of solutions meeting the needs of retailers.

1.3 Scope

The scope of this paper is to outline an architecture for the integration of multiple Smart Card applications into retail systems and is addressed towards large retailers with networked EPOS store implementations, including but not restricted to:

- Debit/Credit cards conforming to EMV standards
- Electronic purses and stored value cards, including Mondex and Visa Cash
- Retailer Card applications such as Loyalty and Staff Functions
- Other third party applications

Where relevant it will consider the implications on systems where retailers network their EFT applications over wide area networks with central EFT applications and acquirer interfaces.

The paper establishes the principles of the required architectures and is not intended to restrict individual retailer or supplier developments. Wherever possible it will reflect the emerging Open Systems standards relevant to retailer systems.

Although written from a UK perspective, the principles should be applicable in any market.

2. Market developments

This section considers current and likely chip card developments which may affect retailers, but over which retailers will often have little or no control.

2.1 Traditional technology

The equipment available for reproducing magnetic stripe cards is now sufficiently widespread that it can no longer be assumed that the information on the magnetic stripe bears any relation to that on the face of the card. Although on-line authorisation and other checks are keeping fraud under control, the card itself no longer plays a useful part in protecting customers' money.

Certain retailers are now utilising secure memory cards instead of magnetic stripe cards for their loyalty schemes.

Cardholder Verification at the Point of Sale in the UK is generally by signature inspection. PIN is used in many other countries, either on-line or off-line. There has not been a consensus among UK banks to move to PIN or another CVM, but APACS is actively reviewing this position.

2.2 Current developments

2.2.1 Applications

There are at least four chip card applications in the UK which may require to be integrated into the retailer's EPOS system at some point in time:

- The APACS (UKIS) ICC credit/debit card system - trials from October 1997 to April 1998 with a bank view of a rollout from the third quarter of 1998.
- Mondex (as an electronic purse application, being trialled in Swindon with various campus systems installed in Universities.)
- VISA Cash (electronic purse - being trialled in Leeds from October 1997.)
- Retailer-owned applications such as retailer payment cards, loyalty applications and staff applications.

Further details of these schemes are provided in Appendix C.

Many developments in smart cards are being driven by telecommunications companies, which are by some margin the largest issuers of smart cards. Public-sector and similar applications (e.g. utilities, lotteries) are also expected to play an increasingly important rôle, and retailers in some sectors may have to handle cards from such schemes.

Whilst this paper addresses specific UK developments, the UK is typical of smart card developments in Europe.

2.2.2 Terminal developments

Standalone EFT terminals are developing to accommodate multi-application developments. Many of these have been developed to meet the requirements of acquirers; they incorporate Secure Application Modules (SAMs), large amounts of memory, “firewalled” partitions and cryptographic functions and may be considered over-specified for use in those retail networks where terminals have considerable computing power.

It is generally accepted that this architecture presents the only practical approach in the short term to making a standalone terminal capable of handling multiple applications but it does not map well on to large retailers’ multiple EPOS in-store configurations.

The later sections of this paper outline the direction these architectures need to take in order to offer an open, secure, supportable multi-application chip environment, namely that the chip card applications need to be layered across the EPOS system with the Card Accepting Device at point of sale performing only those functions which cannot be performed by a server system.

2.3 Anticipated developments

2.3.1 Technology

Cards are becoming more powerful. As well as permitting faster operations (which is of particular significance for authentication and encryption functions), they are also able to support operating systems which protect applications from one another and allow applications to be downloaded after the card is initialised. Such applications must be authenticated before they can be downloaded or used.

An increasing number of applications (in Internet trading, software downloading and computer systems access as well as smart cards) use public keys which must be distributed and authenticated by a trusted network or third party. The development of this Public Key Infrastructure is dependent on political and commercial issues as well as technology; its final shape is by no means clear. Most “open” card schemes will, however, have to connect to such an infrastructure.

2.3.2 Applications

It is now assumed that the banks will go ahead and roll out the UKIS (EMV) application for debit and credit.

It can also be assumed that retailers will want to accept their own issued smart cards through the same device.

The position on electronic purses is less clear. The speed of acceptance of electronic cash by consumers and major retailers remains an open question.

2.4 Critical assumptions

Based on these trends, this paper assumes that:

- Smart cards will replace magnetic stripe cards for all bank cards, but magstripe cards will co-exist for the foreseeable future;
- The UK banks will roll out cards to the UKIS specification starting in the third quarter of 1998;
- Electronic purses will become widespread over the next few years. The major players will use both the Mondex and Visa Cash models;
- Although initially many cards will be single application, multi-application cards will become the norm within three to five years;
- No decision on cardholder verification will be made by July 1998, but provision must be made for an automatic CVM within the lifetime of equipment currently being installed;
- PIN is the only practical and acceptable CVM in the short term, but other CVMs may be considered in the longer term.

3. Chip card handling requirements in multiple retailers

3.1 Business requirement

Retailers wish the option to accept all cards offered in payment by customers, subject to cost and operational difficulty. As a minimum, this will require the ability to handle chip-based credit/debit cards issued in the UK and overseas. It would be desirable to be able to accept a range of electronic purse cards, provided that these can be processed using similar operational procedures and without extra equipment at the point of sale.

The smart card provides the opportunity for retailers to interact with customers using a variety of new media. A high level of flexibility in implementing the customer and systems interfaces is required. The solution must take into account the needs of unattended terminals, kiosks and remote payment systems.

Whilst most retailers wish to maximise the opportunities for their customers to make payment by any convenient method, the retailer must ultimately remain in control of the payment methods acceptable for any given transaction. Where there is a choice of acceptable payment methods, however, that choice will be the cardholder's.

Retailers have a range of potential applications for smart cards, including staff discounts, loyalty, credit and incentives. These must be handled through the same reader as payment applications, and the retailer must retain the flexibility to add or update these applications.

Retailers are already used to handling magnetic stripe cards for a number of different applications and major investment will only be needed if the chip cards do not follow the systems and procedural practices used in existing card handling methods. Any move to chip card should follow most of the principles that are already being applied:

- Minimise changes to hardware, and where possible synchronise these with the EPOS replacement cycle.
- Low cost of readers and authentication hardware
- Confidence in the longevity of the technical solution (5 years +)
- Negligible risk to existing business processes (e.g. magstripe transaction processing)
- Well-defined fallback procedures

A migration path must allow new chip card applications to be added progressively to EPOS systems without the need for major changes. As more applications become available to retailers using chip cards, existing procedures may well be challenged but today the way retailers handle magstripe should provide the basis for the way forward for handling chip cards.

The architecture must support unattended and customer activated terminals.

3.2 Operational requirements

3.2.1 General

Operationally there are some clear retailer objectives in handling card transactions:-

- To maximise customer throughput by avoiding unnecessary discussions at POS;
- To minimise transaction timing: authorisation time should not normally be longer than voucher printing time;
- To minimise cardholder confusion due to unfamiliar devices and procedures;
- To minimise staff training requirements. There should be a consistent operation for all types of card, and no need to recognise the scheme-specific visual features on a card;
- To minimise customer confrontation in case of card rejection, capture etc.
- To provide a secure and integrated operation and minimise risk to other systems;
- To ensure adequate fallback procedures for both manual and system supported mechanisms
- To maintain or improve the existing proven systems for interfacing with card schemes and acquirers;
- To move rapidly towards an effective and objective means of cardholder verification. The verification device must have a small footprint and must be flexible enough to handle current and reasonable future requirements (e.g. 5 years).

These objectives apply to any card device. For smart cards, the following additional requirements apply:

3.2.2 Readers

There must only be one chip card “slot” for all types of chip card.

Whether or not this is combined with a magstripe reader, with either or both being motorised, should be a separate consideration based on environment and cost. For new equipment, a single device for reading magstripe and smart cards is likely to be preferred, but where existing terminals are fitted with magstripe readers, a separate slot for chip cards may be used. Motorised and insertion readers are both acceptable and each may be more appropriate in different POS environments.

3.2.3 Chip and magstripe on the same card

Where a chip and magstripe are both present on a card the chip should be the primary source for processing the transaction. The magstripe should only be used where the IC cannot, for whatever reason, be processed and then only if allowed by the retailer's system and card scheme rules.

3.3 Functional requirements

3.3.1 Principles

The primary requirement is to integrate smart card reading into the EPOS system, using as far as possible similar processes to those existing.

As with the operational requirements, retailers have established several common principles which should be carried forward into the chip card architecture. They include:

- 'Open' technical architectures
- Standard server and interface protocols
- Central or store server control of application logic
- Network authorisations of financial transactions
- Implementable on a wide range of current and (within reasonable limits) older hardware
- Scalability

As applied to chip cards, this implies that:

- Systems and IC cards must have a consistent interface allowing communication between third party software on the terminal / host system and third party software (including both EMV and non-EMV applications) on the IC card. Application software may be written in any one of a number of common languages including C, C++ and Java.
- IC cards and systems must conform to a consistent interface specification conforming to ISO7816, in order to ensure that systems can communicate with and select applications on the widest possible range of cards.
- CAD designs must take into account the needs of existing and future Point of Sale equipment; it is accepted that CADs being used in system with older equipment will incorporate more functions, computing power and memory than those for use with modern PC networks. Software should as far as practical be compatible with legacy systems.
- Hardware interface definitions should be independent of the application and vice versa. The software to handle one card application should as far as possible be identical regardless of the hardware and network platform used.
- Ability to integrate readers to a range of PC based hardware using open standards where possible.

- Ability to retrieve keys or application versions dynamically when a reader/POS is missing the relevant key or version.

3.3.2 New functions

In addition to the current functions of:

- card reading and validation;
- communication with the EPOS system, external host, operator and cardholder;
- transaction recording and processing;
- assuring the integrity of the transaction and recovery from errors,

a chip card-based system must be able to:

- select an application from those supported by both card and retailer system;
- authenticate the card and/or the application using cryptographic techniques;
- respond to similar cryptographic “challenges” from the card;
- protect the confidentiality and integrity of personal or other sensitive data which may be stored in the card and transmitted to and from the system;
- support secure storage for any “keys” (other than public keys) used in the cryptographic process and for the value which may be stored in an electronic purse;
- handle version control for card applications and, in the future, download applications both to the point of sale and to the card.

3.3.3 Cardholder verification

The upgrade to chip cards is a unique opportunity to provide a path towards the infrastructure required for migrating from signature inspection to a more objective and accurate Cardholder Verification Method (CVM). This should include the provision of the necessary hardware and software interfaces, and setting down principles for template storage and cashier responsibilities.

Any CVM must be

- objective;
- simple and fast for both customers and cashiers;
- appropriate for use at unattended terminals; and
- not susceptible to false rejections (the current bank criteria in this respect are appropriate).

3.3.4 Backwards compatibility

The replacement cycle of many retailer owned POS equipment is between 5 and 10 years. The investment and training required to replace old equipment is considerable. Costs for introduction of chip will have less impact when old equipment is replaced than when undertaking specific upgrades. It is unlikely that retailers will have replaced all POS equipment which is incapable of accepting chip by the time the UK card base is fully chip-enabled.

Any solution adopted must not only be capable of accepting magnetic stripe cards for the foreseeable future, but must be adaptable to a range of older and less powerful EPOS systems (provided such systems meet minimum criteria for speed and software support). Conversely, hardware and software installed today should be capable of being upgraded or used with tomorrow's more powerful systems and cards.

3.3.5 Security

Hardware security modules should as far as possible be restricted to server functions; security at the point of service level should be provided by software. Some current bank schemes (e.g. Proton, Danmønt) insist on a hardware security module at the point of service: this restricts the generality of the solution but may not be avoidable in the short term.

4. Architecture

4.1 Rationale

The architecture proposed below takes into account the architecture used in typical multiple retailer installations today. (Separate conditions apply to petrol stations and other specialist delivery channels).

The current architecture envisaged includes a card reader linked to an intelligent EPOS by a direct (serial or keyboard wedge) link. The EPOS system (which may or may not include a store concentrator or back office system) is LAN-connected and connected by a WAN to a host system at Head Office. Communications with the acquirer may be from the store or from Head Office.

In the smart card environment, a smart card accepting device is used instead of the magnetic stripe card reader. This card accepting device requires two-way communication with the point of sale unit. It is, however, desirable to minimise changes to the other parts of the system.

The architecture proposed carries forward the division of functions between these components, but attempts not to constrain future changes. It isolates functions or groups of functions which are independent of the hardware configuration. A modular implementation is recommended, and would allow the smart card extensions to be mapped onto different hardware configurations; functions could also be upgraded and moved where necessary.

In order to provide flexibility, as many functions as possible should be carried out in software. Firmware within a device is an acceptable alternative, provided that upgrades and modifications can be downloaded using the retail network.

4.2 Framework

The framework derives from a simple three layer model (see Figure 1).

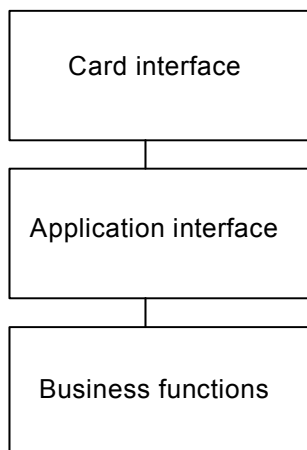


Figure 1 - Three layer model

The top layer forms the interface with the **card**; it should be independent of applications and business functions, but provides all the physical and electrical aspects of the card handling. These services should be common to multi-application smart card handling in any environment (e.g. transport or telephony as well as retail).

Below this is a set of services which relate to the card **applications** supported by the retail system; as a principle, there will be an application (a program) in the EPOS system for every

card application supported, and these programs should again be re-usable in other environments where the same card application is supported.

Below these is the **business** logic which determines the way the retailer accepts this card application, how the transaction is processed and which external hosts it must communicate with. Most of this will be common to other similar cards (e.g. chip-based credit and debit cards will follow the same rules as magstripe-based credit and debit cards).

Surrounding these are several support functions which are necessary to interface with external systems and to provide the additional security functions referred to in section 3.3.2.

In Figure 2, the layers are broken down into functional "services", which are described in greater detail below:

4.2.1 Card transport

This service covers the physical and electrical interface with the card other than through its I/O port. These functions include:

- Physical insertion / removal of card; control of contact closure and latches
- Status signals and commands to/from terminal
- Power supply and clock provision (includes determination of voltage, removal of voltage in case of card removal etc.)

4.2.2 Protocol conversion

The functions of this service are closely linked with the card transport during insertion, initialisation and removal of the card. They include:

- Communications protocol determination, translation and buffering
- Card type identification / selection (ATR handling)

In some instances, these functions must also apply to magnetic stripe cards (see section 4.4).

4.2.3 CAD display / keypad handling

This service is only required where a keypad and/or display are incorporated in the CAD. Data may be exchanged between these CAD features and the application logic, but in the specific case of off-line PIN entry the PIN is passed directly to the card. It is expected that other CVMs would be handled in the same way. The integrity of the message transfer and the confidentiality of any PIN exchange must be ensured by a combination of card scheme and hardware design.

4.2.4 Card authentication and application selection

In a multi-function card, any application-independent card authentication checks should be performed before an application is selected. There is also a practical advantage in a checkout environment in performing card authentication as soon as the card is inserted, since this part of the operation can be removed from the critical timing path (although this would require a change from the current procedure). Some form of parallel processing may be required to keep transaction times to a minimum. Some applications (such as EMV) may include further authentication checks on application selection.

Figure 2 - Functional services

Application selection may be performed automatically by the POS device, from an application list, or the application may be manually selected by the cardholder or operator. There may be a hierarchy of applications (e.g. EMV Payment Systems Environment - ISO Directory - cardholder selection).

4.2.5 Application authentication

There may be further authentication checks associated with the application, and these will often (as in EMV) form an integral part of the application logic. The application may also include terminal authentication checks.

4.2.6 Application logic

This refers to the functions required in the terminal to support the application within the card. If the retailer accepts several card types, or if any of the cards are themselves multi-application cards, then there will be several of these applications. Applications will be added

Application interface

and updated within the retail system from time to time, and so these must be in software. Applications may consist of “applets” downloaded on a periodic or on-demand basis.

There may be data associated with each application. Keys and other cryptographic data must be handled in an appropriate way, taking into account the need to prevent not only disclosure of keys, but also system abuse by a fraudulent merchant or following theft of a device.

Off-line processing of the transaction at this level should not include business functions (such as hot-list checks), since these will be carried out by higher-level processes. The logic may include implicit transaction routing decisions, but these are passed to the higher-level processes for action.

The application logic service should include provision for handling card errors.

Business functions

4.2.7 Common functions

The application-specific software may be supported by **functions common to several applications**, such as encryption. Such functions may be implemented as library functions (i.e. they are built in to the application software), or called by the application using a higher-level mechanism such as DDE. Encryption functions may be performed in software, hardware (cryptographic co-processors) or a combination of the two. There should not normally be any data storage associated with these functions.

4.2.8 Point of service logic

The chip card application functions should communicate with the point of service logic (the existing EPOS program or customer interface), and any peripherals controlled by that logic

(such as displays, keyboards and printers on the EPOS device) through a defined Application Program Interface (API). Communications with the cashier and/or customer are controlled by this set of functions, which should also have specific facilities for cancelling or reversing the current transaction.

This service should have provision for handling application and operator errors.

4.2.9 Storage of value

This service provides the secure value store required by an electronic purse or similar system. It may consist of hardware or software, and may be located at whichever point in the EPOS system provides a suitable balance between the risks of non-availability, permanent failure, theft or loss, and the lifetime costs of installation, updating and maintenance. Transaction timing may also be affected by the location of the value store in the network and must be taken into account in the design.

There will normally be two interfaces to the store of value: one from the application logic (i.e. from the card) and the other from the business logic (i.e. from the host system).

4.2.10 Business logic

This covers the commercial processing of any payment transaction and its routing to a host system or acquirer. It also includes the posting of the transaction to the retailer's own system and subsequent processing.

Other functions which should be performed by this service include:

- Secure transaction storage
- Validation of card application for this transaction
- Risk management, including hotlist storage / checks
- Generation of on-line authorisation request parameters
- Interpretation of on-line response
- Subsequent processing
- Handling of reversals (for completed transactions)
- Terminal error handling
- Network error handling
- System error handling
- System initialization
- End of day functions

Encryption functions which may be associated with the business logic include:

- Secure storage of private keys
- Encryption functions requiring private keys and transaction keys

4.2.11 Logging and recovery

There must be a logging and recovery system capable of tracking transactions through the system and reacting correctly to failed transactions. It is likely that each level will

incorporate some logging functions, but that a control service will be required to ensure correct recovery from errors and incomplete transactions at each level.

4.2.12 Host communications

This service is responsible for high-level communications, including normally the interface to an acquirer or other external system. It will use existing communications paths and may incorporate many common functions with other applications. It should include:

- Formulation of the on-line message
- Parsing of on-line response
- Communications with external host system
- Communications error handling

4.2.13 Application control

This service will control the list of valid applications, the application selection parameter tables and any authentication parameters. It must be able to track the applications loaded by store or by till where necessary. It may also be necessary to record the version number of any application and of the electrical and protocol standards required, and to compare these with the versions installed in or connected to each till.

The service should also include control of the downloading process (where applications are downloaded) or of the server functions for applets.

Specific functions will include:

- Application list updating
- Authentication key updating
- Application updating

4.3 Cards

Systems should be able to accept all cards meeting ISO 7816 parts 1, 2 and 3 (1989 and later). Most of these cards will be microprocessor-based, although memory cards which conform to the T=0 or T=1 protocols and which deliver an answer to reset (ATR) may also be handled. These memory cards will not support the inter-industry commands for interchange (ISO 7816 pt 4) but may still be handled by a low-level branching sequence in the CAD.

Although it is anticipated that the majority of cards issued in 1998 will be 5 volt, systems capable of handling lower voltage cards (following the draft amendments to ISO 7816-3) will have a longer life.

The architecture proposed will be capable of accepting multi-application cards (meeting, for example, the Multos or Javacard API specifications).

4.4 Card accepting device

The first group of functions (card transport, protocol handling and keypad/display handling) may be considered to form the card interface. They must be performed in a tamper-evident device; as far as we can see, the device must be tamper-*proof* to the extent of losing any stored data if tampered with. We call this the card accepting device (CAD). The CAD may

be a separate peripheral or a part of the point of service device (e.g. in a vending machine); its functions are, as far as possible, common to all cards and applications accepted by the retailer.

There is no terminal standard corresponding to ISO 7816 or to EMV pt 1 (although EMV pt 1 implies several aspects of a terminal standard). The EMV standards (particularly the EMV3 Errata) give a closer definition of tolerances and testing methods, and CADs should meet these closer definitions. Cards may, however, deliver ATR responses which are listed as “undefined” in the EMV specifications, and CADs should not (despite the requirements of the Errata) reject these cards.

The CAD is seen as a peripheral or, more correctly, as a “thin client” to the rest of the system. Its principal functions are those of protocol conversion, and these functions are available in a single chip format. To provide the flexibility required by retail systems, however, it is recommended that a microprocessor controller be included in the CAD. Security Application Modules (SAMs) may be physically located within the CAD or externally.

The microprocessor allows some application functions (e.g. card authentication, RSA signature verification or even UKIS) to be carried out in the CAD, which should facilitate the introduction of chip card systems in retail systems with limited power POS terminals. In an extreme case, all the services which form the application interface could be resident in the CAD. However the aim should be to migrate these functions to an EPOS or higher level device. Where card authentication is carried out within a CAD which is not equipped with the relevant SAMs, any public keys should be downloaded from a secure key storage area on initialisation or when first used and deleted when power is removed.

Where the CAD contains software functions, thought should be given to the method and ease of downloading upgrades.

CADs may have all or some of the following optional functions:

- Cardholder display
- Keypad (accept / reject / cancel, input of application selection or PIN entry)
- Secure transmission of PIN to card
- Magstripe reading.

Incorporating a magstripe reader in the CAD allows a single operation for all types of card, but it increases the effort required to update existing systems, most of which will already have integral magstripe reading capability. Retailers will have different views on this subject. However, most current smart card reading terminals have separate magstripe and chip card slots in a single device, which is the least satisfactory solution for a retailer with existing magstripe reading capability. This model supports any of these options.

The CAD may be free-standing or integrated into a till device; consideration must be given to a physical arrangement such that the customer can insert the card or perform keying operations, and to the need for hoods or other provision for secrecy of PIN input. The model permits and supports the use of a second CAD (e.g. for staff functions) if required.

4.5 Point of service device

The architecture proposed implies (but does not demand) that the application interface functions (application selection, application logic, point of service logic and common encryption functions) be performed in a point of service device such as an intelligent EPOS till. This device (including any co-processor) must be able to perform relevant cryptographic

operations within a time regarded as reasonable for the retail sector concerned - this may be in the range 0.3 - 3 seconds.

4.6 Back office / head office systems

The other services referred to in section 4.2 may be carried out at any point in the network. The intention is to provide a high level of commonality with existing systems, and it is assumed that each system will separate back office and head office functions in the way which best fits the retailer's business model.

4.7 Impact of other standards

A list of relevant standards and specifications is included at Appendix A. Future versions of this document will list the standards relevant to each functional service or interface.

4.8 Equipment certification and bank approvals

A modular implementation of chip card processing is in the interests of all parties. To match this, however, a modular certification process will be required. It will be necessary to test and certify hardware and software elements separately against several standards. Testing of Card Accepting Devices **must not** be application-dependent.

A system of independent testing by accredited laboratories is required. Low-level testing of Card Accepting Devices must be carried out against ISO 7816; a régime of component and module testing for the other elements must be devised and will require definition of test processes associated with each specification used. For hardware devices and network components, tolerances must be specified for each side of the interface.

Even when a system consists entirely of certified components, acquirers will carry out end-to-end testing using test cards and test scripts. These should be made available to suppliers at an early opportunity.

5. Interfaces

Interfaces between elements of this model should be defined at each relevant Open Systems Interconnection (OSI) layer. For the software components, definitions should be in terms of a generalised API.

Although it would be desirable for future versions of this document to include such definitions, it may not be practical to produce generalised definitions applicable across a wide range of suppliers. Suppliers should, however, produce and where relevant make available these interface definitions.

Interfaces should, wherever possible, be defined in terms of one of the open standards listed in Appendix A. Software interfaces should be independent of hardware or network configuration, and in general it should be possible to perform all operations which are not real-time (i.e. all services above the card interface) across a local area or high speed wide area network.

6. Summary

This paper sets out a model for acceptance of multiple chip card applications in integrated retail systems. The model proposed differs substantially from that currently envisaged by the card schemes and on offer from major EFT terminal manufacturers:

- It can be mapped on to any EPOS architecture;
- Applications need not be resident in the Card Accepting Device;
- Security Modules and Merchant Purses may be located at any point in the network, to match the retailer's infrastructure;
- Type approval must be modular; approval of Card Accepting Devices must not be application-specific;
- The architecture will support the introduction of new applications, including non-banking applications.

These changes are necessary in order to implement multiple chip card applications efficiently in integrated retail environments and to provide the flexibility required for the long term application of this technology.

The key recommendations are:

- **Card reader and EFT terminal suppliers should consider making their architectures more modular and more suitable for network implementation. Software suppliers may have to provide additional interfaces.**
- **Card schemes should reconsider their type approval requirements to reflect the cross-industry nature of chip card applications.**
- **Retailers implementing chip card schemes or accepting card payments under current bank initiatives should support this architecture now in order to permit suppliers to develop products to meet their long term requirements.**

The paper recognises that there are outstanding issues which must be resolved in parallel with these activities, and some of these are listed at Appendix D.

Appendix A: Related standards

ISO 7813	<p>Identification Cards - Financial transaction Cards.</p> <p><i>Fourth Edition 1995 includes definition of extended service codes</i></p>
ISO 7816	<p>Identification cards - integrated circuit cards with contacts..</p> <p>Part 1: Physical characteristics</p> <p>Part 2: Dimensions and location of contacts.</p> <p>Part 3: Electronic signals and protocols (<i>2nd edition, 1997 includes extended protocol and voltage negotiation</i>)</p> <p>Part 4: Inter-industry commands for interchange.</p> <p>Part 5: Numbering system and registration procedure for application identifiers.</p> <p>Part 6: Inter-industry data elements.</p> <p><i>Part 7: Inter-Industry commands for Structured Card Query Language (SCQL)</i></p> <p><i>Part 8: Security commands</i></p> <p><i>Part 9: Enhanced commands</i></p> <p><i>Part 10: Synchronous cards</i></p> <p><i>Part 11: Security architecture, access control security attributes</i></p> <p><i>Parts 7-11 are still in committee draft</i></p>
ISO 10202	<p>Financial Transaction Cards - Security Architecture of Financial Transaction Systems Using Integrated Circuit Cards.</p> <p>Part 1: Card life cycle</p> <p>Part 2: Transaction process</p> <p>Part 3: Cryptographic key relationships (draft)</p> <p>Part 4: Secure application modules</p> <p>Part 5: Use of algorithms (draft)</p> <p>Part 6: Cardholder verification</p> <p>Part 7: Key management (draft)</p> <p>Part 8: General Principles and Overview (draft)</p> <p>Part 6 is mainly concerned with PIN verification, although an annex allows for passwords or biometric methods.</p>
EN 1546	<p>Identification card systems - Inter-sector electronic purse.</p>
EMV	<p>Integrated circuit card specifications for payment systems. (Europay, MasterCard and Visa)</p> <p><i>Part 1: electromechanical characteristics, logical interface and transmission protocols.</i></p> <p><i>Part 2: data elements and commands</i></p> <p><i>Part 3: Transaction processing.</i></p> <p><i>ICC Terminal Specification.</i></p> <p><i>EMV3 Errata (published January 1998)</i></p>
UKIS	<p>United Kingdom Integrated Circuit Card Specification</p>
Mondex IFD	<p>Mondex System Architecture Specification: IFD-Purse Application Interface. This specification is available only to Mondex licensed developers, and may shortly be substantially updated.</p>
APACS 29,30,40,50	<p>The standards used in the UK for communication between retailer</p>

	systems and acquirers for settlement and authorisation of card transactions.
APACS 60	UK Specification for Message Interchange between Card Acceptor & Acquirer; this newly issued standard, which complements and may supersede the existing APACS 30, 40 and 50 standards, is based on the European <i>prENV1750</i> and ISO 8583 standards.
APG Guideline 8	Point of Sale Procedures for the Use of Extended Service Codes
APG Guideline 9	Point of Sale to Acquirer Message Requirements for the Support of Integrated Circuit Cards
<i>prENV1750</i>	Financial transaction card originated messages - interchange standards.
PC/SC	<p>The PC Smart Card architecture is an open architecture developed by a group of smart card and PC operating system vendors, notably CP8 Transac, HP, Microsoft, Schlumberger and Siemens Nixdorf. It is intended to ensure interoperability between components from different vendors and across different hardware and software platforms. It comprises:</p> <p>Part 1: Introduction and Architecture Overview Part 2: Interface Requirements for Compatible IC Cards and Readers Part 3: Requirements for PC-Connected Interface Devices Part 4: IFD Design Considerations and Reference Design Information Part 5: ICC Resource Manager Definition Part 6: ICC Service Provider Interface Definition Part 7: Application Domain / Developer Design Considerations Part 8: Recommendations for ICC Security and Privacy Devices</p>
OpenCard Framework	OpenCard is an architecture intended for the use of smart cards in a Network Computer (NC) environment. It is promoted by Apple, IBM, Netscape, NCI and Sun.
OPOS	Microsoft OLE for Point of Sale standards
ARTS	Association for Retail Standards (US) Retail Data Model
IFSF	International Forecourt Standards Federation: a group of 10 European oil companies which develops common specifications for various electronic devices used on the forecourt.

Appendix B: Glossary

APACS	Association for Payment and Clearing Services
API	Application Program Interface
ATR	Answer To Reset: the data sent by a card to the reader when it is first powered up.
BRC	British Retail Consortium
CAD	Card Accepting Device
CVM	Cardholder Verification Method
DDE	Dynamic Data Exchange: a form of program to program communication.
EFT	Electronic Funds Transfer (electronic payment)
EMV	Europay, MasterCard and Visa (standards for chip-based credit and debit cards)
EPOS	Electronic point of sale
ICC	Integrated Circuit Card (=chip card)
IFD	Interface Device: a general term for a card peripheral
IHCF	Industry Hot Card File (standardised list of lost and stolen cards distributed by banks to retailers)
OPOS	OLE for Point of Sale standards (see Appendix A)
OSI	Open Systems Interconnection: model for communications between similar computer systems from different manufacturers.
PC/SC	PC Smart Card standards (see Appendix A)
PIN	Personal Identification Number
POS	Point of Sale (or Point of Service)
SVC	Stored Value Card
UKIS	UK Integrated Circuit Card Specification
USB	Universal Serial Bus

Appendix C - Details of schemes

C1. APACS ICC Trial

The UK banks were in the vanguard in implementing a trial with the EMV standards for debit and credit cards. (The only other current EMV implementation is in Japan.) APACS' specification "UKIS" is the UK implementation of EMV. Both the UKIS and EMV standards are still subject to change.

The trial is taking place in Northampton and Dunfermline and commenced on October 1st 1997. The trial is scheduled to run through to the end of April '98 although a first tranche of data will be taken at the end of February to allow the banks to commence reporting on the results of the trial.

The trial has been set up by APACS (Association for Payment and Clearing Services) with an ICC Project Team set up on behalf of the member banks. 14 card issuers are issuing cards in the trial covering four card schemes (VISA, MasterCard, Switch and AMEX) and transactions from the trial are being acquired by seven acquirers.

110,000 cards from several manufacturers have been issued for the trial and it is expected that between 0.1 and 0.2 million chip-based transactions will be completed. The acquirers are placing EFT terminals in 600 smaller retail locations and six major retailers will participate in the trial, although none of the major retailers entered the trial until early 1998.

The requirement is to produce a system with a suitable Card Accepting Device (CAD) and to change the EPOS systems to be conformant with the new messages as defined in APACS Guideline 9. There are three EFT terminal manufacturers involved in the trials: VeriFone, Racal Transcom and De la Rue Card Systems (Fortronic).

The UK Banks have announced that they will take a decision on rollout of the systems in July '98. Assuming this goes ahead APACS' intention is to have rolled out Chip enabled terminals across 50% of the UK terminal base and accounting for 65% of transactions in three years.

C2. Electronic Purse Schemes

Mondex has now been in trial in Swindon for over two years. The application of the scheme has increasingly focused on the niche markets best suited to electronic purses such as parking, ticketing and transportation.

Mondex is unique in that it is "not accountable". Individual transactions are not reconciled back to individual bank accounts. The scheme uses sophisticated public key cryptography to protect the data which must be held in a physically secure "chip" environment, i.e. a hardware security module. In addition to Swindon Mondex has now been implemented in some five UK Universities. NatWest and Midland were the original owners of Mondex but 51% of Mondex is now owned by MasterCard. Mondex trials are now taking place widely around the world.

Visa Cash started a UK Trial in October '97 in Leeds. There are 2,000 acceptance points and 70K cards being issued in the trial. Around the world there are many different electronic purse implementations branded Visa Cash. The Leeds trial is the first Visa trial using their strategic public key encryption system.

Whereas the Mondex cards issued in the trial are single function cards the Visa Cash cards have been issued as a secondary application on debit cards. For instance, Barclays have placed the Visa Cash chip on Connect cards which are magnetic stripe for debit.

All the electronic purse pilots use specific ICC terminals to meet the application requirement. These terminals are placed in individual retailers by the banks and schemes in the trial.

Elsewhere in Europe there are several other electronic purse schemes using different protocols and encryption schemes.

C3. Retailer Smart Card Applications

A number of retailers have introduced Smart Card (mainly secure memory card) applications in the areas of Customer Loyalty and Staff Applications. These cards are accepted in CADs which are small intelligent terminals either connected to EPOS or standalone.

Appendix D - Issues for resolution

- a) The banks' requirement for card retention in case of stolen cards may be difficult to achieve with insertion readers and customer insertion.
- b) The use of electronic purses may increase the number of occasions on which customers ask for split tender. Customers may not know the balance on their purses. Readers will need to be made available for this purpose, or cashiers, checkout operators and unattended devices must be able to show a balance before proceeding with the tender operation.
- c) The current UKIS procedure for voice referrals (which involves accepting the transaction "provisionally" using the retailer over-ride) is unsatisfactory since a check of the Transaction Certificate issued by the card would not provide any proof that the referral procedure has been followed.
- d) Where the POS device is unable to go on-line (either because it does not have this facility or because the network is unavailable) the card may decline the transaction. The terminal will indicate that a decline has been given but will give little or no information behind the reason for the decline. Contacting the help desk of the relevant bank will not help as no transaction details have been received by that bank. Some retailers may wish a way for their Customer Service desks to be able to assist customers to ascertain the reasons for a decline before putting the goods back on the shelves (which is not always possible).