The plastic card: Information carrier for money-replacement and identification applications

UDC: 351.755.62 336.777 336.736

J.-F. Moser

In the past 25 years the highly developed industrial countries have experienced a continual increase in the use of credit cards for financial transactions. The «Cashless and Checkless Society» is today the catch-phrase of the economists, leading us unavoidably towards the world of EFTS (Electronic Funds Transfer System) where an identity card will be one of the pre-requisites of entry. In the not too distant future, so we are led to believe, the rapid technical innovations and developments in the field of electronics will allow even the card to be dispensed with, and the human voice will suffice as a means of identification of an account holder. Must we therefore assume that the plastic card is already outdated as a means of identification and payment?

1. Summary of card types and applications

To answer the question posed above, it is firstly necessary to examine the character, functions and manifold uses of the plastic card. A general overview of the various areas of application can serve as a helpful reference basis. The classification shown in *figure 1* illustrates the wide range of card applications which exist today. This list includes only some of the more common uses and could be readily extended.

It is convenient to divide the application areas for cards into four main types. Each of the applications covered by a main card type will in general possess well defined organizational and operational goals, which together with a particular infrastructure, constitute a system. The card forms only a component of the system. Obviously the complexity of systems differ widely: for example, a visually checked identity badge is conceptually simple within the context of both organization and operation, whilst an access control system using machine readable cards can be extremely complex.

The requirements that must be met by a particular card must be formulated by considering the system as a whole. One very important aspect is concerned with whether the card will be checked visually, or read by means of a machine. This difference allows a major subdivision into two classes: visually checked cards and machine readable cards. The latter class will be of special concern in the following sections.

Card types with dominant function

Cheque card[1]	Credit card[2]	Identity card	Prepaid card
Provides authorization for a cashless payment or withdrawal of cash from a personal bank account	Provides authorization for a credit transaction with for example a credit limit, and repayment by instalments	A card providing identification of the holder	A card which can be purchased and then used to obtain goods or services. This card is transferable
Examples			
- EUROCHEQUE - BARCLAYCARD - LLOYDS BANK CARD : - etc. for nearly all major banks - MIGROS cheque card - BANCOMAT card (cash dispensing)	- DINERS CLUB - AMERICAN EXPRESS - BANKAMERICARD HERTZ - AVIS - VISA - Gasoline card - Shopping card (department stores eg. Jelmoli)	- Drivers license - Identity badge - Passport - Identity card - Computer access card - Access control system card - Membership card - Season tickets	- PHONOCARD - Gasoline card - Ski-lift card - Parking card - Electricity card - Cards with a jeton or token function

Further types

Cards for organizational simplification or rationalization n)

- Diners card (for ordering and payment in restaurants)
- Hotel room card (also as a security room-key system)
- Programming card (for process control, operation of machines etc.)
- Time card (time checking, Flexitime etc.)

930 462e

1) Also termed Debit card, allowing account transactions without any authorization for credit. Also hybrid forms allowing a number of various personal account transactions.

2) Cards for settlement of debt upon presentation of account, or with monthly settlement on revolving credit basis, usually with credit limit. The general term for such a card is Transaction card.

Fig. 1 Types of card and some main application areas

Fig. 2 Some plastic cards as information carriers

2. The visually controlled card

In the case of a visually controlled card, it is clear that the card takes on the role of a passport, that is, a document which allows the holder to «enter» the system of which it is a component. The control procedure is limited essentially to checking the identity of the card user and the validity of the card, and an assessment of the genuineness or authenticity (or otherwise) of a card is the responsibility of the person who performs the check. Consequently there are basically three types of information which need to be present on or in such a card:

- Information which identifies the card user.
- Information enabling a check on the authenticity of the card.
- Information which shows at sight the validity of the card, for example data in alphanumeric form.

2.1 Examples

2.1.1 The credit card

The average credit card – subject only to a visual check – serves as a particularly simple example. Such a card bears the name and address of the holder in embossed characters, together with a signature. An additional sequence of embossed alphanumerics gives information concerning the operating organization, use and holders account number. The embossed information normally conforms to an ISO Standard, which allows the use of a simple imprinter to capture the card information and obtain a record of transactions. When a transaction takes place the card holder is usually required to add his signature to the imprinted record. A comparison of the signatures on the card and on the imprinted records provides the only means of identifying the card user. Very little information is available to check the authenticity of a card, as such cards are commonly printed with rather simple graphics.

2.1.2 The bank card

As a second example of a visually controlled card we consider a bank card, and take the well-known Eurocheque card as our illustration. This differs from a credit card in that the card must be used in conjunction with a «matching» Eurocheque. Card identification information is again provided by the name of the card holder in embossed characters together with a signature. Authenticity information is provided by the basic card structure, where a watermarked paper insert colour printed with guilloche patterns is hot-laminated together with plastic cover foils. An embossed numeric sequence gives information concerning the system operator (i.e. bank), card number and account number of the holder. Transactions take place only in combination with a Eurocheque, whereby the signature, bank name and account number must correspond on both card and issued cheque. In addition to this the cheque is further personalized by means of a machine readable numeric sequence used for cheque processing purposes by the bank.

2.1.3 The access control card

As a final example of visually controlled cards we consider briefly an access control card. Here the major function is the identification of a person authorized to enter a particular location, and for this, the name, signature and a passport photograph of the holder should be incorporated in the card in such a way that alteration or replacement is not possible. Further information on the card will be concerned with system operator details

Type of card	Type of information		
	Identification	Authenticity	Data
Credit card	– Name – Address – Signature (for comparison)	Practically non-existent Simple graphics and colour printing	– Name of operator – Operators number in coded form – Number of card holder – Card number
Eurocheque card	– Name	Laminated paper containing a watermark and colour guilloche patterns	– Name of Bank – Account number – Card number
Access control card	– Name – Signature – Photograph	Graphics and colour printing	– Indication of operator (eg. name) – Validity of card (eg. zones) – Card number

Fig. 3 The types of card information

and card validity (zones, times, etc.). The graphics and colour printing used provide the authencity information.

2.2 Card information requirements

The above three examples clearly do not exhaust the possibilities for the visual control of cards. They do however permit an overview of the typical requirements for this type of card. *Figure 3* shows the correlation between the various features that have been considered here.

3. Machine readable cards

Let us now examine the characteristics of a card which is solely designed to be machine readable. The card fulfils the function of an information carrier between the holder and a machine, whereby the information must be in a machine readable form. Despite this, the three categories of information shown in *figure 3* are readily discernable. The machine checks the authenticity of the card in some way, identifies the card holder by for example comparing information supplied by the holder with information coded into the card (a Personal Identification Number – PIN – or a physical feature such as a fingerprint), and finally reads functional data from the card for transfer to the next stage in the system.

3.1 Coding methods for machine readable cards

In order to build up a clear picture of card coding methods which are compatible with machine reading, we first list – omitting specific detail – the major technologies which are used in this field:

- Embossed raised characters (for example OCR)
- Punched holes
- Magnetic stripes
- Printing using magnetic or doped inks
- Magnetic holes
- Capacitative foils
- Inductive foils
- Ferroelectric inserts
- Radioactive tracers
- Printed conductors
- Optical bar-codes (black and white)
- Printing with fluorescent inks
- Colour coding
- Optical reflection coding
- Watermark magnetics
- Drexon strip
- Integrated circuit
- Holographic coding

Combinations of technologies shown in the above list are of course also possible. Obviously the reading equipment used must be matched to the technology involved. The choice of a particular method of coding depends strongly, as we shall see later, on the security needed in relation to the costs involved. All three information categories – identification, authenticity and functional data – must be included in the card in machine readable form. In general a need for higher security dictates the choice of a more sophisticated coding method.

3.2 Cards and systems: examples

We select a number of examples drawn from identification card and pre-paid card applications in order to examine the information-structure requirements for such cards. In the applications considered we expect clear advantages to be obtained from the use of machine reading.

3.2.1 Access control

As a representative example of a system having many requirements we first look at an access control system, without going too deeply into the complex problems associated with it. In *figure 4* a typical access control system is shown schematically, where a number of doors are supervised and controlled from a central location.

Each door is equipped with a card reader, which reads and verifies the card information, and the readers are connected on-line to a central computer which upon receipt of information from the readers takes some appropriate action.

The system can be so constructed that the card readers act solely as peripheral elements, and simply relay the card information to the central computer without themselves being involved in any decision making process. Here the card readers function as terminals. The disadvantage of such a centralized system is that any defect in the computer may block the entire system. In a decentralized system, the peripheral elements take over at least some of the decision making functions, the load on the central computer can be decreased and it is possible to avoid a breakdown of the entire system when for example a failure occurs in the central computer. The shift of intelligence to the peripheral elements can allow the system to function in an off-line mode.

The elements of the system are connected together via some communications network using either existing wir-

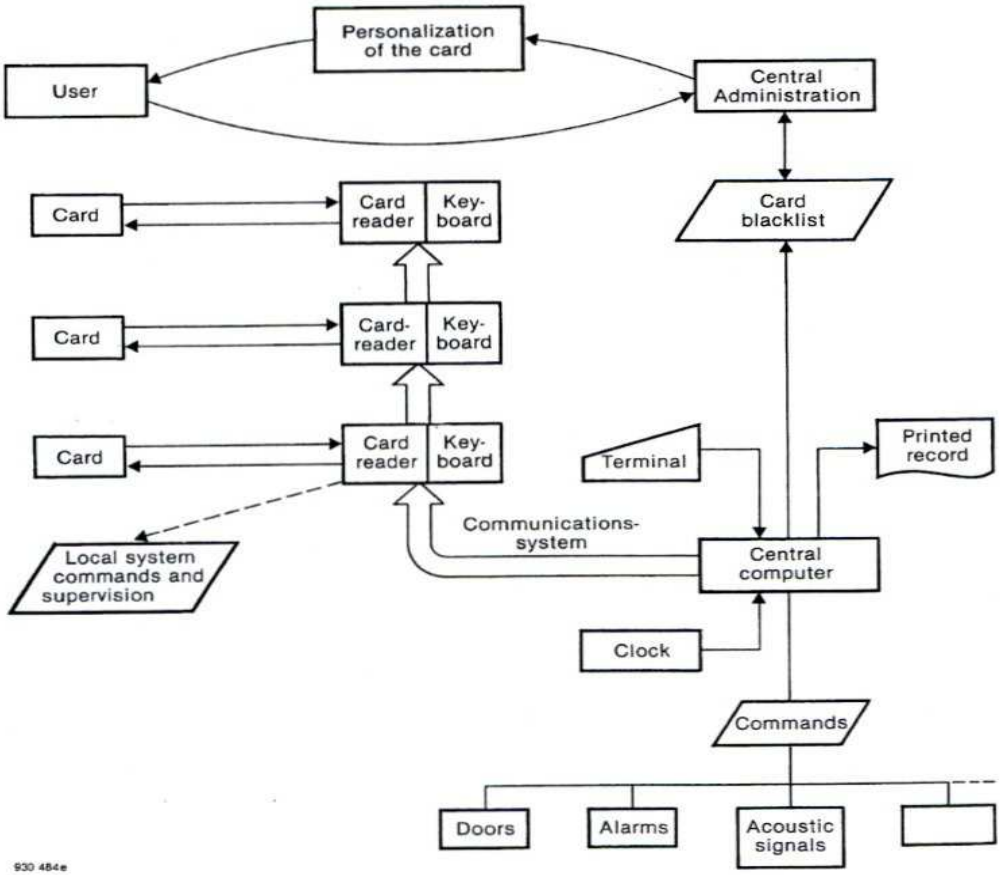

Fig. 4 Structure of an access control system

Identification	Authenticity	Data
Name (eg. in OCR) ID number Physical features eg. - hand geometry - voice PIN number	- Printed graphics - Colour - See list of machine reading technologies in section 3.1	Examples: - Company code 16 bit - Validity 4 bit - Time zones 8 bit - Spatial zones 16 bit - PIN issue number 4 bit - ID number 20 bit - Issue number 4 bit - Reserve 24 bit Total 96 bit

930 485e

Fig. 5 The information structure of machine readable cards

ing (for example telephone lines) or a dedicated link. So-called Modems installed at the ends of each communication link in the network allow the insertion and extraction of information from the data links. The individual characteristics of the system, for example centralized or decentralized, on-line or off-line, type of modulation or modems, have a decisive influence on the information structure needed in the cards. This is particularly true when a card must be altered after each reading operation, for example when a random number is generated by the central computer each time a card is used, and coded by the reader into the card.

We now examine the information structure requirements of a card. The identification information consists of the name of the card holder (for examle in OCR) and an ID number which can be visually and/or machine readable. The amount of functional data of course varies with the application: some typical requirements in terms of information capacity can be seen by reference to *figure 5*.

Additional information may be present to specify zone and time priorities. The inclusion of a personal identification number (PIN) which must be entered into a keyboard on entry, is also a means of obtaining high security. The PIN number may be obtained from the total card information by means of a complex algorithm which cannot be decoded in a simple way.
The authenticity information plays an important role (in contrast to the purely visual aspects of a card), and is intimately related to the technology chosen to provide machine readability. The possibilities are considerable (see 3.1) but an acceptable security - cost relationship must always be kept in mind.

3.2.2 Gasoline (petrol) card

As the next example we briefly consider a gasoline card. A gasoline card system is today typically decentralized and off-line i.e., the peripheral elements (the card readers) must contain considerable intelligence, and at the same time be available at an economic price.

The elements of such a system are illustrated schematically in *figure 6*.

The data structure of a card is very similar to that of an access control card, the combination of card and system must of course also permit the accounting operations involved for each transaction made using the card to be carried out economically.

3.2.3 Prepaid or «money replacement» cards

As an example of this type of application we consider the PHONOCARD® system which allows the use of the public telephone system by means of a prepaid card.

Cards for the system are made available to the public at convenient outlets – for example at Post Offices – and contain a number of value units representing cash value (say to a total of SFr. 20.—). The card user introduces the card into the slit of a reader built into the telephone cabin, and a display indicates the credit remaining on the card. When the telephone connection is made, the card is de-rated unit by unit for the duration of the call. At the termination of the call the card is returned to the user and may be used again for further calls until the capacity is exhausted. The requirements for the information structure of the card are self-evident. The personal identification information is no longer necessary as the card is anonymous and transferable, but system identification information must be present. The functional data must therefore identify the system together with the remaining credit. Authenticity information here becomes of paramount importance as the card effectively represents money. This information must be in a form so that copying, alteration, or forgery of the card is to all intents and purposes excluded. In addition to this, if the card is to be expendable, then cards must be capable of being produced in large quantities at very low cost.

This example raises the question of overall card security, and this is now examined in more detail in the following sections.

4. Security of cards and card systems

The secure operation of a card system, free from all fraud and other misuse, requires the development of a very well

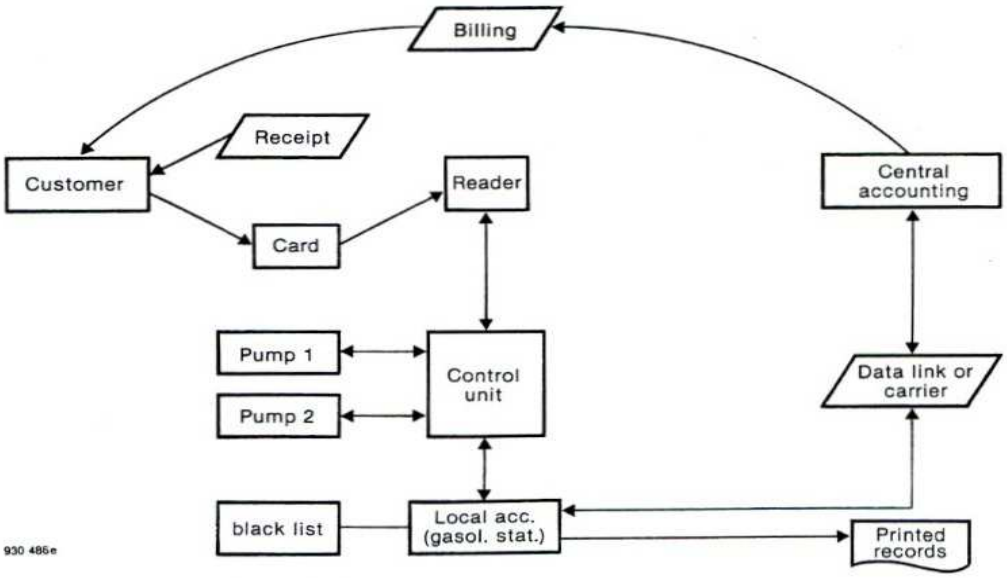

Fig. 6 Structure of a gasoline card system

thought-out security concept. The overall security is determined by the weakest link in the total system operational chain. An analysis of the various types of crime and misuse which are relevant, shows that danger can exist at at least two different levels: in the «life-cycle» of a card from its manufacture to its ultimate destruction, and in the possibility of manipulation of the hardware and software of the system (including the card). In this discussion we do not consider the security aspects consequent upon system reliability.

4.1 Security aspects of the card

Figure 7 shows a schematic representation of the life-cycle of cards in prepaid and identification card systems. We draw the distinctions between those major aspects which are associated which card manufacture, the system supplier and operator, the card distribution, the card user, and the visual or machine verification of the card and its destruction.

Clearly the security must begin with the card manufacturer, but the necessity for high integrity and scrupulous bookkeeping applies not only here, but equally to the further links in the chain, i.e. to the system supplier and operator, card distributor and finally the card user. In the fields of cheque cards, credit cards, and ID cards, the steps involved in the personalization of cards require similar measures to those associated with the manufacture of banknotes for the maintenance of security. Access to blank (unpersonalized) cards by unauthorized personnel must be completely exluded, and this dictates secure storage and transport facilities. This is particularly true for all prepaid cards. The card user as the final link in the chain can also influence the security: for example, the practice of writing down a secret PIN number of a access control card, either on the card itself, or on a piece of paper kept with the card, can constitute a security risk and should obviously be avoided.

The control of cards in circulation and their withdrawal can give rise to logistic problems. Should one withdraw expired cards from circulation either by rewarding the return or by not issuing a new card until the expired one is returned, or should the destruction of old cards be left to the card user? These are all important aspects which must be considered for both visually controlled and machine readable cards.

4.2 Hardware security

Security at the hardware level is concerned essentially with the nature of the authenticity features coded in a card (both for visual and machine reading) and with the equipment needed to realize the complete system. Not only the electronic apparatus is concerned (card readers etc.), but also the necessary constructional measures (the "bricks and mortar" aspects of security). The card itself must be proof against fraud, i.e. difficult to copy, difficult to simulate, and difficult to alter. Difficult in this context means that the investments or efforts necessary to copy, simulate or alter a card are considerable, and out of proportion to the return expected.

Very large systems, for example extended access control systems, require particular attention to security. The main danger here may lie in the possibility of technical manipulation of the equipment (eg. a card reader) so that valid electronic signals are transmitted to a central computer, without the use of a valid card, or by the use of techniques which simulate the behaviour of a card. Such possibilities must of course be eliminated.

The need for hardware security applies not only to the card readers, but equally to all elements of the system.

4.3 Software security

Software security is of major importance and is concerned with storage, transmission and processing of information within a system. The unauthorized extraction of data, or data tapping with the purpose of insertion of false information, or of unravelling coding algorithms used within the system, all represent danger areas which must be avoided, and which require today an increasing level of computer software expertise. With increasing system complexity, attention must also be given to ensuring that personal information about the users of the system is adequately protected and not available to unauthorized persons.

Passing now to the security of information stored in a card, it is useful to analyse the resistance of the three information types (identification, authenticity, functional data) to various hazards which may be encountered. This analysis is shown in tabular form in *figure 8*, and leads to the following conclusions:

The security of the identification information can be increased to a level which gives adequate protection against most of the expected areas of fraud or criminal attrack. Where the protection is still problematic (for example points 7 and 8 of *figure 8*), further security can be obtained by the use of adequate authenticity information. In general the functional data require a lower level of security, but again in exceptional cases where higher security is necessary, the functional data can be combined with the authenticity information.

These conclusions apply especially to cheque cards, credit cards, and ID cards, where the identification information is predominant. In the case of prepaid cards, which are anonymous and transferable, no protection is available from the identification information, and the security of a card rests solely on the authenticity information

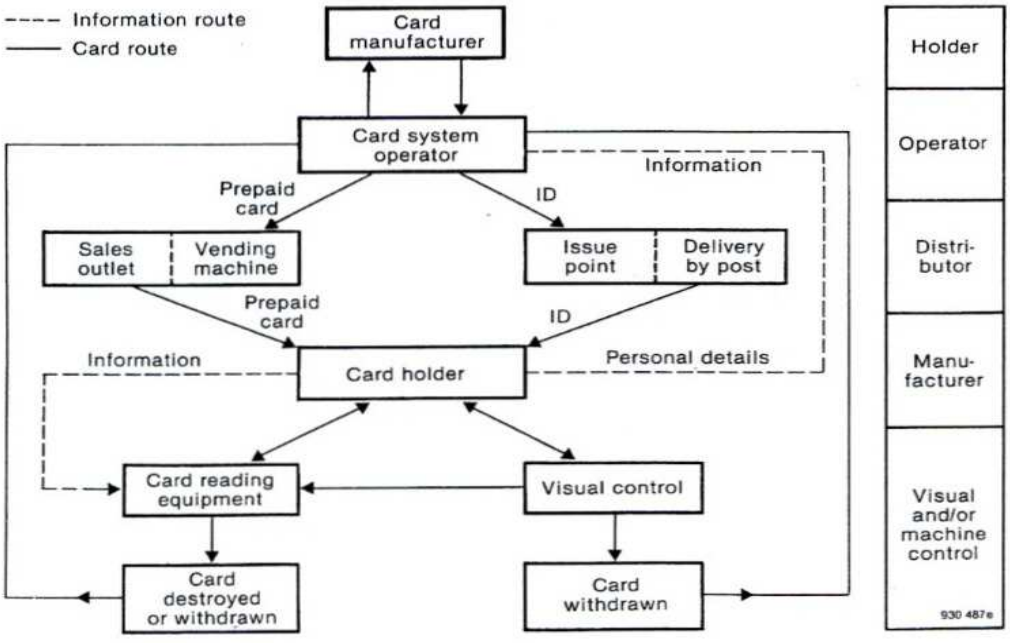

Fig. 7 Schematic representation of the life cycle of a card

which must be of the highest level possible, but still compatible with an acceptable cost. These cards represent money, and are susceptible to similar dangers to those encountered with banknotes.

5. The cost of security

To conclude we give some comments on the cost of security. An absolute security does not exist. Security is expensive but it is often necessary to pay the price which is entailed. Security should be such that the cost of defrauding the system is higher than the return expected. There is therefore little point in the introduction of security measures which cost significantly more than the loss to be expected from fraudulent use of the system.

Finally, it is important to reach an economic compromise which will be of a dynamic nature. As is well known, measures introduced to enhance security will eventually result in countermeasures, and flexibility must exist in order to deal with these situations.

Author: J.-F. Moser
LGZ Landis & Gyr Zug Corporation
CH-6301 Zug (Switzerland)

Translator: David L. Greenaway
LGZ Landis & Gyr Zug Corporation
CH-6301 Zug (Switzerland)

Dangers, forgeries, types of misue	Identification	Authenticity	Data
1. Loss of card (falls into wrong hands)	good (with physical feature and PIN)	bad	bad
2. Theft of a card	good (with PIN)	bad	bad
3. Theft of the information	good but not totally safe (fingerprints can be stolen, a PIN number seen or heard	depends on technology	
4. Card passed to third party	good (with exceptions)	bad	bad
5. Blackmail to obtain card information	good (with exception of the PIN number)	bad (see 4)	bad (see 4)
6. Coercion	bad (with exception of ALARM PIN)		bad
7. Mistaken entry or refusal of entry	problematic because physical features cannot be machine recognized with complete reliability	good	problematic
8. Copying, alteration, forgery	good, but not without problems	good, but depends strongly on technology (see list in section 3.1 in order of increasing resistance) Punched holes: weak Mag. stripe: weak Holograms: very good	bad, but can be improved by combining with authenticity information

930 486e

Fig. 8 Resistance of the types of card information to various hazards.