Cards and card readers for voucher and access control systems

UDC: 681.131.336.7.002.69:535.411
531.755.6:535.411

D.L. Greenaway

In this article a broad description is presented together with some of the technological background, of two new product areas. The first of these is concerned with the realization of card operated pre-paid voucher systems, and is typified in the following description by the PHONOCARD System which is currently being manufactured by Sodeco-Saia, a company of the Landis & Gyr Group. The second product area is concerned with the realization of card operated machine readable identification systems, and is typified by the ID 2000 access control reader currently being manufactured by Landis & Gyr in Zug.

1. Introduction

Both of these products are based on common information coding concepts where the need for high security plays a central role. Bearing this in mind, it will be realized immediately that in the following sections, the omission in a number of places of specific detail is both intentional and necessary. With this limitation it is nevertheless hoped that an interesting overview can be given of the application of a modern technology to an area of increasing commercial importance.

2. Applications

It is useful to separate the applications into two general classes: so-called voucher systems and identification systems. Each class is subject to a different set of boundary conditions in terms of the security concepts needed, and of the economics of manufacture of both the card and the related reading equipment. Consequently the two classes will where necessary be treated separately in the following sections.

Voucher applications are typified by the PHONOCARD System. The PHONOCARD unit is a full replacement of the present coin box station used in the public telephone service. The PHONOCARD station (shown in *figure 1*) contains no money or coin box, but accepts a pre-paid card representing a number of value units. The value units (up to 120 in the simplest form of the card) correspond to the tax units of the telephone network and are debited at the appropriate rate during the course of a call made using the card. The card is a one-way card and cannot be recharged, but can be used repeatedly for both local and long distance calls until the capacity is exhausted.

Fig. 1 PHONOCARD station

The PHONOCARD station gives a visible indication of the balance of units remaining in a card, and in addition a card will be available where the balance is at all times visible on the card itself. The system has high user-convenience, particularly for longer distance calls, when the correct small change presents frequent problems with traditional coin-boxes, also the pre-payment does not in effect represent any meaningful financial loss to the user. The system operator obtains a significant benefit from the accumulated pre-payment, and in addition saves the expense of collecting, counting and recirculating large amounts of small denomination coinage. In a number of countries, the absence of coinage is expected to lead to a reduction in vandalism — a factor which can heavily influence operating costs.

The pre-paid card and the reader which is incorporated in a PHONOCARD station, are not restricted to telephone applications, but can be used wherever automatic revenue collection is needed. Some examples are:

- petrol vending from unattended petrol pumps,
- the collection of parking revenue from large car parks,
- the payment of electrical energy by means of a card reader connected to an electricity meter,
- Public transportation revenue collection.

As concrete examples of the varied applications, the PHONOCARD system is at present undergoing public field trials in Belgium under the auspices of RTT, the Belgium telephone organisation. It is planned to initiate field trials in several other countries including France, Austria, and Switzerland during the course of 1980. Petrol vending using a pre-paid card has been in operation within the Sodeco-Saia Geneva plant for the past year. The introduction of a parking system using the card is planned to commence at two locations in the Zurich city area early in 1980.

The second general class of applications is concerned with personal identification, and is represented by the ID 2000 access control reader and card.

In the simplest form, the readers and cards function as a sophisticated key system allowing access to a number of locations with pre-determined time and zone priorities depending on the information coded into the cards issued. Readers can operate autonomously or may be connected to a central processing unit which allows a whole range of additional features to be incorporated.

The basic card reader (shown in *figure 2*) contains no transport mechanism, the card is inserted by hand and passed through a slot to enable the card information (which is not visible) to be collected by an optical head within the reader. Cards in their issued form are either neutral for pure access control use, or are combined with an engraved photograph of the user and other graphic information to serve as a means of visual identification (for example a badge to be worn by the holder).

Access systems, such as the ID 2000, which can offer high security, have a significant part to play in the whole security industry which is an area of dynamic growth in todays unsettled world. Although the applications of the ID 2000 are at present directed mainly at the problems of controlled access to specific locations and equipment (for example access to a computer terminal), we expect the future to bring an extension into the wider field of general identification, ranging perhaps from the control of financial transactions to passport checking.

3. Principles

The coding methods used for the cards for both the PHONOCARD-type and the ID 2000 systems are based on holographic techniques. A hologram is the record of the interference between two or more fields of mutually coherent radiation, and the spectacular aspects of this type of record – including 3-dimensional images reconstructed with a visible laser beam — are well known. Such 3-dimensional holograms are in general characterised by an extremely high information density (the hologram may contain up to 10^8 bits of image information per square millimetre), and extremely high resolution (the image information is recorded as a spatial modulation of for example absorption of light at spatial frequencies of up to 1000 lines/mm or even higher). The high spatial frequencies involved, necessitate a highly specialized technology for hologram recording, and this aspect alone can provide security against for example forgery. The high resolutions are retained in the application of holographic techniques to our card systems, but to meet the need of a machine readable system, the information content is drastically reduced. This reduction in information content has two important consequences both of which relate to the economics of producing a viable reading channel for this type of information. Firstly only a small number of dectectors is needed in a reading channel. A large number of detectors causes an immediate escalation of reader cost. Secondly, because the information content is small, a laser light source is no longer needed to reconstruct the holographic information, and an incoherent (for example a light emitting diode) light source can be used in the reading channel.

In the voucher and identification systems described here, a holographic recording is buried within the card structure during the card manufacturing process. The reader contains an infrared light source and optical system, which interrogates the buried recording and produces a characteristic signal at the detectors which establishes the authenticity of the card. In a voucher system – e.g. PHONOCARD – the card carries a sequence of such recordings, and each field must produce the correct optical signal. The debiting operation is carried out thermally, and the recordings are destroyed successively by means of a heated erasing head within the reader which is triggered by the tax pulses from the telephone line. Erasure is accompanied by a characteristic change in the detector signals, and provides a further control of the authenticity of the card.

In the case of identification systems – e.g. ID 2000 – the reader contains no erasing head. The card contains instead a coded sequence of recorded fields. Each field must produce a characteristic signal at the detectors, and the particular sequence of signals produced as the card information is scanned within the reader is related to digital information (typically 96 bits) recorded in the card.

Fig. 2 ID 2000 card reader

Compatability between cards for two different systems, e.g. telephone cards for two countries, is not in general desired, consequently each major card user requires a unique authenticity code. Here, the geometry of the reading channel and the number of sources and detectors used in a particular channel provide the necessary degrees of freedom so that a sufficiently large set of unique codes can be provided.

The principles described above particularly for voucher cards, are of limited application unless a manufacturing method is available with which large quantities of cards can be produced at an economic price. Such a process is now available and the realization of this technology has involved a major development effort within Landis and Gyr over the past few years. Section 5 below, describes this technology in general terms.

4. Coding logistics and security

4.1 PHONOCARD and allied systems

The production of voucher cards is analogous to the production of banknotes in that large numbers of cards must be produced which (apart from a serial number for administrative purposes) are identical. Differentiation between systems is achieved by the use of a different optical authentification code for each system. Within a particular voucher system a further subdivision of card coding is possible in the form of an optical pre-code or address applied to each card. The pre-code allows the system operator to include additional information concerning for example tariffs, times of issue or validity of a card, or to identify a specific sub-system where the card is valid. The pre-code is applied during card manufacture, consequently the cards when manufactured have an immediate cash value. Appropriate security measures covering both the handling of cards, and the full control of all cards produced, are an essential part of the manufacturing and distribution operations. When cards are in circulation, the security against fraudulent misuse of the system, for example by card forgery or manipulation, is assured by the complex nature of both the card coding and the technology needed to produce cards. From this viewpoint we believe that these systems have the highest currently available security for this type of application.

Fig. 3 Card components:
optically coded component
neutral card cover
laminated photoengraved card

4.2 ID 2000 System

Because of the personalized nature of access or identification cards, it has been necessary to develop card logistics which can safeguard the security of the card coding through the various stages of manufacture and distribution. ID 2000 cards are made with two initially separate components, a coded machine readable component and a component with graphic information. As with voucher systems, the machine readable component of the card is manufactured with the holographically recorded code which uniquely identifies a major system or set of systems. The as-produced cards are not readable in an access-control reader but must undergo two separate supplementary coding steps using two different card programming units. The first of these steps (involving a coded sequence of erasures in the optical field) is used to define a particular sub-system. This first coding step is carried out within the card manufacturing organisation. The second step is used to code individual user information into the card. For high security applications, the second programming unit is in the hands of the system operator who is able to determine an algorithm which converts the personal information to be coded, to the particular coding sequence applied to the card. The operators programming unit will only accept cards which contain the appropriate sub-system address thus the coding sequences and the individual user information do not come into the hands of card manufacturing personnel, and in addition a system operator is only able to programme cards destined for his own system. After the appropriate information has been coded, the coded card is laminated to a second component bearing graphic information, by means of a specially developed laminating unit. The graphic component is either neutral – i.e., it carries no personal information, or is personalized with an engraved photograph of the card holder and other personal information such as a signature and department number. The choice of the second component allows the final laminated card to be used either solely as an access control card, or as a combined identification card and access control card. Large system operators have the possibility therefore of coding and issuing cards of both types from their own premises. This results in maximum security and a minimum time delay in issuing new or replacement cards. *Figures3* and *4* show examples of the various card components, and the three pieces of equipment – programming unit, photoengraving unit, and laminating unit – used for the personalization of cards.

5. Card manufacturing technology

5.1 Printing matrices

The key to the large scale manufacture of cards for the applications described here lies in the realization of special printing matrices which are used to create the high resolution optical information within the card structure. The printing matrices are the result of a chain of carefully controlled operations which begins with the holographic recording in a suitable photosensitive medium of the authenticity pattern for a particular system. The coherent radiation for this step is produced by a laser, and the recording is made under conditions of extremely high mechanical and thermal stability. The optical system used must be completely isolated from building vibrations and thermal fluctuations. The exposed recording is developed and then a series of metal replicas of the recording are made which are formed into printing plates for the production of cards. Each printing plate can be used repetitively for a large number of cards.

5.2 Card manufacturing

Card manufacturing begins with the preparation of a suitable substrate material. The material is derived from two plastic foils which are laminated together at the start of the manufacturing chain. Each foil is subject to stringent acceptance conditions with

respect to uniformity and optical properties and is handled under conditions of extreme cleanliness. After lamination, card blanks are stamped from the foil and are passed through a chemical cleaning process in preparation for the printing operation. The high resolution optical information representing the value units or the identification field is then applied to the card blanks from the printing matrices. After printing, the optical information is covered with protective lacquers which also serve to protect the information from damage during the life of the cards. After testing and inspection, the cards are embossed with a running serial number and packed ready for shipment.

The operations involved in card manufacturing are such that, with the exception of a visual quality control for cosmetic defects, a high degree of automation can be employed. This automation is currently being introduced into the card manufacturing area. Automation not only leads to a reduction of costs but also plays a major role in maintaining the high degree of cleanliness essential to the card manufacturing in that physical handling during the production is held to an absolute minimum.

5.3 Control and testing

Several different aspects are involved here. Firstly, all cards must fulfil a set of optical criteria that ensure that the cards will be accepted by the subsequent reading equipment. For voucher cards where every unit represents a sum of money, this means that the optical properties of each unit must be controlled. For a 120 unit voucher card several hundred measurements are necessary for each card where each of the measured signals must be between predetermined minimum and maximum absolute values. These measurements are carried out using automatic test equipment in which cards are taken from a magazine, passed through a high speed measuring station, and sorted into "accept" or "reject" magazines. The signal evaluation is performed with the aid of a desk computer which is also used to assemble statistics on the signals measured for each batch of cards. Unless required for evaluation purposes, rejected cards are destroyed using a granulator and are not permitted to leave the manufacturing area.

In addition to the optical tests, tight control over all card dimensions is necessary to ensure that cards can be correctly inserted in the reading equipment. A visual control of card quality is also made to eliminate cards with for example printing or other surface defects.

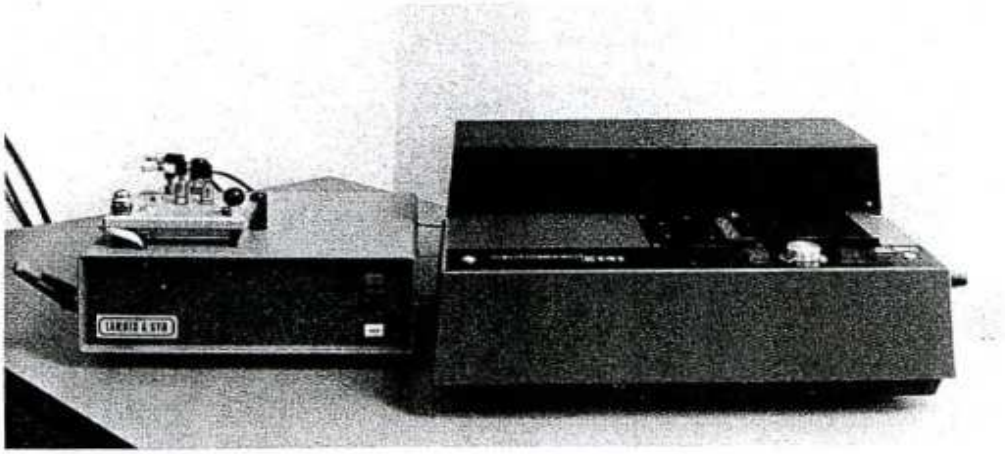
A different but nonetheless vital aspect of control is concerned with the security of the card production operations, in many ways similar to the production of banknotes or other security documents. The need for control exists in three different areas: the limitation of access to the considerable amount of technical information together with coding details involved in the whole production chain, physical security measures to protect sensitive materials such as the printing matrices and stocks of finished cards within the manufacturing areas, and the presence of an inventory and bookkeeping system which enables complete control to be exercised over all cards produced. These security measures lead to increased but unavoidable additional costs in card production. Admittance to all locations concerned for example with matrix and card production is restricted, and entrances are protected with an access control system; visitors must be accompanied at all times by responsible personnel. Alarm systems provide an indication of unauthorized access at times when the production areas are unoccupied.

6. Card reading and related equipment

6.1 PHONOCARD and allied systems

The PHONOCARD station consists of two basic modules: the card reader and the related electronics, and the telephone system related electronics which is coupled to the card reader, and also interfaces with the telephone line, handset and dialling mechanism. Here we are only concerned with the reading module. Cards are inserted against light spring pressure through a slit on the front panel of the case. A hemispherical depression at the centre of the slit enables part of the card to be seen when in position, and serves as a visible reminder that a card has been inserted. The reader contains a clamping mechanism that prevents cards from being withdrawn when a call is in progress. The clamping mechanism does not operate when an invalid card (for example a blank card or a card from another system) in inserted, or when there has been a power failure. In these cases the card is immediately ejected part-way from the slit. Part-ejections also takes place when a card is exhausted, or when a call is terminated by replacing the handset. The remaining credit on a valid card can be checked at any time by inserting the card without removing the handset. A liquid crystal display shows the number of units remaining, and after 1 second the card will be ejected. For a normal call, the handset is first removed, and the card inserted; an optical head driven by a small stepping motor scans first the authenticity code to establish card validity, and then the individual value units to establish both authenticity and the credit remaining on the card. The number is then dialled (push button

Fig. 4 Equipment used in card personalization: programming unit



laminating unit and photoengraving unit

dialling); when the connection is made, a short heat pulse is applied to the value unit field by means of an erasing head in contact with the card. The change in optical signals is monitored during the erasing operation; if the expected change is measured, then the optical head and coupled erasing head are stepped to the next value field and the authenticity check repeated. The timing of the erasing operations is of course determined by the distance called, and the necessary pulses are transmitted through the line from the exchange. The PHONOCARD reader can erase up to 3 units per second, and can thus be used for transatlantic calling if desired. An additional feature is incorporated which allows the caller to insert a new card if a card will be exhausted during a call. 15 seconds before a card is due to expire, an optical warning is given (flashing light), which lets the user press a button to initiate rapid erasure and storage of the remaining credit on the card, and enables a new card to be inserted without breaking the connection.

For voucher card applications outside the area of telephony, where a high value unit capacity and fast derating are required, an alternative card reader has been developed in conjunction with Zuhlke Engineering AG (Schlieren). This reader is designed with a transport mechanism that draws the inserted card fully into the reader, and also has a facility for inserting a second card which is held in readiness. Card for this system have an extended value field and are coded with 200 value units in addition to the address field. The derating operation takes place at a frequency of around 10 units per second. The use of this reader in car-park revenue collection systems in the Zurich city area in planned for early 1980.

6.2 ID 2000 System

The ID 2000 access control reader contains no motor transport, instead the reading operation takes place when cards are passed by hand through the vertical slot on the front panel (see *figure 2*). The speed with which cards are passed through the slot need not be constant, and the card edge is held by the user for the reading operation which avoids the risk of cards being left in the reader. The reader is available either with or without a keyboard, permitting use in data collection applications (time checking etc.) or in high security access applications where a secret personal number must be entered. When used as autonomous units, the readers require only a low voltage supply. The logic contained within the reader establishes the validity or otherwise of an inserted card, (including comparison with a limited black list to exclude umwanted cards), and delivers signals which drive a series of potential free contacts. These contacts are used for the direct connection of a door-opening solenoid, an override facility (when exit from a restricted area is required) and either visual or acoustic alarm devices which indicate irregularities in use.

The readers may be connected to a central processing unit to allow a range of additional functions to be incorporated. These include full data logging for security and time checking purposes, immediate display by means of a video terminal of all traffic within the system, the maintenance of an extended black-list for undesired or blocked cards, and immediate central reporting via a series of alarm signals of irregularities within the system. Besides the readers and central processing unit, the additional equipment shown in *figure 4* is required for full operation of the ID 2000 system. For the highest security, or for large users these units can be located in the premises of the system operator and run by office personnel. The two versions of the programming unit (user address coding and end-user personal information coding) are mechanically similar but differ in their internal logic configuration to preserve the separation of the two coding operations. The necessary card information is entered by means of a keyboard and the coding sequences are applied to an inserted card automatically.

When photographic identification is required the second card component is provided with fields which can be engraved with an identification photo and other personal information. The photoengraving is performed with a commercially available unit which accepts a passport photograph of standard format as input and produces an engraved half-tone black and white image on the card. When no photograph is needed a neutral second card component is supplied printed with a appropriate graphic design.

The two components which constitute a finished card are bonded together using a small specially designed laminating unit. No additional adhesives are necessary. The two components are inserted into a template, and an automatic heating and cooling cycle applied which bonds the components together. When laminated, the two components cannot be separated without destroying the integrity of the card.

7. The relationship between security and cost

It can be seen from the above description that voucher and identification systems involve different security considerations, and that in general an increase in security will probably result in an increase in costs to the operator. From the standpoint of cost, the systems described here lie broadly in the middle-range of what is available from the palette of current technology: Systems using solely punched-hole or a simple magnetic-stripe coding are undoubtedly cheaper both for the reader and the information carrier, but offer little security; systems involving for example machine recognition of a voice-print, fingerprint or signature are potentially extremely secure, but are very expensive and in addition may be either unsuitable or aesthetically unacceptable for some applications.

The need for security for a particular application must be measured in terms of the total value which is at risk. Thus a system where a large number of small value transactions is involved (for example PHONOCARD) must be assessed in terms of the value of cards which are in circulation at any time, and will have a security requirement comparable to a system where a very limited number of large transactions may be involved (the restricted access of for example employees to a bank).

In the case of the PHONOCARD system, the security should not be based on the reading equipment – the theft of a telephone call station would present no difficulty to a criminal – but must rest in the card technology and of course the manufacturing and distribution organisation for the cards. This concept allows the reading equipment to be produced at an economic price (which is anyway essential), and permits the costs of the complex card manufacturing technology to be absorbed by the very large numbers of card which must be produced to satisfy the demands of the system. The number of cards needed also justifies the use of a highly automated production process, which enables the security inherent in this type of card to be obtained at an acceptable price.

For the ID2000 access control system, the security is shared between the card itself, the logistic chain which controls the coding of the final card, and the reader together with any terminal equipment which must contain sufficient intelligence to interpret the card information. The overall cost of security is necessarily higher than with the PHONOCARD system because of the wider range of pieces

of equipment that are needed, the smaller production volume, and the number of separate operations concerned with the individualization of cards. In addition to this, the installation of a secure access control system must be accompanied by appropriate attention to the physical ("bricks and mortar") security of the areas being protected and to the means of ensuring that the system is used in a responsible way.

In conclusion, it is clear that security is always relative, and that no system can be produced which is absolutely safe from criminal mis-use. For the two basic systems described here the security inherent in the technology has been matched to the particular needs of the systems and we believe that the financial outlay and level of technical knowledge required for any serious fraud constitutes a more than sufficient deterrent.

8. Acknowledgments

The realization of the PHONOCARD system, the related voucher systems, and the ID 2000 access control system has involved team efforts of a number of different divisions of the Landis & Gyr Group. It is not possible here to mention by name all those concerned with the manifold aspects of the work. It is a pleasure however, to acknowledge the efforts, cooperation and support of the members of the Staff of the Central Research and Development Laboratories of Landis & Gyr, of the Telephony Division of Sodeco-Saia SA Geneva, of the Comfort-Control-Systems Division of Landis & Gyr in Zug and of the manufacturing Divisions of Landis & Gyr in Zug who have been intimately involved in the realization of the systems described here.

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