Access control system ID 2000

UDC: 351.755.6:535.411

U. Wirth

The following is a description of the access control system ID 2000 which has been developed by Landis & Gyr as a means of authorising access by a holographically coded card.

The special feature of the system lies in the high forgery proof quality of the card and the large number of processing functions contained in the "intelligent" access control reading unit.

The following is a detailed account of the design and operation of the ID 2000 system and the use of the holographically coded card.

1. The ID 2000 card

1.1. Card makeup

The ID 2000 card consists of two PVC card components which are heat-bonded together after encoding and engraving the photo, signature etc. by means of the ID 2000 card heat seal unit.

One of the two components carries the two hologram bands:

The synchronisation track gives the reading unit the direction of movement of the card and the sequence for the various bits on the data track to be read.

The data track acts as the data carrier proper and contains the company code pre-coded by Landis & Gyr and the entire information specific to the customer.

The second card component forms a cover facilitating the engraving of a photograph, personal identity number, department reference, signature etc.

Figures 2 and 3 show two examples of this type of cover.

The size of the card corresponds to the ISO credit card size, being 85.7 × 54 mm.

1.2 Information carried by the card

The information is invisibly encoded on the card and cannot be recognised without knowledge of the card code and the bits distributed according to a specially selected algorithm.

The following information can be encoded on the card:

Company code:
Number to differentiate between the various Landis & Gyr customers. This code is pre-coded by and at Landis & Gyr and cannot be altered subsequently in any way, without rendering the card unuseable.

Territory range:

States those readers which will secure access to the card user.

Time range:

Shows that period of time during which the card user has access.

Validity:

States the validity of a card series.

Identification number:
Distinguishes between the various card owners.

Issue number:
Specifies the issue of the identification number.

PIN-Code:

This code gives the number of PIN digits. (PIN = Personal Identification Number which in any event can be fed-in via the keyboard after card has been inserted.)

Fig. 1 Encoded holo card

Fig. 2 Cover without customer-specific data

Fig. 3 Cover with card user data

2. Encoding of the ID 2000 card

2.1. Sequence of customer-specific card preparation

The operator of an ID 2000 system has basically two alternative modes for encoding and designing his ID 2000 card.

a) The card is supplied by Landis & Gyr ready for use:
This option means that the client provides Landis & Gyr with all information necessary for encoding the card on a pre-printed form *(fig. 5)*.
The client will provide the artwork *(fig. 5)* for engraving the desired data relating to the card owner (photo, signature, personal reference number) so that these particulars can be engraved on the cover *(fig. 3)*.

b) Landis & Gyr supply the pre-coded holo card and the non-engraved cover:
In this option, the client will have his own card programming *(fig. 6)* and thermo-sealing unit *(fig. 7)* for encoding the card and bonding it to the cover. The client will also supply the desired engraving of the cover using his own photo engraving unit *(fig. 8)*.

Option b) gives the operator of a ID 2000 system the following advantages as compared with option a):

- The data required for encoding the card need not be disclosed to Landis & Gyr who supply the cards. This means that the card supplier will not be enabled to obtain unauthorised access to the client's premises.
- The issue of new cards in the event of card loss or personal identity change can be despatched through the normal goods forwarding channels.

2.2. The ID 2000 card programming unit

An ID 2000 card programming unit *(fig. 6)* is available for encoding the holo card *(fig. 1)* with data specific to the customer.

The unit is operated and controlled via the display screen terminal. To start the unit, the operator must feed in a personal identity number via the terminal. If the unit is not used within the following five minutes all input data will be automatically blocked until the user re-presents his personal identity number.

After the unit has been released the user is requested by a clear text output to in-put the various card parameters and subsequently to start encoding the card.

If the unit is also fitted with a printer all parameters will be printed out complete with the date and the user's name while the card is being encoded. At the same time, a comparison is carried out between the company code pre-coded on the card and the company code permanently programmed in the programming device. If this comparison check leads to a discrepancy being detected an error statement will be printed out and the card will be encoded such as to render it unsuitable for further use.

The in-putting of a personal identity number and the comparison check for the company code is to prevent encoding being carried out by an unauthorised person or by an authorised person on someone else's programming unit. The encoding time proper with the print-out takes less than 1 minute.

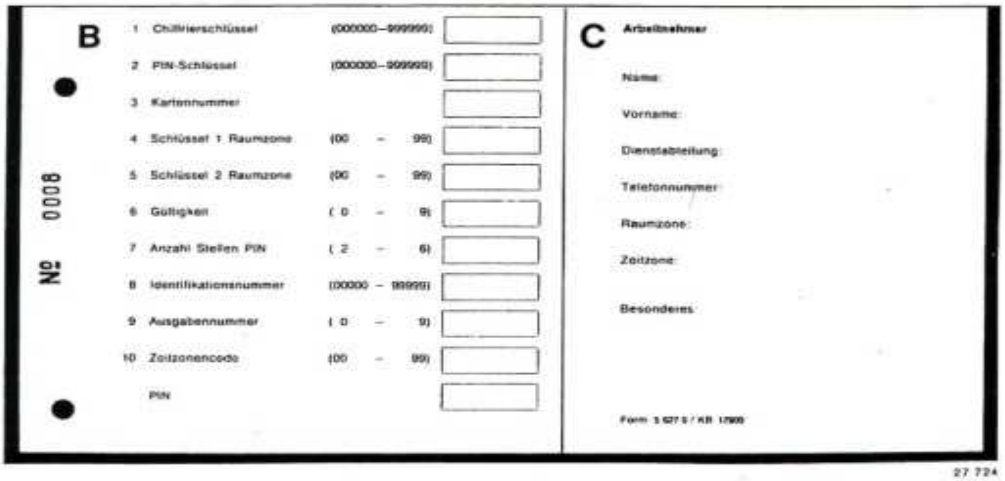


Fig. 4 Form for encoding the card

Fig. 5 Artwork for engraving the cover

2.3. The ID 2000 card bonding unit

The ID 2000 card thermo-bonding unit *(fig. 7)* is designed to thermoseal the cover *(figs. 2 or 3)* on to the encoded holo card *(fig. 1)*.

The thermo-seal unit is extremely easy to operate, simply by inserting the two card components into the card holder and by subsequently closing the thermo-seal mould and pressing the START button. The thermo-melting process will be complete after about 1.5 minutes.

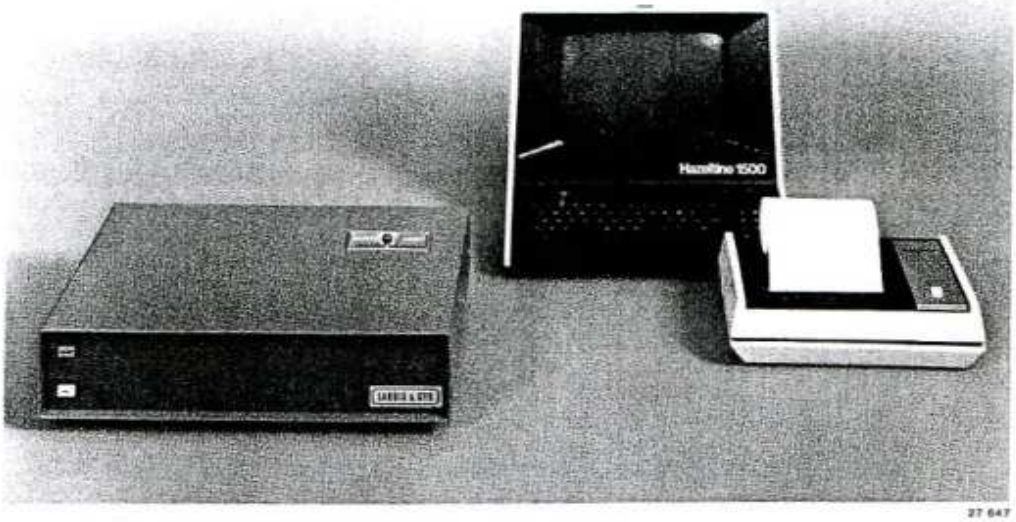
2.4. Photo and text engraving

The Identograph K141 *(fig. 8)* is used to produce the black/white gravure on the cover *(fig. 3)* according to a given artwork *(fig. 5)*. The data on the artwork can also be entered by hand (e. g. signature).

3. The ID 2000 reader

3.1. Design

The ID 2000 reader is divided into a wall recess mounted unit and a wall mounted housing. The in-wall unit houses all connection terminals for the reader so that the supply cables can be laid inside the wall or fed in direct from the secured room. The in-wall unit can be mounted and wired without any electronic modules being plugged in. The flush mounted part is a solid (2 mm chrome steel sheet) and splash waterproof (DIN IP54) design. It is secured to the in-wall housing by a safety lock the position of which is monitored by the reader. To prevent the flush mounted outer housing being drilled open a "surface guard" is fitted which will cause the reader to release an alarm as soon as the walls of the housing are damaged.



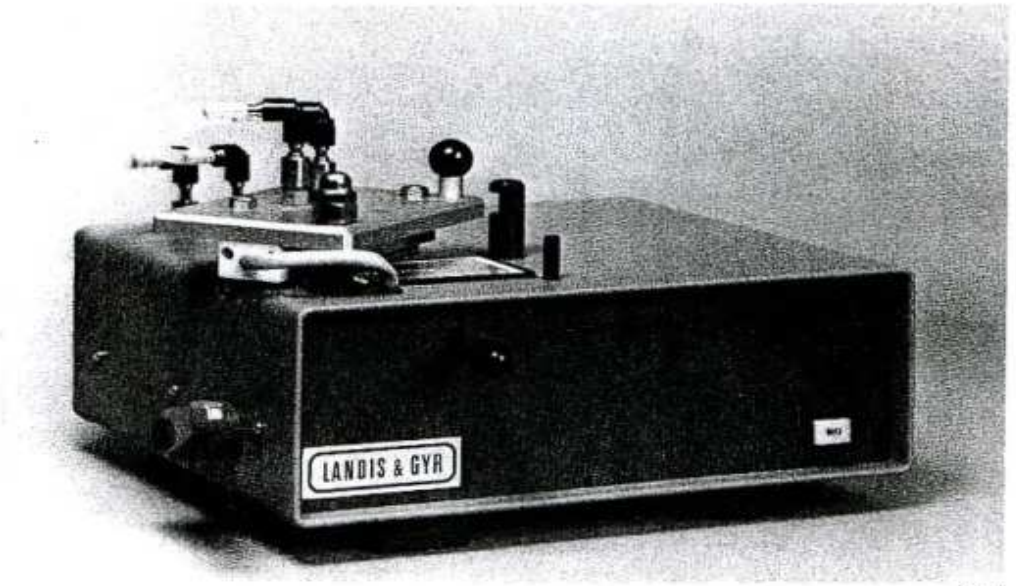
27 647

Fig. 6 ID 2000 card programming unit with display terminal and printer

3.2. Card reading sequence

The ID 2000 reader has been carefully designed to ensure no moving parts and no card infeed aperture are required which might have given rise to the reading mechanism being damaged as a result of incorrect operation, willful intervention through the infeed aperture or by the mere wear of the moving parts themselves. For this reason, the reader has been designed on a principle allowing the card to be pulled by hand through a card slot.

Reading the card will thereupon involve its being scanned by a light source illuminating the hologram bands incorporated in the card and deflecting the light at closely defined angles towards the light-receiving devices of the reading head. The light will then be checked for intensity as it is being received, thereby facilitating the detection of false or falsified/altered cards.



27 639

Fig. 7 ID 2000 card thermo-bonding unit

3.3. Storing the reader parameters

The ID 2000 reader must have a certain number of variable parameters so as to enable it to carry out a complete, autonomous evaluation of the card. The setting and adjustment of these parameters shall be described next.

The *company code* is permanently inscribed in the reader by Landis & Gyr and will be compared with the company code on the card when the latter is being read.

27 643

Fig. 8 Photo and text engraving unit "IDENTOGRAPH K141" manufactured and supplied by Hell GmbH

The *territory range* can be in-put by the operator of an ID 2000 reader by means of encoding plugs. The plugged code will indicate the territory or zone to which access will be made available according to a pre-determined key program and a territory key encoded on the cards.

The parameters below are stored in a semi-conductor memory and can be varied during autonomous operation via the reader operating unit *(fig. 12)* or from a central control station in the case of system operation.

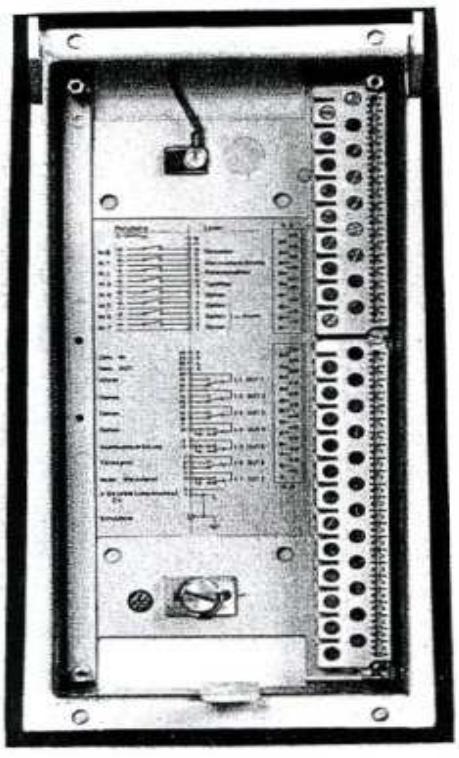
The *validity* is compared only with the validity code on the card.

The *decipher key* is the algorithm applicable to the deciphering of the data held on the card.

The *PIN key* is the algorithm applicable to the calculation of the PIN. The calculated value is compared with the code printed-in on the typewriter.

The *time range list* can hold a maximum of 10 time ranges. The timing unit inside the reader will set the various time limits either actively or passively as required.

The *black list* can carry a maximum of 40 lost or invalid cards.



27 655

Fig. 9 ID 2000 reader — Wall recess mounted part with connection terminals

3.4. Autonomous operation of the ID 2000 reader

a) Card evaluation

After a card is read the information it carries is checked for the following criteria:

- Are the signal levels of the data read within certain limits? This is to allow the detection of wilful card alteration
- Checking the deciphering algorithm.
- Checking the company code, the territory range, the validity, the time range, the black list and the PIN in any event (the latter is to be printed-in on the typewriter).

If these tests produce a positive result the reader will allow access by keeping the gate/door open for a certain time. After a gate/door has been opened the hold open duration is monitored by the reader.

b) External input/output contacts

The ID 2000 reader offers the use of relay contacts for command outputs and galvanically separated statement inputs.

The output contacts carry command outputs such as the operation of the door magnet, the local warning and alarm signal, the suppression of the alarm and three contacts which can only be operated from the central control station. Of the statement inputs, three contacts are reserved for controlling the gate/door and the remaining five for transmitting information about the condition of the reader to a central control station with which it may possibly be linked up.

27 653

Fig. 10 ID 2000 reader with external flush mounted part opened up

3.5. Programming an autonomous ID 2000 reader

As shown in *figure 12* a special operating unit may be connected to the reader for input purposes or for changing the reader parameters. This ancillary device will also be very useful during commissioning or trouble-shooting as an aid for operating the external input/output contacts and for checking various state registers.

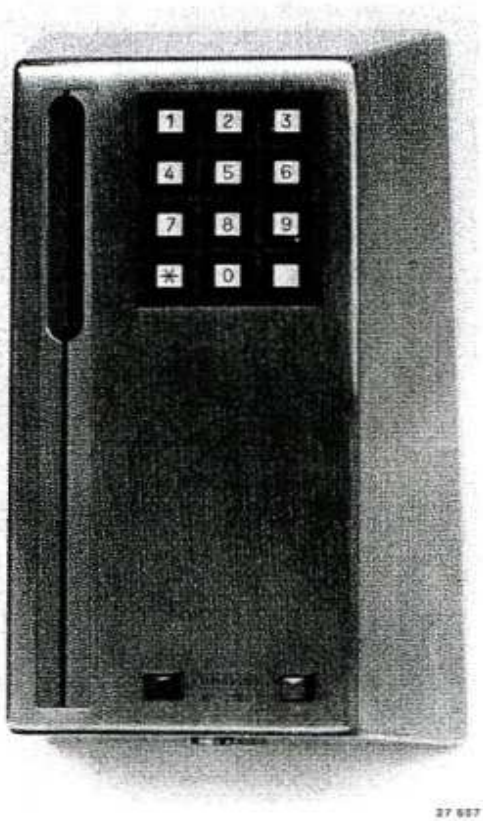
4. The ID 2000 reader in the VISONIK® building automation system

4.1. The makeup of the VISONIK system

The Landis & Gyr VISONIK building automation system incorporates access control as a part function with the ID 2000 reader.

Figure 13 shows the structure of the VISONIK system.

A maximum of 120 ID 2000 reader may be connected to the VISONIK system by means of 6 two-core ring lines.



27 657

Fig. 11 Closed ID 2000 reader

4.2. ID 2000 reader function in system operation

In system operation, the reader will carry out the same functions as in autonomous operation (see section 3.4) by reporting all changes of the external input contacts and the evaluation of the cards to the central control station.

Card evaluation:

After a card is read the reader will report all card data and the appropriate evaluation and decision to the central control station. If the reader does not report in its card evaluation a full black list or an inactive time zone it will make independently a positive or negative decision, even in system operation. Otherwise, the reader will await a decision from the central control station.

This card evaluation mode means that only exceptional incidents are dealt with by the central control station so that a very quick access response will be assured at any time even when the systems concerned are very extensive ones and the various readers heavily used.

Switching over to autonomous operation

If the data ring line is damaged or faulty or if the access response is not forthcoming from the central control station after a card has been evaluated by the reader, the latter will automatically switch over to autonomous operation. It will thereupon continue operating independently until the central control station gives the return-to-system-operation command.

4.3. Duties to be met by the central control station

a) Access response:

The central control station has the following three lists to arrive at a decision on access:

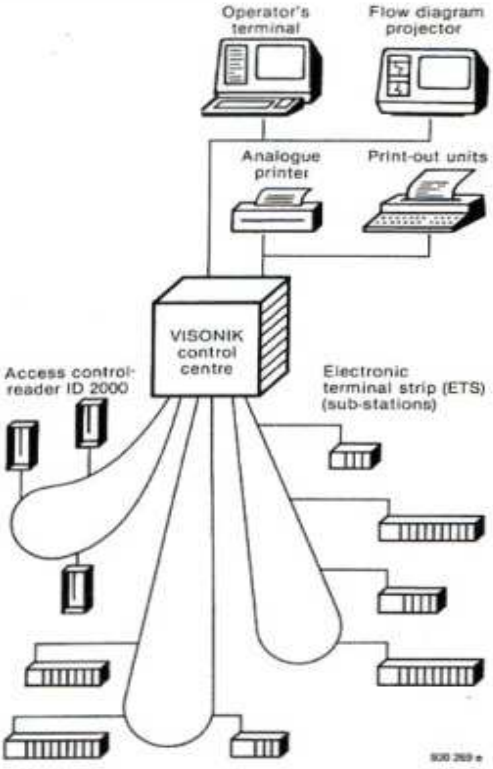
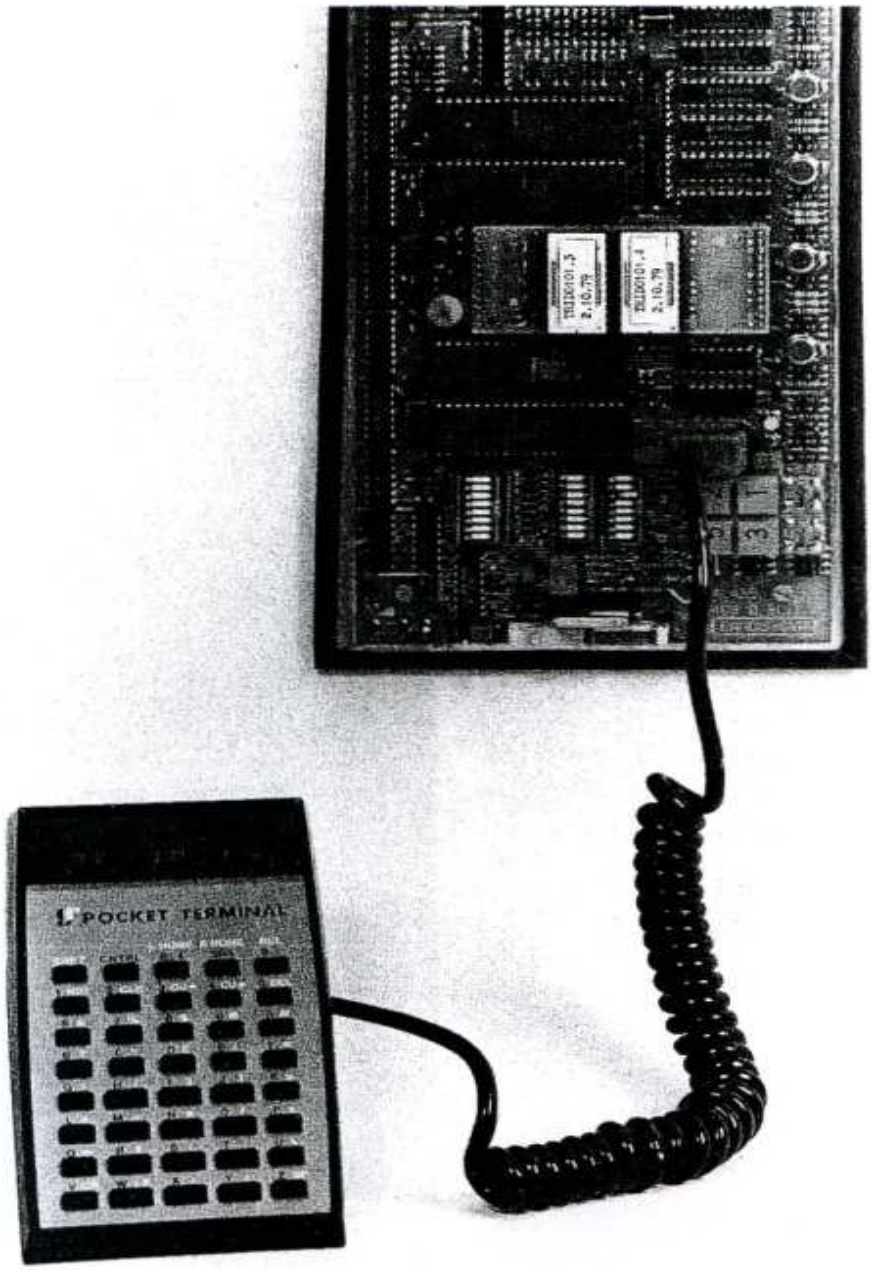


Fig. 13 Makeup of the VISONIK system



27 654

Fig. 12 ID 2000 reader operating unit

25 743

Fig. 14 VISONIK system operating station

- The black list serves as an extension of the local lists inside the individual readers.
- The time limit list serves as an extension of the local lists inside the individual readers.
- The access list has the capability of listing temporary exceptions in connection with the time range list.

b) Recording:

All alarm statements or reports from the readers and the card data in the event of a negative access response are automatically recorded.

c) Operation:

The following functions can be executed via the control console:

- Varying all parameter lists inside the readers and in the central control station.
- Allocating the output medium (printer, disc) to the spontaneous reader statement or report.
- Directly changing the correlation of the reader's external contacts to the central control station or assigning a time switch or reaction program.

Author: Ulrich Wirth
LGZ Landis und Gyr Zug Corporation
CH-6301 Zug (Switzerland)

Translator: Sally Walker
Language Services
43 Nicholas Street
GB-Bristol BS1-1TP

Fig. 15 Supervised entry zone of an administrative building of the Swiss Confederation. The revolving doors will only be opened, when the access control readers ID 2000 have identificated the authorization of access.

www.optical-cards.com
Alain Knecht, June 2009