

A system for cashless transactions

The present invention relates to a system for cashless transactions having a data carrier with an embedded IC and a terminal for communicating with the data carrier or IC, a read-only memory provided in the IC containing an initial credit which is gradually reduced in accordance with the transaction selected by means of the terminal.

A data carrier or electronic card of the abovementioned type is known for example from DE-A 30 29 641. The card described in the reference having an electronic circuit and a memory with erasable and writable memory cells is suitable for using a great variety of goods and services machines, for example telephones, drink dispensers, food dispensers, highway toll machines, etc.

The known card belongs to the category of so-called debit cards. It uses a nonvolatile memory comprising a multiplicity of memory cells which is erased globally but written cell by cell. Before the card is issued the memory is erased so that the initial state corresponds to the erased state. This initial state is equated with a certain money value which entitles the user to avail himself of goods or services. At each use of the card the initial value is reduced by memory cells being written in accordance with the particular service utilized until the memory is completely written. Each memory cell thus represents a certain unit of value (smallest deductible unit) so that the total number of cells determines the total value of the card.

To prevent a used-up card from being returned to the initial state, i.e. the erased state, with intent to defraud, a line of the memory comprising several cells is loaded with a code which can only be written to memory once and which is checked for correctness at each transaction by the particular inquiry device or terminal. If an attempt is made with intent to manipulate to erase the memory, i.e. reset it to the initial state, this also erases the code since the memory can only be erased globally. Since the code cannot be written to memory a second time, as mentioned above, the card is now useless. The known card seems to be sufficiently protected in terms of security but has the disadvantage that memories with a relatively high number of cells must be provided for customary use of the card.

To permit flexible use of a card of the stated type in a great variety of fields of application one must make sure that the value per deductible unit is as small as possible, on the one hand, and the number of deductible units, i.e. the maximum value of the card, can be as great as possible, on the other hand. If the value per unit is to be one penny and the maximum value of the card DM 200, for example, the known card thus requires a memory of about 20 kilobits solely to deduct these 20,000 units.

Large memories require large chip surfaces and are therefore known to be accordingly expensive. Particularly

for the stated applications in which the data carrier will be a mass-produced article it is of crucial importance to find a cost-effective solution. Integrated circuits with large dimensions are accordingly to be avoided if only for reasons of cost. However they are also disadvantageous because they are known to break much more easily than circuits with smaller dimensions when being incorporated in flexible cards and also during use of these cards. Although it is possible to implant large circuits in cards with a sufficiently long life, the necessary measures of card technology are relatively elaborate and generally unreasonable for cheap cards due to the higher costs involved.

The invention is therefore based on the problem of proposing a data carrier having an integrated circuit which is highly flexible in application but requires little memory and involves no disadvantages in terms of security.

This problem is solved by the features stated in the main claim.

In a preferred embodiment of the invention the integrated circuit provided with control, data and supply lines includes a volatile counter operated in the known way with a clock signal, and a nonvolatile memory adapted to the size of the counter. The integrated circuit also bears a control and safety logic which processes the signals applied to the control and data lines and controls the data transfer between counter and memory in the way explained below.

An example shall illustrate how the integrated circuit manages with a small memory volume in the inventive solution despite a low value as the smallest deductible unit and a relatively high initial value.

Let us assume the counter is a 16-bit counter and the unit of value per clock pulse corresponds to one penny. In this configuration it is possible to reach a total value of about DM 650 with a memory having only 16 memory cells. The ratio between memory size and maximum value of the card with a simultaneously low value per unit is thus considerably improved in comparison to known data carriers. This substantial saving of necessary memory volume and thus also chip area considerably reduces the price of the circuit and that of the card due to the simplified production. This is not altered by the fact that a control and safety logic must be additionally provided on the integrated circuit in the inventive embodiment. It has turned out that the additional effort for the logic required by the inventive solution to protect against manipulations is relatively low and thus hardly diminishes the advantage obtained by the dramatic reduction of memory. Although data carriers according to the invention are thus much cheaper to produce than known data carriers they have no disadvantages in terms of security.

The control and safety logic provided on the circuit ensures, among other things, that before each transaction an initialization process automatically takes place which cannot be influenced with intent to defraud. The particular residual value present in the memory or, upon the first use

of the data carrier, the initial value is thereby transferred to the counter, among other things. The counter is designed such that, driven by clock pulses, it can count only in the direction that reduces the value transferred from memory. During or after the transaction the counter reading reached is transferred to memory so that the memory value is likewise reduced by the number of used-up units.

The inventive solution makes it possible to realize a data carrier having an integrated circuit which can be produced cost-effectively and implanted in a data carrier due to the little memory required with a relatively small surface. The circuit is thus usable as a mass-produced article in a great variety of fields of application. It is easy and costs virtually nothing extra to assign different card values by changing the number of deductible units per card, or to change the value of the individual deductible unit while retaining the total value of the card. If one extends the memory and counter by only one memory or counter position in the inventive solution one can double the total value of the card, for example. In the known card this goal can only be reached by doubling the total memory.

Further advantages and developments of the invention will result from the subclaims and from the following description of embodiment examples with reference to the Figures, in which:

Fig. 1 shows an integrated circuit according to the invention in an exemplary embodiment,

Fig. 2 shows a schematized representation of a memory in the erased and in the loaded state,

Figs. 3a and 3d show the different phases during a transaction,

Figs. 4, 5 show detail circuits of the control and safety logic shown in Fig. 1.

Fig. 1 shows an exemplary embodiment of integrated circuit 1. Only the elements necessary for understanding the invention are shown, namely memory 2, counter 3 and control and safety logic 4.

Memory 2, which has for example 16 memory cells, is produced by so-called E²PROM technology. These memories are nonvolatile memories that are electrically erasable and writable. A memory cell of this type of memory is written by applying a charge to a so-called "island" of the cell. A memory cell is accordingly erased again by removing the charge from the "island". Electric erasure and writing are performed via separate lines.

The integrated circuit contains along with memory 2 volatile binary counter 3 that comprises for example 16 bi-stable flip-flops. The counter is constructed such that the binary number provided at the outputs is lowered by one at each clock pulse.

Counter and memory are interconnected via data and control bus 5, 6 with control and safety logic 4 likewise located on the circuit. Between memory 2, counter 3 and logic 4 the data are processed in parallel form. In control

and safety logic 4 there is a parallel-serial converter that permits communication with corresponding output devices in serial form.

Control bus 5 contains the signal lines necessary for controlling the units, for example a clock line for the counter and write, erase and read lines for memory and counter. The control of these processes is commonly known so that it need not be discussed in any detail here.

As Fig. 1 shows, the integrated circuit in this embodiment example has 8 connections, a connection to ground (GND), a connection for the supply voltage (Vcc) and a connection for the programming voltage (Vpp) for nonvolatile memory 2. A bidirectional data line (I/O), a clock line ($\emptyset$) for the counter, a reset line (R) and two control lines (C1, C2) are also provided. The control lines can be used to select different operating modes, for example reading of the counter reading, operation of the counter or loading of the E²PROM with the counter reading. The reset line is required for each initialization process of the integrated circuit before the beginning of each transaction. Details of this will be described in connection with Fig. 4.

In the embodiment example shown the stated operating modes are controlled from the terminal, for example a telephone. During operation one must make sure the signals on the lines are not manipulated with intent to defraud.

The technical measures necessary for protecting the lines are known and already provided in the means in question here.

These protection measures can be omitted if the signals for the reset lines and control lines are not supplied externally but generated in-circuit by control and safety logic 4. In particular it is possible to use in-circuit control for initializing the circuit before each use and updating the memory with the particular counter reading reached. However in this case control and safety logic 4 will be accordingly more extensive.

Before details of the control and safety logic are dealt with, the processes taking place during a transaction will be explained with reference to Figs. 2 and 3.

For simplicity's sake let us assume memory 2 having four memory cells and accordingly large counter 3. The erased state of the memory still corresponds to the invalidated state. When the memory reaches this state the card is useless. This memory state is symbolically characterized in Fig. 2 in that each memory cell has a zero. The bank card as it is handed over to the user in the loaded state accordingly has a one in each memory cell.

Figs. 3a - 3d show the four phases during the course of a transaction with reference to an example.

In phase 1 (Fig. 3a) the content of memory 2 is transferred to counter 3. Only when this process is over can the counter be operated. In the logic selected in this embodiment example the counter is designed such that the counter reading can only be decremented by corresponding clock

pulses. The counter reading transferred from memory to the counter can therefore always only be reduced.

During phase 2 (Fig. 3b) the counter reading is continuously decremented by the clock pulses produced for example by a telephone. The Fig. shows in this phase the state of the counter after 5 clock pulses. Let us assume an external or an in-circuit control is designed such that after every 5 clock pulses the memory is updated with the particular counter reading reached. Using a memory produced by E²PROM technology this necessitates that the memory first be erased. Fig. 3c shows the erased state of the memory reached in phase 3. Finally, in phase 4 (Fig. 3d) the current counter reading is transferred to memory by a write operation.

As already indicated by the sequence described with reference to the Fig., safety precautions must be taken to prevent the particular counter reading present in memory 2 from being changed by fraudulent measures in favor of the user. For this purpose the circuit is provided with a control and safety logic to be described in more detail in the following.

A first essential function for protecting the circuit from manipulation is that the circuit is only operative for a transaction when the particular counter reading last stored in nonvolatile memory 2 has been transferred to counter 3 as a new initial value.

Fig. 4 shows an exemplary embodiment of a circuit that is part of control and safety logic 4 and performs the abovementioned function.

The circuit shown in Fig 4. comprises substantially monoflop 14 with a Schmitt-trigger input, flip-flop 15 and gates 11, 12, 13 for blocking input lines $\emptyset$, C1 and C2.

Upon application of supply voltage Vcc monoflop 14 with a Schmitt-trigger input produces a predefined pulse. The Schmitt-trigger input is connected for this purpose with the supply voltage via delay circuit 17 (RC unit). The pulse produced by the monoflop leads to set input S of flip-flop 15 so that the latter is switched to a predefined state regardless of what signal is carried by reset line R leading to clock input T of the flip-flop. The inverting output of the flip-flop, which has the state log. 0 in the selected logic, is connected with AND gates 11, 12, 13 so that they block input lines $\emptyset$, C1 and C2 in this phase.

The pulse produced automatically by monoflop 14 upon application of the supply voltage can also be used to switch further circuit elements into predefined initial states if desired.

To permit operation of the circuit a reset pulse is necessary. This pulse is utilized on the one hand as a load pulse for counter 3 and on the other hand, at the same time or with a time lag, as a reset pulse for flip-flop 15. With the load pulse the content of memory 2 is transferred to counter 3. For this purpose the counter is equipped with so-called set inputs to which the information of memory 2 is

applied. With the reset pulse, which leads to the clock input of flip-flop 15, the inverting output of flip-flop 15 is set to log. 1, thereby enabling the clock input and the control lines.

The explained circuit thus ensures that the circuit can be operated only when the particular last memory content (residual value) has been transferred to the counter as a start value for the following transaction.

As mentioned, a second function of the circuit relevant for security is that the counter counts only in a predefined direction. A binary counter constructed for example from several flip-flops provides, with customary wiring, a binary number that increases by one at each clock pulse at its non-inverting outputs and a binary number that accordingly decreases by one at each clock pulse at the inverting outputs.

Using a hard-wired decoding of the desired counter outputs one can realize the required function in a simple way.

Finally, a third function of the control and logic circuit relevant for security is that the so-called overflow of the counter is detected and the circuit blocked in case of overflow or before overflow.

In the example explained with reference to Figs. 3a - 3d counter 3 reaches the maximum counter reading (overflow $\approx$ decimal 15) when a further clock pulse is fed to the counter at the counter reading zero. If this counter reading were transferred to the memory the card would be loaded again with the initial value. The possibility of manipulation resulting from the overflow of the counter is thus excluded.

As Fig. 5 shows, one can use for this purpose a simple decoding logic that always produces a signal when all flip-flops of the counter have reached the zero condition. All outputs 9 of flip-flops 8 of counter 3 are led to OR gate 10 that only produces a log. 0 level at its output when all inputs have a log. 0 level. In this state AND gates 11, 12 and 13, which can be identical with gates 11, 12, 13 described in connection with Fig. 4, are blocked so that no further clock pulses pass to counter 3. Only the counter reading zero can thus be transferred to memory. This corresponds to the invalidated state as assumed at the outset.

The explanations of the measures necessary for security show that the inventive solution involves no disadvantages in security over known data carriers, on the one hand, and that relatively little logic circuit effort is necessary for technically realizing the necessary measures.

The dramatic reduction of required memory and thus of the surface of the integrated circuit attained with the inventive solution is thus hardly diminished by the additional effort for safety logic.

As already mentioned, a so-called debit card is set to an initial value before being issued to the user. It is thereby possible to assign a certain initial value to a card by writing the binary combination corresponding to this

value to memory. However it is also possible to load all memory cells universally by a write operation for example immediately after production of the circuit so that the card first has the maximum possible initial value. In this case the particular institution issuing the cards will reduce the memory to the desired initial value with the aid of the method described with reference to Figs. 3a - 3d.

It must of course be ensured that solely authorized institutions are in a position to load the memory to the initial value. Depending on the design of the card this process can be performed either once or repeatedly.

Claims



1. A system for cashless transactions having a data carrier with an embedded IC (1) and a terminal for communicating with the data carrier or IC, a read-only memory (2) provided in the IC containing an initial credit which is gradually reduced in accordance with the transaction selected by means of the terminal, characterized in that

a dual counter (3) is provided which is adapted to be driven in only one direction and has available at its output a dual number corresponding to a credit,

the read-only memory (2) is an electrically erasable and writable memory such as an E²PROM,

the number of storage locations in the read-only memory corresponds to the counter stages,

the counter reading is reduced according to a transaction value inputted via the terminal, and

a hard-wired control and safety logic (4) is provided for controlling the data transfer between the memory (2) and the counter (3) such that before each use of the data carrier the current memory value is transferred to the counter and after use of the data carrier the memory is updated with the current counter reading.

2. The data carrier assembly of claim 1, characterized in that the control and safety logic (4) has a circuit comprising a decoding logic (10) and at least one blocking gate (11) for blocking operation of the counter before it overflows.

3. The data carrier assembly of claim 1, characterized in that the control and safety logic (4) has a circuit (14, 15) for generating a definite pulse to block at least the control lines (Ø, C1, C2) leading to the circuit after the supply voltage is applied.

4. The data carrier assembly of claim 3, characterized in that the circuit (14, 15) is designed such that the block can be lifted by a reset pulse, this pulse also serving as a load pulse for the counter (3).