The present invention concerns a device for protecting an electronic card and its use to protect the electronics of a terminal for reading a magnetic and/or microprocessor card.

In an electronic card comprising, on a printed circuit, a microprocessor and memories intended to contain confidential information, that is not to be accessible to a person intending to commit fraud, it is necessary to protect access to these memories by physical means. However, this protection of access by physical means can be circumvented by means destroying the protection without damaging the memories and the content thereof. It is therefore necessary to prevent, as far as possible, the use of these destructive means. Similarly if, before a memory is disconnected from its power supply, the ambient temperature has been lowered sufficiently, this memory will retain the content of this information even after the power supply has been cut off.

A first aim of the invention is therefore to propose a device for physically protecting an electronic card with a volatile memory.

This aim is achieved by the fact that the device comprises a resistive network embedded in the resin and surrounding the electronic card, the resistive network being incorporated in an electronic circuit for detecting modifications of the resistance of the network in order to cause the destruction of the information in the volatile memories.

According to another characteristic, the circuit for detecting modifications in the resistance of the network is constituted by a resistor bridge connected to the terminals of a comparator.

The other aim of the invention is to propose a protection device making it possible to detect attempts to destroy the physical protection or to preserve the information contained in the memory by lowering the temperature.

This aim is achieved by the fact that the device further comprises means for detecting the temperature of the electronic circuit and means for causing the destruction of the information in the volatile memory when a low-temperature threshold or a high-temperature threshold is crossed.

According to another characteristic, the temperature detection means are constituted by a thermistor mounted in a resistor bridge, connected to the terminals of a window comparator.

A third aim is to propose a device making it possible to detect the opening of the casing in order to guard against physical attack.

This third aim is achieved by the fact that this device comprises means for detecting the opening of the casing in order to cause the destruction of the information in the volatile memory.

According to another characteristic, the means for detecting opening are a flexible blade switch fastened to one half of the casing and controlled by a magnet mounted adjacently on the second half of the casing.

According to another characteristic, the output of the means for detecting temperature, modifications to the resistance of the network, and the opening of the casing, are sent via an AND gate to a multivibrator, the output of which controls an electronic switch cutting off the power supply to the volatile memories.

Another aim of the invention is to use the above device to protect the electronics of a terminal for magnetic cards and/or a microprocessor.

This aim is achieved by the fact that the terminal is associated with a device as described above and further comprises a visual display device, a magnetic track reader and/or a microprocessor circuit reader, a keyboard and at least one communication line, either to another piece of equipment, or to a network.

FR-A-2 596 176 describes a device corresponding to the precharacterising portion of Claim 1 and comprising means for detecting the opening of the casing causing a stop in power supply to the random access memory. It is moreover known from FR-A-2 580 834 that the use of a memory card can be protected by a resistive network surrounding the circuit and by detecting modifications to the resistance of the network.

The present invention is defined by the attached claims.

Other characteristics and advantages of the present invention will become more apparent on reading the following description given with reference to the attached drawings in which:

- Figure 1 represents a diagrammatic view in section of the device for physically protecting an electronic card;

- Figure 2 represents a diagram of the functional elements of the terminal;

- Figure 3 represents the electronic diagram of the device for protecting an electronic circuit with a volatile memory.

A card (1) comprising a set of electronic circuits (10, 11) is surrounded by a resistive network (2) constituted by a polycarbonate film (20) on each of the faces of which a carbon film (21, 22) is screen-printed. As can be seen in Figure 1, the carbon tracks (22) on one face of the polycarbonate film (20) are staggered relative to the tracks (21) of the other face of the substrate film (20).

All these networks of carbon film (22) and (21) arranged on each of the faces constitute respectively one resistor (R1) and a second resistor (R2) which are connected to the electronic circuit of the card (1) by a linkage (220) and respectively a linkage (210). The assembly formed by the electronic card (1) and the resistor network (2) is embedded in polyurethane resin. This resin remains in the solid state up to a temperature of around 100°C. The distance D between the faces of the

resistor network and the printed circuit constituting the electronic card is small enough to prevent a probe of a measuring instrument from being slid between the resistor network (2) and the electronic circuit card (1) via the faces where the card is not surrounded, since the resistor network (2) has a U-shaped cross-section.

In an improved embodiment it would be conceivable to surround the card with four resistor networks arranged so that there is no open gap allowing access to the electronic card (1).

The resin block (3) is then enclosed in a casing (4) constituted by two half shells (40, 41), the first of which comprises, near the parting plane, a magnet (50), and the second of which (41) comprises, adjacent to the separation surface, a flexible-blade switch (51) which is connected by the wires (52) to the electronic circuit of the card (1).

Figure 2 shows an interesting application of the principle of the invention according to Figure 1, especially for protecting a credit card reader terminal. This credit card reader terminal shown in Figure 2 comprises a magnetic track reader (6) connected by an interface circuit (15) to a bus (110) to which a microprocessor (11) is connected. A second reader (5) is designed for reading credit cards, comprising, in addition to the magnetic track, an integrated circuit with an autoprogrammable microprocessor. This reader (5) is connected by a second interface (14) to the bus (110). A display device (7) constituted, for example, by light-emitting diodes is also connected to the bus (110). A volatile random access memory (12) is also connected to the bus (110). This random access memory (12) (RAM) is transformed into a non-volatile memory by a battery (18) or lithium cell which makes it possible to ensure a power supply to the volatile memory even in the event of the main or ancillary power supply being cut off. This power supply (18) to the random access memory is transmitted by an electronic circuit (10) for detecting attempts at fraud; this electronic circuit (10) is connected by the wires (220, 210 and 52) to the resistors in Figure 1 and to the flexible-blade switch (51). Similarly, a keyboard (8) is connected, via an interface circuit (16), to the bus (110). Finally, a programmable read-only memory of the EPROM type, is connected to the bus (110). The terminal

also comprises an interface circuit (17) making it possible to produce a connection of the RS 232 type or a local network.

The electronic circuit (10) for protecting the card (1) against fraud is shown in Figure 3. These electronics comprise a thermistor (101) mounted in a bridge constituted by the resistors (1022, 1021, 1024 and 1029). The bridge is connected to the input of a window comparator (102) which receives at its clock input (OSC) the signal supplied by a pulse generator constituted by the common point of a resistor (1208) and a capacitor (1022) connected in series between earth and a supply voltage. The output of the comparator (102) is sent to a first input of an AND gate (103). The second input of this AND gate (103) receives the output of a second window comparator (104) which, at its pulsed input, receives the signal furnished by the common point of a resistor (1048) and a capacitor (1047) connected in series between the supply voltage and earth. This comparator (104) is connected to a resistor bridge constituted, on the one hand, by the resistors (21, 22) of the network surrounding the circuit and, on the other hand, by the resistors (1046, 1044 and 1049). The output of the AND gate (103) is sent to a first input of a second AND gate (105), a second input of which receives the output of an inverter (1050). The input of this inverter (1050) is connected to the common point between a resistor (1051) and the flexible-blade switch (51) connected in series between the supply voltage and earth. The output of the AND gate (105) is sent through a filter (106B) to a multivibrator (107), the clock input (CLK) of which receives the output of an oscillator (110). The output /Q of the multivibrator (107) is sent to a second filter (106A), the output of which is connected to an inverter (1080). The output of this inverter controls an electronic switch circuit (108) making it possible to cut off the output (120) supplying the volatile memories (12) of the card (1). The power supply to these memories is provided by a power switching circuit (109) making it possible to switch the power supply of the terminal automatically to a power supply provided by the lithium cell (18) connected to the input (VS) of the circuit (109).

In operation, the thermistor (101) in association with the comparator (102) makes it possible to detect the crossing of the two temperature thresholds of - 30°C and + 100°C. The - 30°C threshold makes it possible to prevent it being possible, by

lowering the temperature of the electronic circuit, to disconnect the battery without losing the information contained in the random access memories (12). This would allow a person intending to commit fraud to gain access to the information contained in these random access memories (12) and constituted by the keys of customers who have used their cards. Similarly, the + 100°C threshold makes it possible to detect an attempt to melt the resin (3) with a view to gaining access to the information contained in the random access memory. In both cases where one of these temperature thresholds is crossed, the circuit cuts off the power supply to the random access memory (RAM) and thereby causes the destruction of the information contained in it.

Similarly, an attempt to pierce the resistor network (21, 22) is revealed by the corresponding variation in the resistors (21, 22) detected by the comparator (104), the output of which controls the cutting off of the power supply to the memory (12). This makes it possible to prevent the piercing of a channel in order to insert a measurement probe and, subsequently, sample the information contained in the memory. Finally, the opening the casing of the terminal being detected by the flexible-blade switch (51), the contact of which closes as soon as the magnet (50) is moved away from this switch. This situation is detected by the inverter (1050) and transmitted by the AND gate (105) to the multivibrator (107), the output of which controls the cutting off of the power supply to the random access memory (12). The multivibrator (107) makes it possible to store one of the three detection states as soon as one of these three conditions, or two or all three of these conditions, occur at the same time.

In this way, a device has been produced for protecting an electronic circuit and this protection device has been used for protecting the information contained in a terminal adapted to function with bank cards, either of the magnetic-track or the combined type, that is, with magnetic tracks and a microprocessor, or else just with a microprocessor.

CLAIMS

1. Device for protecting a card comprising, on a printed circuit, an electronic volatile memory circuit (12) containing programs or information to be protected and embedded in resin (3), this device comprising detection means for detecting an attempt to access said volatile memory circuit and causing a destruction of said information, characterised in that said detection means comprise a resistive network (21, 22) having a given resistance and surrounding the volatile memory circuit, and an electronic circuit for detecting possible alterations of said resistance in order to cause the destruction of said information in the case when said alterations are apparent, said detection circuit including a window comparator (104).

2. Device according to Claim 1, characterised in that said resistance detection circuit comprises a resistor bridge (21, 22, 1046, 1044, 1049) including said resistive network (21, 22) and connected to input terminals of said comparator.

3. Device according to Claim 1, characterised in that it comprises means (101) for detecting the temperature associated with the resistance detection circuit (10) and means (107, 108) for causing the destruction of the information of the volatile memory (12) when a low temperature threshold or a high temperature threshold is crossed.

4. Device according to Claim 3, characterised in that the temperature detection means (101) are constituted by a thermistor (101) mounted in a resistor bridge (1022, 1021, 1024) connected to the terminals of a window comparator (102).

5. Device according to any one of the preceding claims, characterised in that it comprises means (50, 51) for detecting opening of the casing in order to cause the destruction of the information of the volatile memory (12) in case of opening.

6. Device according to Claim 5, characterised in that the means (50, 51) for detecting opening comprise a switch with a flexible blade (51) fixed on a first half (41) of the casing and controlled by a magnet (50) mounted adjacently on a second half (40) of the casing.

7. Device according to any one of Claims 3 to 6, characterised in that the output signals of the temperature detection means, of the resistance detection means (104) and of the means for detecting opening of the casing (1050) are sent via an AND gate (103, 105) to a multivibrator (107), the output of which controls an electronic switch (108), said switch being capable of interrupting the supply of the volatile memory.

8. Use of a device according to one of the preceding claims for protecting the electronics of a terminal for magnetic and/or microprocessor cards, comprising a central unit (11) associated with random access memories (12).

9. Use according to Claim 8, characterised in that the terminal comprises a display device (7), a magnetic track reader (6) and/or a microprocessor card reader (7), and a keyboard.

10. Use according to Claim 9, characterised in that the terminal comprises a communication circuit (17).