

## METHOD OF BLOCKING INTERNAL COMMUNICATIONS INSIDE AN ELECTRONIC DEVICE

### Background of the invention

5       The present invention relates to electronic devices,  
such as smart cards, for example, that are suitable for  
co-operating with an external reader. The invention  
relates more particularly to controlling communications  
taking place internally in such devices while they are in  
10   operation.

Nowadays smart cards are used in numerous fields of  
application. They are used in particular for  
implementing banking, telephony, identification, and/or  
authentication ... operations. These operations may be  
15   implemented either by contact, with the card typically  
being inserted in a reader (contact mode), or else  
remotely (contactless mode) by electromagnetic coupling,  
generally of the induction type, between a transceiver  
terminal and a smart card placed within the zone of  
20   action of the terminal.

Smart cards are generally capable of operating in a  
contact mode (e.g. in compliance with ISO 7816-2) by  
using external contacts of an electronic module (or  
transponder) integrated in the card. These external  
25   contacts are arranged at the surface of the smart card so  
as to be accessible by an external reader designed to co-  
operate by making contact with these external contacts.

In known manner, certain smart cards are suitable  
for operating in contactless mode with an external reader  
30   designed for that purpose. To do this, a smart card is  
provided with a radiofrequency (RF) antenna. In  
contactless mode, information is exchanged between the  
smart card and the contactless type external reader via  
the RF antenna (e.g. in accordance with ISO 14443).

35

A dual interface card is a smart card suitable for operating both in contact mode and in contactless mode. New smart cards have recently appeared that can be said to be more intelligent, which cards may incorporate various components (biometric sensors, screens, ...) suitable for improving user experience, in particular in terms of making the smart card secure or of supplying service to the user.

For this purpose, in addition to a conventional electronic module (generally known as a "secure element") having a first microprocessor, it is known to include in a smart card a second microprocessor that is external to the secure element and suitable for communicating with the first microprocessor. Typically, such a secure element is suitable for co-operating in conventional manner with an external reader in contact mode or in contactless mode, e.g. in order to carry out a transaction. Furthermore, the second microprocessor is suitable for communicating with the secure element and generally serves to implement at least one function in co-operation with said secure element. By way of example, this function relates to selecting an application to be implemented by the secure element (as described below with reference to Figure 1) or to displaying given information (as described below with reference to Figure 2).

More specifically, Figure 1 shows a known example of a dual interface type smart card 2 comprising a secure element 4 and an electronic module 6, which element and module are suitable for communicating with each other via a link L1 that is internal to the card.

The secure element 4 comprises in particular a first microprocessor 8 suitable for co-operating with an external reader (not shown) by using external contacts 10 or an RF antenna 12 with which the secure element 4 is provided.

In this example, the module 6 comprises a second microprocessor 14 powered by a battery 16 and capable of receiving instructions from a user via a button 18. By actuating the button, the user can cause a particular application to be selected. When the user selects a given application by means of the button 18, the second microprocessor 14 sends a command to the microprocessor 8 of the secure element 4. In response to this command, the microprocessor 8 is configured to select and implement the application selected by the user.

The microprocessor 14 may also be configured to use indicator lights 20-1 to 20-4 (referred to collectively as 20) to display which application has been selected in response to the user commands.

Figure 2 shows an example of a dual interface type smart card 24 similar to the smart cards 2. The smart card 24 comprises a secure element 4 as described above and an electronic module 26 suitable for communicating with the secure element 4 via a link L2 that is internal to the card.

The electronic module 26 comprises a microprocessor 28 powered by a battery 30 and capable of receiving instructions by means of a button 32. By actuating the button, the user is capable for example of initiating or controlling a transaction with an external reader (not shown).

In this example, the microprocessor 28 is also suitable for displaying given information on a display 34, such as the amount of a transaction or a currency selected by the user.

The structures shown as examples in Figures 1 and 2 advantageously enable the smart card to implement functions that are useful for the user, and to do so with the help of an electronic module (or more generally a processor unit) that is suitable for co-operating with the secure element via a link that is internal to the card.

Nevertheless, it has been found that smart cards presenting this type of architecture encounter problems of operation. Conventionally, the secure element in such smart cards is not optimized to provide good management  
5 of commands coming both from an external reader (in contact and/or contactless mode) and commands coming from an electronic module (or processor unit) internal to the card. The secure element can encounter difficulties in taking account of multiple commands coming from these  
10 different sources, and under certain circumstances, that can lead to conflicts that are harmful for proper operation of the secure element.

It has been observed that such conflicts occur in particular when commands coming from an external reader  
15 and from such an electronic module of the smart card are received simultaneously or quasi-simultaneously by the secure element.

At present there does not exist a solution that serves in particular in a smart card (and more generally  
20 in an electronic device suitable for co-operating with an external reader) to resolve the above-mentioned conflict problems when the secure element is communicating both with the external reader and also with a processor unit internal to the smart card but external to the secure  
25 element.

#### Object and summary of the invention

In order to solve the above-mentioned problems in particular, the present invention provides an electronic  
30 device comprising:

- a secure element comprising a plurality of contacts, said secure element being suitable for co-operating with a first external reader that is external to said electronic device in a contact mode by using at  
35 least one of said contacts;

- a processor unit external to the secure element, said processor unit being suitable for sending a command to the secure element via at least one of said contacts;

- a first detector unit for detecting whether a  
5 communication by contact is ongoing in contact mode between the secure element and the first electronic reader; and

- a control unit configured to block the sending of each command from the processor unit to the secure  
10 element via at least one predefined contact from among said plurality of contacts, so long as a said communication by contact is ongoing.

The invention is advantageous in that it makes it possible to avoid any conflict in the secure element  
15 between an "external" command received from a reader external to the electronic device in contact mode, and an "internal" command received from a processor unit internal to the smart card. As mentioned above, such conflicts can lead to operating problems in the secure  
20 element insofar as it is not designed to process simultaneously both an external command and an internal command, as defined above.

The invention serves in particular to avoid a conflict situation arising in which an internal command  
25 and an external command are received simultaneously by the secure element of the smart card.

The invention is also advantageous in that it can be implemented without affecting the structure or the operation of the secure element of the smart card.

30 In a particular embodiment, the contacts are in compliance with the ISO 7816 standard.

In a particular embodiment, at least one predefined contact comprises (or is) the contacts defined in the ISO 7816 standard as Vcc, RST, CLK, GND, and IO.

35 In a particular embodiment, the control unit is configured to block the sending of each command from the processor unit to the secure element via each of the

contacts of the secure element so long as a said communication by contact is ongoing.

5 In a particular embodiment, the first detector unit is connected to one of said contacts, referred to as the "power" contact (Vcc), that is to receive electrical power when the secure element is co-operating in contact mode with the first external reader in order to power said secure element electrically.

10 In a particular embodiment, the first detector unit is suitable for converting a first voltage detected on the power contact (Vcc) into a second voltage that is different from the first voltage. Such conversion makes it possible to avoid the first detector unit disturbing the operation of the secure element ES.

15 In a particular embodiment, the processor unit is configured to determine that a said communication by contact is ongoing between the secure element and the first external reader only if the second voltage is not less than a first predetermined threshold value.

20 In a particular embodiment, the secure element includes a first radiofrequency antenna, said secure element being suitable for co-operating with a second external reader that is external to said electronic device in a contactless mode by using said first radiofrequency antenna, said electronic device including:

25 - a second detector unit suitable for detecting whether a contactless communication is ongoing in contactless mode between the secure element and the second external reader;

30 the control unit being configured to block the sending of each command from the processor unit to the secure element via said at least one predefined contact so long as at least one of a said communication by contact and said contactless communication is ongoing.

35 In a particular embodiment, the electronic device comprises a second radiofrequency antenna isolated from the first radiofrequency antenna,

the second detector unit being suitable for using the second radiofrequency antenna to detect a radiofrequency signal transmitted or received by the first radiofrequency antenna, indicating that said contactless communication is ongoing between the secure element and the second electronic reader.

The use of the second RF antenna is advantageous in that it makes it possible in particular to avoid contactless communication between the secure element and an external reader being disturbed by the second detector unit.

In a particular embodiment, the second detector unit is suitable for converting an alternating current (AC) voltage obtained from the first radiofrequency antenna into a direct current (DC) voltage.

In a particular embodiment, the processor unit is configured to determine that a said contactless communication is ongoing only if the DC voltage is not less than a second predetermined threshold value.

In a particular embodiment, the control unit comprises a switch at the interface between the secure element and the processor unit, said switch being suitable for switching between a blocking state and a conductive state,

the switch being configured to occupy the blocking state when the control unit blocks said sending of each command from the processor unit via said at least one predefined contact, so as to isolate the secure element electrically relative to the processor unit.

Such electrical isolation is advantageous in that it serves in particular to avoid communication by contact between the secure element and an external reader being disturbed by the processor unit.

In a particular embodiment, the processor unit is suitable for co-operating with the secure element to select an application to be executed by the secure element,

the processor unit being suitable for performing this selection on the basis of an instruction from a user received via an actuator of the electronic device.

5 In a particular embodiment, the processor unit is suitable for obtaining information from data received from the secure element and for causing said information to be displayed by using a display unit of the electronic device.

10 In a particular embodiment, the electronic device is a smart card.

The present invention also provides a blocking method implemented by an electronic device comprising:

- a secure element comprising a plurality of contacts, said secure element being suitable for co-  
15 operating with a first external reader that is external to said electronic device in a contact mode by using at least one of said contacts; and
- a processor unit external to the secure element, said processor unit being suitable for sending a command  
20 to the secure element via at least one of said contacts; the method comprising:
  - first verification to determine whether a communication by contact is ongoing in contact mode between the secure element and the first external reader;  
25 and
  - blocking the sending of each command from the processor unit to the secure element via at least one predefined contact from among said plurality of contacts, so long as a said communication by contact is ongoing.

30 It should be observed that the various embodiments mentioned above with reference to the electronic device of the invention apply in analogous manner to the blocking method of the invention.

Specifically, in a particular embodiment, the secure  
35 element includes a radiofrequency antenna, the secure element being suitable for co-operating with a second external reader that is external to the electronic device

in a contactless mode by using the first radiofrequency antenna, said electronic device comprising:

- second verification to determine whether a contactless communication is ongoing in contactless mode between the secure element and the second external reader; and

- blocking the sending of each command from the processor unit to the secure element via at least one predefined contact, so long as at least one of a said communication by contact and a said communication without contact is ongoing.

In a particular embodiment, the steps of the blocking method are determined by computer program instructions.

Consequently, the invention also provides a computer program on a data medium (or recording medium), the program being suitable for being implemented in an electronic device such as a smart card, or more generally in a computer, the program including instructions adapted to implementing steps of a blocking method as described above.

The program may use any programming language and be in the form of source code, object code, or code intermediate between source code and object code, such as in a partially complied form, or in any other desirable form.

The invention also provides a data medium (or recording medium) that is readable by an electronic device such as a smart card, and more generally by a computer, and including instructions of a computer program as mentioned above.

The data medium may be any entity or device capable of storing the program. For example, the medium may comprise storage means such as a read only memory (ROM), e.g. a compact disk (CD) ROM, or a microelectronic circuit ROM, or it may comprise magnetic recording means, e.g. a floppy disk or a hard disk.

Furthermore, the data medium may be a transmissible medium such as an electrical or optical signal, suitable for being conveyed via an electrical or optical cable, by radio, or by other means. The program of the invention  
5 may in particular be downloaded from an Internet type network.

Alternatively, the data medium may be an integrated circuit in which the program is incorporated, the circuit being adapted to execute or to be used in the execution  
10 of the method in question.

#### Brief description of the drawings

Other characteristics and advantages of the present invention appear from the following description made with  
15 reference to the accompanying drawings, which show embodiments having no limiting character. In the figures:

- Figure 1, described above, is a diagram showing a conventional smart card enabling a user to select a given  
20 application;

- Figure 2, described above, is a diagram showing a conventional smart card suitable for displaying information that is useful for a user;

- Figure 3 is a diagram showing a smart card in  
25 accordance with a first embodiment;

- Figure 4 is a flow chart showing the main steps of an example blocking method implemented in a smart card in accordance with the first embodiment shown in Figure 3;

- Figure 5 shows an implementation of a smart card  
30 of the first embodiment as shown in Figure 3; and

- Figure 6 is a diagram showing a smart card in accordance with a second embodiment.

#### Detailed description of embodiments

35 The present invention relates to electronic devices that are suitable for co-operating with an external reader, such as smart cards, for example. The invention

relates more particularly to controlling communications that are internal to such devices while they are in operation.

5 In this document, implementations of the invention are described in non-limiting manner with reference to a dual interface type smart card. Nevertheless, it should be understood that the invention applies more widely to any electronic device suitable for co-operating with an external reader at least in contact mode, and possibly  
10 also in contactless mode, e.g. in order to implement a given transaction.

The invention may be applied in particular to smart cards in compliance with the ISO 7816 standard.

15 Unless specified to the contrary, elements that are common or analogous to more than one of the figures are given the same reference numerals and present characteristics that are identical or analogous, such that these common elements are generally not described again for reasons of simplicity.

20 Figure 3 is a diagram showing the architecture of a smart card 40 in accordance with a first embodiment of the invention, in this example, the smart card 40 complies with the ISO 7816 standard.

25 More particularly, the smart card 40 comprises an electronic module ES constituting a secure element suitable for co-operating in conventional manner either in contact mode or else in contactless mode with a reader that is external to the smart card 40.

30 The smart card 40 also has a processor unit 44 suitable for sending commands (or data) to the secure element ES via an internal link L11.

In this example, the secure element ES comprises a microprocessor 46, a rewritable volatile memory (or random access memory (RAM)) 48, a rewritable non-volatile  
35 memory 50 (e.g. of the flash type), an RF antenna 52, and external contacts 54.

The rewritable non-volatile memory 50 contains a computer program PG1 including instructions capable of being implemented by the microprocessor 46, in particular in order to co-operate in contact mode or in contactless mode with an appropriate external reader. Alternatively, the memory 50 that stores the computer program PG1 may be a ROM.

In this example, the secure element ES is suitable for co-operating in contact mode with a first external reader RD1 by using at least one of the external contacts 54 provided for this purpose. To do this, the external reader RD1 makes an electrical connection with the external contact 54 so as to be capable of exchanging signals with the secure element ES, and more particularly with the microprocessor 46. Co-operation by contact between a smart card and an appropriate external reader is itself known and is therefore not described in greater detail in the present description for reasons of simplicity.

In this example, the secure element ES is also suitable for co-operating in contactless mode with a second external reader RD2 by using the RF antenna 52. Typically, the secure element ES communicates with the external reader RD2 in contactless mode by electromagnetically coupling (e.g. by induction) the RF antenna 52 with an RF antenna of the external reader RD2. Contactless co-operation between a smart card and an appropriate external reader is itself known and is therefore not described in greater detail in the present description for reasons of simplicity. As mentioned above, it is nevertheless possible to implement the invention without the secure element ES having the ability to operate in contactless mode, in which case the RF antenna 52 need not be present.

Furthermore, the processor unit 44 comprises a microprocessor 60, a communication interface 62, a rewritable volatile memory (RAM) 64, a rewritable non-

volatile memory 66 (e.g. of the flash type), an actuator 68, a battery 70, and at least one indicator light 72, e.g. of the light-emitting diode (LED) type.

5 The rewritable non-volatile memory 66 constitutes a data medium in accordance with a particular implementation of the invention that is readable by the microprocessor 60 and that stores a computer program PG2 in accordance with a particular implementation of the invention. Alternatively, the memory 66 that stores the  
10 computer program PG2 may be a ROM.

In this example, the program PG2 includes instructions for executing a blocking method in a particular embodiment of the invention. The steps of this method in a particular embodiment of the invention  
15 are described below with reference to Figure 4.

The communication interface 62 enables the microprocessor 60 to communicate via an internal link L11 and at least one predefined external contact 54 with the secure element ES, and more particularly with the  
20 microprocessor 46. In the presently-described example, the interface 62 is connected via the link L11 to the external contacts 54.

In a particular embodiment, the interface 62 is included in the microprocessor 60.

25 The link L11 comprises a bus connecting at least one predefined external contact 54 to the interface 62 of the processor unit (as described in greater detail with reference to Figure 5).

In this example, the external contacts 54 comply  
30 with the ISO 7816 standard. The link L11 comprises a bus connecting the processor unit 60 to each of the contacts 54 defined as Vcc (power), RST (reset), CLK (clock), GRD (ground), and IO (input/output) in the ISO 7816 standard.

The processor unit 60 is thus suitable for sending  
35 one or more commands to the secure element ES via at least one of the external contacts 54, i.e. at least one of the contacts Vcc, RST, CLK, GRD, and IO, in this

example. In this context, the processor unit 60 behaves relative to the secure element ES like an external reader (even though the element ES is internal to the smart card 40) insofar as the processor unit 44 co-operates with the external contacts 54 in order to communicate with the secure element ES.

Nevertheless, it should be understood that the particular configuration described herein merely constitutes a non-limiting example of the invention and other examples can be envisaged in the ambit of the invention. Other examples of connection to the external contacts 54 can be envisaged.

The actuator 68 may be a button or any other actuator enabling a user to send an instruction to the processor unit 44.

The battery 70 powers the microprocessor 60 electrically.

It is assumed in this example that the processor unit 44 comprises a plurality of LEDs 72 that are controlled by the microprocessor 60.

As explained below, the characteristics of the processor unit in the meaning of the invention may vary depending on particular circumstances without going beyond the ambit of the invention.

In the presently-considered example, the user can use the actuator 68 to select one from a plurality of available modes of operation (or applications). In this example, it is assumed that four modes of operation (or applications) M1, M2, M3, and M4 can be selected by the user. Naturally, other examples can be envisaged.

In response to a selection command from the user, the microprocessor 60 is configured to use the LEDs 72 to select which mode has been selected (or which application) and to send a selection command (of the application protocol data unit (APDU) type in this example) to the secure element ES in order to cause it to

operate in the mode selected (or the application selected) by the user.

To do this, the ADPU command is transmitted by the interface 62 via the internal link L11 to the secure element ES. By way of example, this selection command includes an identifier of the mode M1-M4 selected by the user. In response to this command, the microprocessor ES is configured to select the appropriate mode of operation M1-M4.

The above-described selection of a mode of operation merely constitutes an example of a function that can be implemented by the processor unit 44 in co-operation with the secure element ES. The processor unit in the meaning of the invention is not limited to implementing this particular function.

In accordance with this particular embodiment, the smart card 40 also has a control unit UC1, a first detector unit UD1, and a second detector unit UD2.

The control unit UC1 is configured to block or not block the sending of any commands (or data) from the processor unit 44 to the secure element ES via at least one predefined external contact 54 from among the plurality of external contacts 54.

In this example, the control unit UC1 is configured, where necessary, to block the sending of each command from the processor unit 44 to the secure element ES via each of the external contacts 54 defined as Vcc, RST, CLK, GND, and IO. As explained in greater detail below, the control unit 60 is configured to implement such blocking so long as an external communication is ongoing between the secure element ES and a reader that is external to the smart card 40.

In the presently-considered example, the control unit UC1 is controlled by the processor unit 44, and more particularly by the microprocessor 60, even though other embodiments can be envisaged.

The control unit UC1 in this example is external to the processor unit 44. Nevertheless, it should be understood that other variant embodiments can be envisaged. Alternatively, the control unit UC1 may be included in the processor unit 44. By way of example, the control unit UC1 may be implemented by the communication interface 62 or by the microprocessor 60 executing instructions of the program PG2.

Still in the presently-considered example, the control unit UC1 is a switch suitable for switching between a blocking state and a conductive state so as to control communication via the link L11. Nevertheless, the use of such a switch is not essential for implementing the blocking function of the invention, in particular when the control unit UC1 is implemented by the microprocessor 60 itself. By way of example, it is possible to envisage such blocking of commands from the processor unit being implemented in software.

In the blocking state, the control unit UC1 isolates the processor unit 44 electrically from the secure element ES, thus preventing any communication between the processor unit 44 and the secure element ES via the external contacts 54. Putting the control unit UC1 in the blocking state serves to block the sending of any command from the processor unit 44 to the secure element ES via any one of the predefined external contacts 54, i.e. the external contacts Vcc, RST, CLK, GND, or IO in the presently-described example. As mentioned above, the blocking of the invention may be implemented more generally on any one of the external contacts of the secure element ES, and preferably on those via which the secure element ES could receive an internal command (coming from the processor unit 44 in this example) that might come into conflict with an external command coming from a reader that is external to the smart card 40.

In the conductive state, the control unit UC1 allows communication between the processor unit 44 and the

secure element ES and in particular allows commands to pass from the processor unit 44 to the secure element via said at least one predefined contact (i.e. the external contacts Vcc, RST, CLK, GND, and IO in this example).

5        Furthermore, the first detector unit UD1 is suitable for detecting whether a communication by contact is ongoing in contact mode between the secure element ES and an external reader RD1. To do this, in this example, the detector unit UD1 is electrically connected to at least  
10 one of the external contacts 54 of the secure element ES in such a manner as to be capable of determining that a communication is ongoing in contact mode between the smart card 40 and the external reader RD1.

      The communication protocol used by the smart card 40  
15 for co-operating in contact mode with the external reader RD1 may vary depending on circumstances. In a particular embodiment, the secure element ES communicates by contact using the universal serial bus (USB) or the single wire protocol (SWP) protocol with the external reader RD1.

20        In the presently-envisaged example, the first detector unit UD1 is electrically connected to one of the external contacts 54, specifically the power contact. This power contact Vcc is for receiving an electrical power supply from the external reader RD1 when the secure  
25 element ES is co-operating in contact mode with said external reader RD1 so as to power the secure element ES electrically. Connecting the first detector unit UD1 to the power contact advantageously makes it possible to detect all contact communication between the secure  
30 element ES and an external reader, e.g. including communication using SWP protocol or the USB protocol.

      As explained also with reference to Figure 5, in this example, the external contacts 54 comply with the ISO 7816 standard and the above-mentioned power contact  
35 is the contact defined as Vcc by the ISO 7816 standard.

      Typically, when a communication by contact is being implemented between the secure element ES and the

external reader RD1, power is supplied by the external reader RD1 via the power contact Vcc of the secure element ES. The power contact Vcc thus remains at a high level so long as the transaction is ongoing between the secure element ES and the external reader RD1. Detecting that electrical power is being received on the power contact Vcc makes it possible to deduce that a communication by contact is ongoing.

It should be observed that other alternatives are possible for enabling the detector unit UD1 to monitor the electrical state of at least one external contact other than the power contact Vcc in order to determine whether a communication by contact is ongoing between the secure element ES and an external reader.

Furthermore, the second detector unit UD2 is suitable for detecting whether a contactless communication is ongoing in contactless mode between the secure element ES and an external reader RD2.

In this first embodiment, the detector unit UD2 is electrically connected to the RF antenna 42 so as to be capable of detecting an RF signal being transmitted or received by the RF antenna 52, this RF signal indicating that a contactless communication is ongoing between the secure element ES and the external reader RD2.

It should be observed that in the presently-described example, the detector units UD1 and UD2 are external to the processor unit 44. Alternatively, it is possible to implement at least one of the detector units in the processor unit 44, or indeed in the microprocessor 60 itself.

The conduct of a blocking method implemented by the smart card 40 in a particular embodiment is described below with reference to Figure 4. More precisely, the microprocessor 60 of the processor unit 44 implements a blocking method by executing the program PG2 in interaction with the units UC1, UD1, and UD2.

It is assumed that an initialization step S2 of initializing the processor unit 44 triggers the start of execution of a blocking method in the smart card 40. By way of example, this triggering may be the result of  
5 powering the processor unit 44 and/or detecting that at least one predefined criterion is satisfied (receiving a command, a date, a time, ...).

During a step S4, the microprocessor 60 determines:

1) whether a first communication is ongoing in  
10 contact mode between the secure element ES and any external reader; and

2) whether a second communication is ongoing in contactless mode between the secure element ES and any external reader.

15 More specifically, in this example, the microprocessor 60 verifies 1) whether a first communication by contact is ongoing by using the first detector unit UD1, and verifies 2) whether a contactless second communication is ongoing by using the second  
20 detector unit UD2.

By way of example, these two verifications 1) and 2) are implemented in step S4 in continuous manner or at regular time intervals. These verifications 1) and 2) may also be implemented simultaneously or else one after  
25 the other, depending on circumstances.

So long as no external communication (with or without contact) is detected between the secure element ES and a reader RD1, RD2 external to the card 40, the control unit UC1 remains in the conductive state so that  
30 each command from the processor unit 44 can reach the secure element ES. In the presently-considered example, it is the microprocessor 60 that maintains the control unit UC1 in the conductive state.

In this particular implementation, it should be  
35 observed that when the processor unit 44 sends a command to the secure element ES, the processor unit 44 is configured to wait for a predefined period of time after

sending the command before verifying once more whether an external communication is ongoing between the secure element ES and an external reader. The above-mentioned predefined time is selected in such a manner that while a command is in the process being sent from the processor unit 44, no collision is detected between an internal command and an external command. This configuration makes it possible to avoid a command from the processor unit 44 sent via the external contact Vcc of the secure element ES being interpreted by the detector unit UD1 as being an ongoing communication by contact between the secure element ES and an external reader. By way of example, the above-mentioned predefined time is less than or equal to 100 milliseconds (ms) (e.g. equal to 100 ms).

15 In contrast, if the microprocessor 60 detects (S4) by using the units UD1 and UD2, that a communication by contact or a contactless communication is ongoing between the secure element ES and a reader external to the smart card 40, then the method moves on to step S6.

20 During step S6, the microprocessor 60 configures the control unit UC1 to take up the blocking state so as to block the sending of any command from the processor unit 44 to the secure element ES via at least one predefined external contact 54 (specifically the external contact Vcc, RST, CLK, GND, and IO in this example), and this continues so long as at least one communication with contact or at least one contactless communication is detected as being ongoing between the secure element ES and an external reader.

25

30 As mentioned above, the invention also applies to a smart card (or more generally to an electronic device) that is suitable for operating in contact mode but not in contactless mode. In a variant embodiment, the card 40 does not have the RF antenna 52. Under such

35 circumstances, the detector unit UD2 is not needed. In this variant, during the step S4, the microprocessor 60 performs only the above-defined verification 1) in order

to determine whether a communication with contact is ongoing between the secure element ES and any external reader. If this verification 1) is positive, the method moves on to step S6. During step S6, the microprocessor  
5 60 configures the control unit UC1 to take up the blocking state so as to block the sending of any command from the processor unit 44 to the secure element ES over at least one predefined external contact 54 (i.e. the external contacts Vcc, RST, CLK, GND, and IO in this  
10 example), with this continuing so long as a communication with contact is detected as ongoing between the secure element ES and an external reader.

The invention is advantageous in that it makes it possible to avoid any conflict (or collision) in the  
15 secure element between an "external" command received from a reader external to the smart card in contact mode (or possibly in contactless mode), and an "internal" command received from a processor unit internal to the smart card.

20 As mentioned above, the secure element of a conventional smart card is not optimized for properly managing both commands coming from an external reader (in contact and/or contactless mode) and also commands coming from a processor unit (or electronic module) internal to  
25 the card. In certain circumstances the secure element can encounter difficulties in taking account of commands coming from these different sources, and this can lead to conflicts that are harmful for the proper operation of the smart card.

30 The invention makes it possible in particular to avoid a conflict situation arising in which an internal command and an external command are received simultaneously by the secure element of the smart card.

The invention is also advantageous in that it can be  
35 implemented without affecting the structure or the operation of the secure element of the smart card.

Furthermore, in the above-considered element, the microprocessor 60, in step S6, configures the control unit UC1 into the blocking state so as to isolate the secure element ES electrically from the processor unit 44. Although other embodiments can be envisaged, such electrical isolation is advantageous in that it serves in particular to avoid a communication by contact between the secure element ES and an external reader being disturbed by the processor unit 44.

Furthermore, in the presently-described example, the microprocessor 60 uses the interface 62 to send an APDU command to the secure element ES via at least one external contact 54 (using the internal link L11). The nature and the content of this APDU command may vary depending on circumstances. In the presently-described example, the APDU command is a selection command informing the secure element ES of a mode of operation (or an application) M1, M2, M3, or M4 that it is to implement. Naturally, other types of command can be envisaged.

Figure 5 shows an implementation of the smart card 40 in accordance with the first embodiment. Certain elements of the smart card 40 are omitted from Figure 5, for reasons of simplicity.

The microprocessor 46 (not shown) of the secure element ES is connected to the RF antenna 52 so as to be capable of communicating in contactless mode with the external reader RD2.

Furthermore, in this example, the microprocessor 60 includes:

- an input IN1 connected to the actuator 68 so as to be capable of receiving a command CMD1 from a user via the actuator 68;

- an input IN2 connected to the output of the detector unit UD1, the input IN2 being suitable for receiving a signal SG2 from the detector unit UD1

indicating whether a communication by contact is ongoing between the secure element ES and an external reader;

- an input IN3 connected to the output of the detector unit UD2, the input IN3 being suitable for receiving a signal SG3 from the detection unit UD2 indicating whether a contactless communication is ongoing between the secure element ES and an external reader; and

- an output OU1 via which the microprocessor 60 can send a command CMD2 to the secure element ES;

- an output OU2 via which the microprocessor 60 can control the states of the LEDs 72-1 to 72-5.

In this example, the control unit UC1 is connected via a bus BS1 of wired connections to at least one predefined external contact 54, namely the predefined external contacts 54-1, 54-2, 54-3, 54-4, and 54-5 (referenced collectively as 54) of the secure element ES in this particular example.

As mentioned above, the predefined external contacts 54-1, 54-2, 54-3, 54-4, and 54-5 correspond in this example respectively to the contacts Vcc, RST, CLK, GND, and IO as defined in the ISO 7816 standard. For reasons of simplicity, the other contacts defined by the ISO 7816 standard are not shown in Figure 5.

Furthermore, the control unit UC1 is connected via a bus BS2 to the output OU1 of the microprocessor 60. The microprocessor 60 can thus transmit a command CMD2 (e.g. of the APDU type) via the buses BS1 and BS2 to any of the external contacts 54-1 to 54-5.

As described above, the control unit UC1 in this example behaves like a switch serving to take on a blocking state or a conductive state under the control of the processor 60.

Furthermore, the detector unit UD1 is electrically connected to the external contact 54-1 (Vcc) so as to be capable of receiving as input a signal (e.g. a voltage) indicating whether electrical power is being received from an external reader RD1 by contact with the secure

element ES. The detector unit UD1 is suitable for sending a signal SG2 to the input IN2 of the microprocessor 60 indicating whether a communication by contact is ongoing between the secure element ES and the external reader RD1.

In this example, the detector unit UD1 also acts as a voltage converter so as to convert a signal received from the external contact 54-1 (Vcc) from a first voltage (e.g. 5 volts (V)) into a second voltage (e.g. 3 V). The detector unit UD1 is preferably implemented so as to comply with the specifications of the microprocessor 60 and in particular so as to protect the microprocessor 60.

The processor 60 determines that a communication by contact is ongoing between the secure element ES and the external reader RD1 only if the voltage of the received signal SG2 is not less than a first predetermined threshold value.

Furthermore, the detector unit UD2 is electrically connected to the RF antenna 52 so as to be capable of receiving as input a signal indicating whether a contactless communication is ongoing between the secure element ES and an external reader RD2. The detector unit UD2 is suitable for sending a signal SG3 to the input IN3 of the microprocessor 60 to indicate whether a contactless communication is ongoing between the secure element ES and an external reader RD.

In this example, the detector unit UD2 converts the AC signal (e.g. a voltage signal) potentially picked up from the RF antenna 52 into a DC signal SG3 (e.g. a voltage signal) suitable for being processed by the microprocessor 60. The way in which such conversion is performed is known to the person skilled in the art and is therefore not described in detail herein (e.g. envelope detection, etc.).

Still in this example, the microprocessor 60 determines that a contactless communication is ongoing between the secure element ES and the external reader RD2

only if the voltage of the received signal SG3 is not less than a second predetermined threshold value.

As mentioned above, it should be observed that various variant embodiments can be envisaged in the ambit  
5 of the invention.

For example, it is possible to envisage blocking the sending of all commands from the processor unit 44 to the secure element ES but without electrically isolating the secure element ES from the processor unit during said  
10 blocking.

In a variant embodiment, the control unit UC1 is implemented in the microprocessor 60 itself. In other words, the microprocessor 60 is configured to block the sending of all commands to the secure element ES via at  
15 least one predefined external contact 54 (i.e. the contacts Vcc, RST, CLK, GND, and IO of the ISO 7816 standard, in this example), so long as a communication by contact or a contactless communication is ongoing between the secure element ES and an external reader.

In the event of detecting that a communication by  
20 contact or a contactless communication is ongoing between the secure element ES and the external reader, the processor 44 (and more particularly the microprocessor 60) may be configured by way of example to generate no  
25 commands for the secure element ES, or to defer the sending of any command that it might generate for the secure element ES (in which case each deferred command is stored in memory), and to do this so long as a communication is ongoing with or without contact between  
30 the secure element ES and an external reader.

If the secure element ES is not designed to operate in contactless mode, the microprocessor 60 may alternatively be configured to perform the blocking of the invention so long as a communication by contact is  
35 ongoing between the secure element ES and an external reader.

The blocking of commands from the processor unit 44 can thus be performed internally within the processor unit 44 itself and/or externally relative to the processor unit 44 (typically via the link L11).

5 Furthermore, in the above-described embodiments, it is the microprocessor 60 that uses the signals from the detector units UD1 and UD2 to determine whether there is any ongoing communication in contact mode or in  
10 external reader, and that controls the state (blocks or conductive) of the control unit UC1. It can be understood that at least one of these operations may be performed by any control unit (e.g. a microprocessor) internal to the smart card situated in or outside the  
15 processor unit 44.

In a variant embodiment, the processor unit 60 is also configured to control the state of an indicator light (not shown), e.g. such as a LED, with which the smart card 52 is provided, this control being performed  
20 as a function of whether or not an ongoing external communication is detected between the secure element ES and an external reader. The processor unit 60 may for example control such an indicator light so that its state (brightness, flashing frequency, etc.) informs the user  
25 whether an external communication is ongoing between the secure element ES and an external reader.

Figure 6 shows a smart card 75 in a second embodiment of the invention. The smart card 75 differs from the smart card 40 shown in Figure 3 only by the fact  
30 that an additional RF antenna 78 is included in the card 75 in order to detect whether a contactless communication is ongoing between the secure element ES and an external reader RD2.

More specifically, the second detector unit UD2 is  
35 suitable for using the additional RF antenna 78 to detect an RF signal transmitted or received by the first RF antenna 52 indicating that a communication is ongoing in

contactless mode between the secure element ES and the external reader RD2.

To do this, the RF antennas 52 and 78 in this example are electromagnetically coupled (e.g. by induction; link L14) so that all of the communication activity via the RF antenna 52 can be detected by the RF antenna 78. Any RF signal picked up by the RF antenna 78 is transmitted to the detector unit UD2, which operates in the manner described above with reference to the first embodiment.

Using this additional RF antenna 78 is advantageous in that it makes it possible in particular to avoid a contactless communication between the secure element ES and an external reader RD2 being disturbed by the second detector unit UD2.

As explained above, in the context of the invention it is necessary to block the sending of all commands from the processor unit (44) to the secure element (ES) via at least one predefined external contact whenever an ongoing communication with or without contact is detected between the secure element (ES) and an external reader. It should be observed that that the blocking may be unidirectional so that while blocking is being implemented, commands can still pass in the opposite direction, i.e. from the secure element (ES) to the processor unit (44). Alternatively, the blocking may be bidirectional such that all communication is prevented in both directions between the secure element (ES) and the processor unit (44).

It can thus be understood in the present disclosure that a command in the meaning of the invention may be any message (or any data) from the processor unit for the secure element.

Furthermore, in a variant, the blocking of commands from the processor unit to the secure element is maintained for a predefined length of time starting from the instant when an ongoing communication with or without

contact is no longer detected between the secure element ES and the processor unit.

As already mentioned, the nature and the elements making up the processor unit in the meaning of the invention may vary depending on circumstances. In the examples considered above, the processor unit 44 comprises in particular memories 64 and 66, an actuator 68, a battery 70, and LEDs 72. The processor unit 44 is suitable for co-operating with the secure element ES to select an application or a mode of operation to be executed by the secure element ES, the processor unit 44 being suitable for performing this selection, e.g. from a user instruction received via the actuator 68. Nevertheless, it should be understood that processor units for performing other functions can be envisaged in the ambit of the invention.

Thus, in a variant embodiment, the processor unit 44 is suitable for obtaining information from data received from the secure element ES and for causing the information to be displayed by using a display unit of the smart card 44. To do this, the processor unit 44 may for example receive said data from the secure element via the link L11. By way of example, the display unit may comprise a display screen suitable for displaying information that is useful for the user, such as the amount of a transaction or a total of units of account, or indeed an indication of a currency selected by the user. During this display method and where applicable, at least one command may be sent by the processor unit to the secure element, providing the blocking of the invention has not been triggered.

Other variants of the processor unit suitable for communicating with the secure element can naturally be envisaged in the ambit of the invention.

As mentioned above, the invention also applies to smart cards operating exclusively in contact mode. Under such circumstances, it is only the existence of

communication by contact that is monitored in order to determine whether or not to trigger the blocking of the invention. Thus, so long as an ongoing communication by contact is detected, any sending of a command from the processor unit to the secure element is blocked via at least one predefined external contact (e.g. Vcc, RST, CLK, GND, and IO in the IOS 7816 standard).

As mentioned above, the invention is not limited to smart cards, but applies more generally to any electronic device suitable for co-operating with an external reader in a contact mode, and also in a contactless mode, where applicable.

A person skilled in the art understands that the above-described embodiments and variants merely constitute non-limiting implementations of the invention. In particular, the person skilled in the art can envisage any combination of the above-described embodiments and variants in order to satisfy some particular need.

## CLAIMS

1. An electronic device (40; 75) comprising:

- a secure element (ES) comprising a plurality of contacts (54), said secure element being configured to co-operate with a first external reader (RD1) that is external to said electronic device in a contact mode by using at least one of said contacts;

- a processor unit (44) external to the secure element, said processor unit being configured to send a command (CMD2) to the secure element (ES) via at least one of said contacts (54);

the electronic device being characterized in that it further comprises:

- a first detector unit (UD1) for detecting whether a communication by contact is ongoing in contact mode between the secure element (ES) and the first electronic reader (RD1); and

- a control unit (UC1) configured to block the sending of each command (CMD2) from the processor unit (44) to the secure element (ES) via at least one predefined contact from among said plurality of contacts, so long as a said communication by contact is ongoing,

wherein the first detector unit (UD1) is connected to one of said contacts (54-1), referred to as the power contact, that is to receive electrical power when the secure element (ES) is co-operating in contact mode with the first external reader (RD1) in order to power said secure element electrically,

the first detector unit (UD1) being configured to convert a first voltage detected on the power contact (54-1) into a second voltage that is different from the first voltage,

wherein the processor unit (44) is configured to determine that a said communication by contact is ongoing between the secure element (ES) and the first external reader (RD1) only if the second voltage is not less than a first predetermined threshold value.

2. An electronic device according to claim 1, wherein said contacts (54) are in compliance with the ISO 7816 standard.

5

3. An electronic device according to claim 2, wherein at least one predefined contact comprises the contacts (54-1, 54-2, 54-3, 54-4) defined in said ISO 7816 standard as Vcc, RST, CLK, GND, and IO.

10

4. An electronic device according to any one of claims 1 to 3, wherein the control unit (UC1) is configured to block the sending of each command from the processor unit to the secure element via each of said contacts (54) of the secure element (ES) so long as a said communication by contact is ongoing.

15

5. An electronic device according to any one of claims 1 to 4, wherein the secure element (ES) includes a first radiofrequency antenna (52), said secure element being configured to co-operate with a second external reader (RD2) that is external to said electronic device in a contactless mode by using said first radiofrequency antenna, said electronic device including:

20

25       - a second detector unit (UD2) configured to detect whether a contactless communication is ongoing in contactless mode between the secure element (ES) and the second external reader (RD2);

25

the control unit (UC1) being configured to block the sending of each command (CMD2) from the processor unit (44) to the secure element (ES) via said at least one predefined contact so long as at least one of a said communication by contact and a said contactless communication is ongoing.

30

35

6. An electronic device according to claim 5, including a second radiofrequency antenna (78) isolated from the first radiofrequency antenna (52),

5 the second detector unit (UD2) being configured to use the second radiofrequency antenna (78) to detect a radiofrequency signal transmitted or received by the first radiofrequency antenna (52), indicating that a said contactless communication is ongoing between the secure element (ES) and the second electronic reader (RD2).

10

7. An electronic device according to claim 5 or claim 6, wherein the second detector unit (UD2) is configured to convert an AC voltage obtained from the first radiofrequency antenna (52) into a DC voltage.

15

8. An electronic device according to claim 7, wherein the processor unit (44) is configured to determine that a said contactless communication is ongoing only if the DC voltage is not less than a second predetermined threshold

20

value.

9. An electronic device according to any one of claims 1 to 8, wherein the control unit (UC1) comprises a switch at the interface between the secure element (ES) and the

25

processor unit (44), said switch being configured to switch between a blocking state and a conductive state,

the switch being configured to occupy the blocking state when the control unit blocks said sending of each command from the processor unit via said at least one predefined contact, so as to isolate the secure element (ES) electrically relative to the processor unit (44).

30

10. An electronic device according to any one of claims 1 to 9, wherein the processor unit (44) is configured to co-operate with the secure element (ES) to select an application to be executed by the secure element,

35

the processor unit being configured to perform this selection on the basis of an instruction from a user received via an actuator (68) of the electronic device.

5 11. An electronic device according to any one of claims 1 to 10, wherein the processor unit (44) is configured to obtain information from data received from the secure element (ES) and for causing said information to be displayed by using a display unit of the electronic  
10 device.

12. An electronic device according to any one of claims 1 to 11, wherein said electronic device (40; 75) is a smart  
15 card.

13. A blocking method implemented by an electronic device (40; 75) comprising:

- a secure element (ES) comprising a plurality of contacts (54), said secure element being configured to  
20 co-operate with a first external reader (RD1) that is external to said electronic device in a contact mode by using at least one of said contacts; and

- a processor unit (44) external to the secure element (ES), said processor unit being configured to  
25 send a command (CMD2) to the secure element via at least one of said contacts (54);

the method being characterized in that it comprises:

- first verification (S4) to determine whether a communication by contact is ongoing in contact mode  
30 between the secure element and the first external reader; and

- blocking (S6) the sending of each command from the processor unit (44) to the secure element (ES) via at least one predefined contact from among said plurality of  
35 contacts (54), so long as a said communication by contact is ongoing,

wherein the first verification comprises converting a first voltage detected on one of said contacts (54-1), referred to as the power contact, into a second voltage that is different from the first voltage, said power  
5 contact being for receiving electrical power when the secure element (ES) is co-operating in contact mode with the first external reader (RD1) in order to power said secure element electrically

wherein the processor unit (44) determines that a  
10 said communication by contact is ongoing between the secure element (ES) and the first external reader (RD1) only if the second voltage is not less than a first predetermined threshold value.

15 14. A blocking method according to claim 13, wherein the secure element (ES) includes a first radiofrequency antenna (52), said secure element being configured to co-operate with a second external reader (RD2) that is external to said electronic device in a contactless mode  
20 by using said first radiofrequency antenna, said electronic device comprising:

- second verification (S4) to determine whether a contactless communication is ongoing in contactless mode between the secure element (ES) and the second external  
25 reader (RD2); and

- blocking (S6) the sending of each command from the processor unit to the secure element via at least one predefined contact, so long as at least one of a said communication by contact and a said communication without  
30 contact is ongoing.

15. A computer program (PG2) including instructions for executing steps of a blocking method according to claim 13 or claim 14 when said program is executed by a  
35 computer.

16. A computer readable data medium storing a computer program (PG1) including instructions for executing the steps of a blocking method according to claim 13 or claim 14.