(12) UK Patent Application (19) GB (11) 2 370 659 (13) A

(43) Date of A Publication 03.07.2002

(21) Application No 0031837.8

(22) Date of Filing 29.12.2000

(71) Applicant(s)
**Nokia Corporation**
**(Incorporated in Finland)**
**Keilalahdentie 4, FIN-02150 Espoo, Finland**

(72) Inventor(s)
**Peter Vestergaard**
**Rune Lindholm**

(74) Agent and/or Address for Service
**Venner Shipley & Co**
**20 Little Britain, LONDON, EC1A 7DH,**
**United Kingdom**

(51) INT CL[7]
**G06F 1/00**

(52) UK CL (Edition T )
**G4A** AAP

(56) Documents Cited
**GB 2346239 A** **GB 2331821 A**
**EP 1085395 A** **WO 00/43875 A**
**WPI abstract 2000-024385 & DE 19816541A**
**WPI abstract 1988-127391 & DE 3736190 A**

(58) Field of Search
UK CL (Edition S ) **G4A AAP**
INT CL[7] **G06F 1/00**
**ONLINE: WPI,EPODOC,JAPIO**

(54) Abstract Title
**Method of controlling access to a data file held by a smart card**

(57) Smart cards 10 can hold data for a number of different applications. A gateway 34 is provided through which access to the smart card by external devices 31 is controlled. Even though the external device may have access to certain application data, such as credit card details, it may not have access to sensitive information, such as authentication and ciphering keys. The external device may be a mobile telephone.

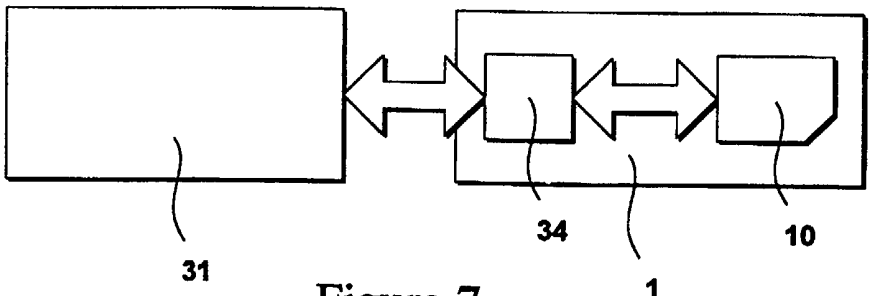


Figure 7

GB 2 370 659 A

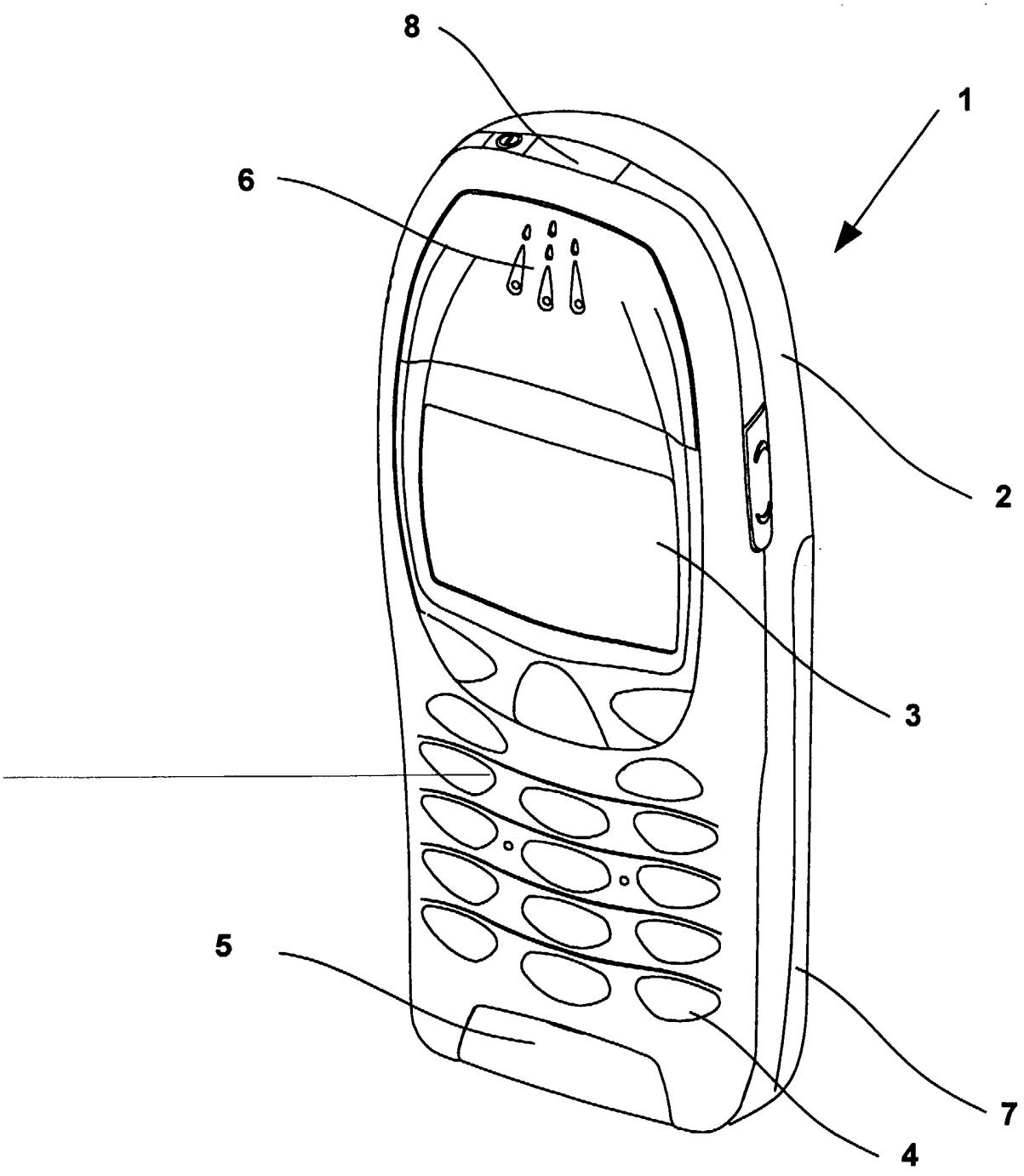


Figure 1

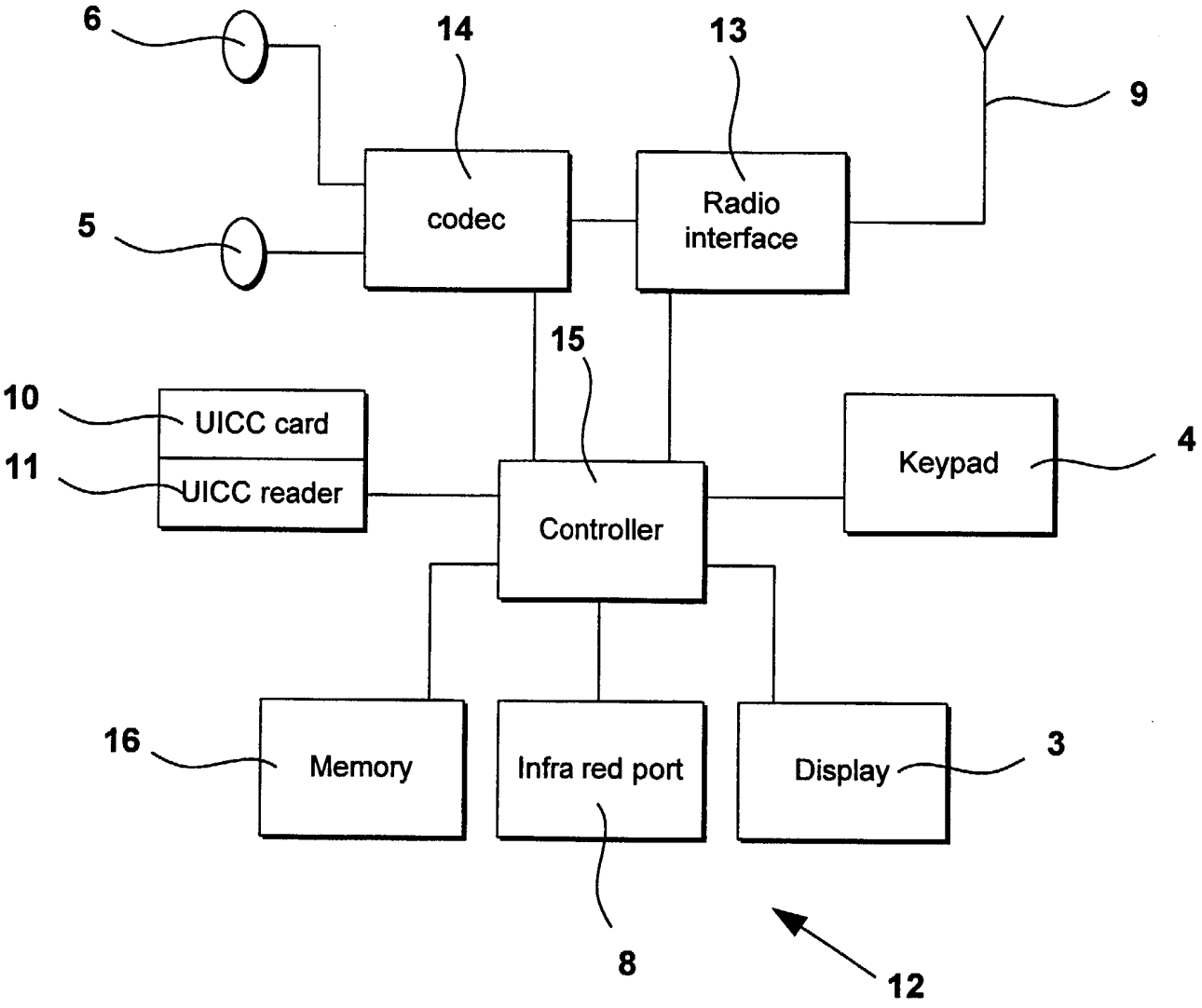


Figure 2

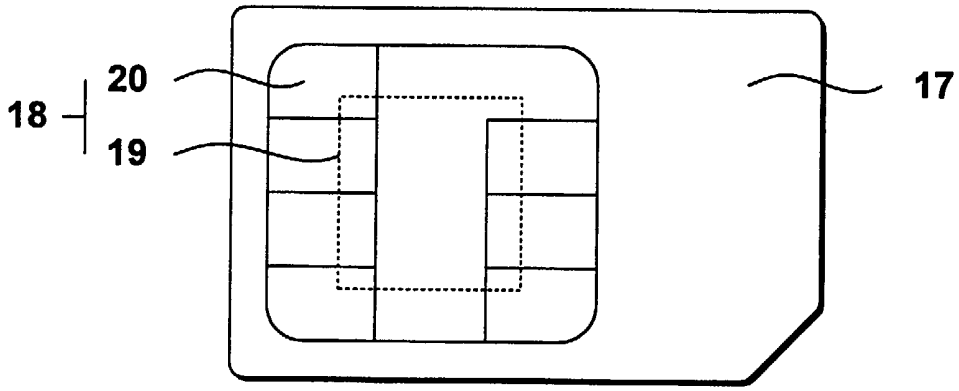


Figure 3

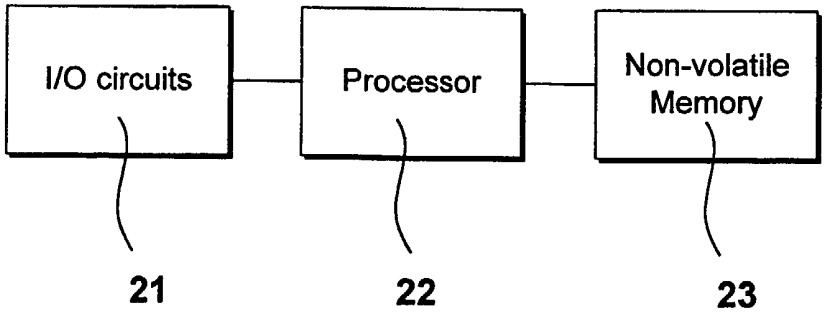


Figure 4

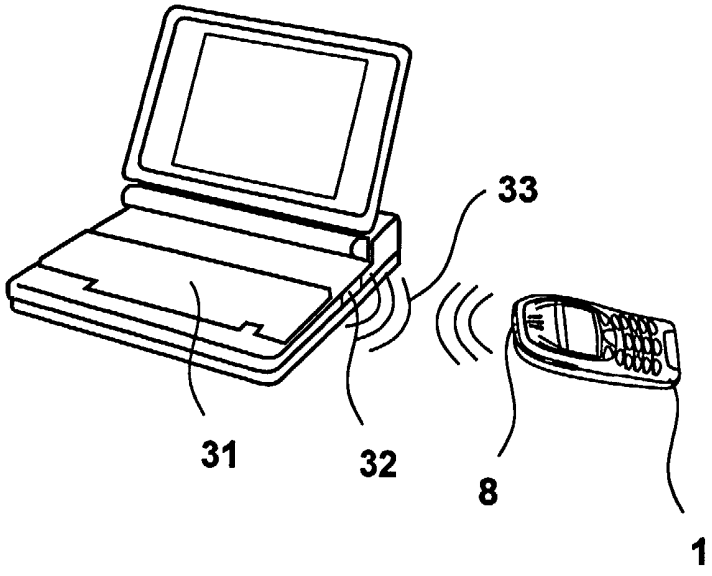


Figure 6

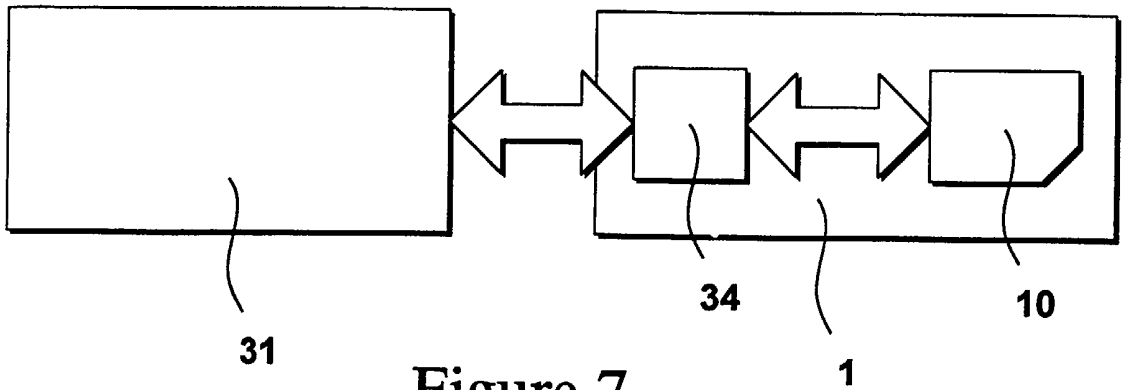


Figure 7

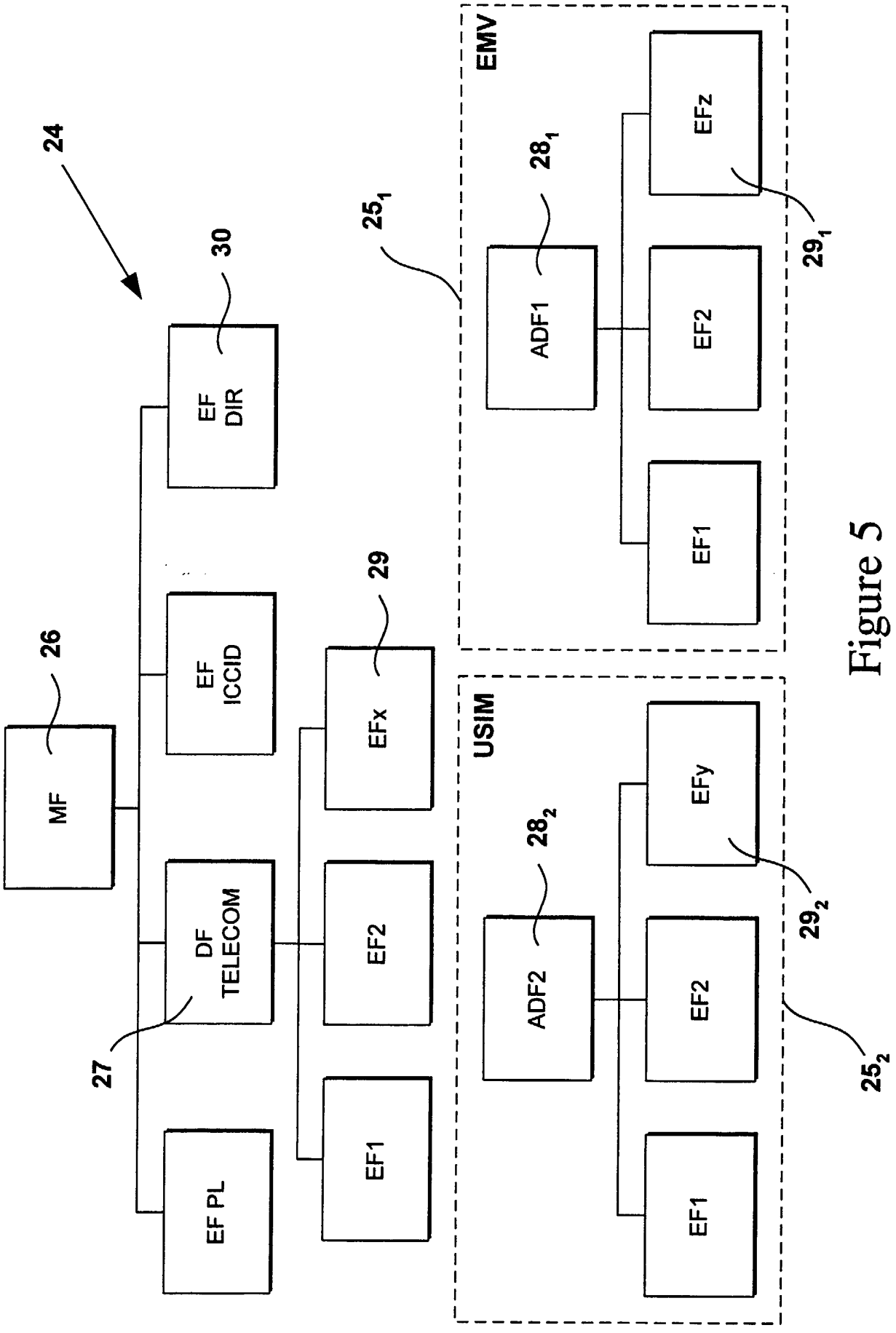
24
MF
26
EF DIR
30
EF ICCID
DF TELECOM
27
EF PL
EFx
29
EF2
EF1
EMV
$25_1$
$28_1$
ADF1
EF2
EF1
EFz
$29_1$
USIM
$25_2$
$28_2$
ADF2
EF2
EF1
EFy
$29_2$

Figure 5

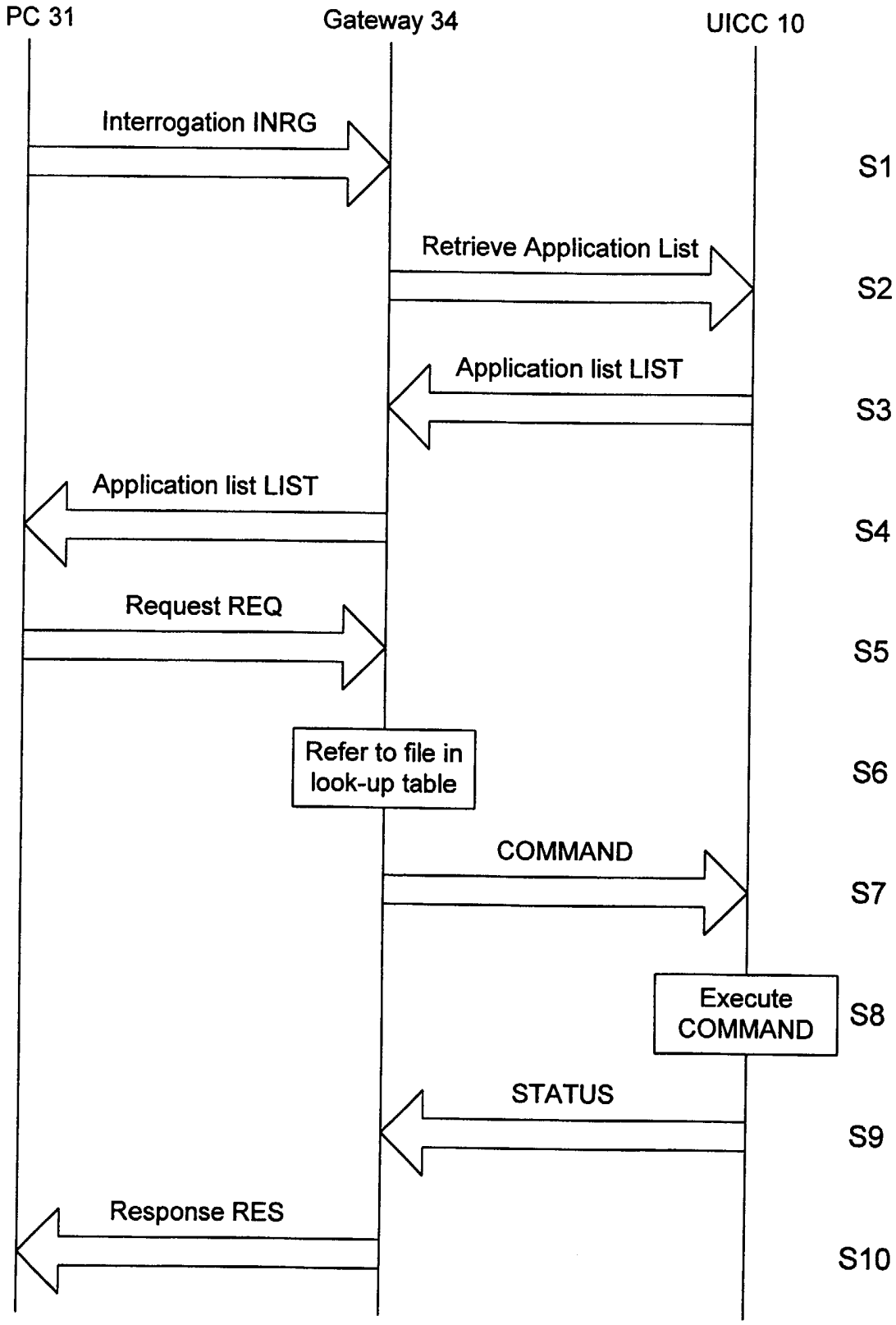
PC 31
Gateway 34
UICC 10
Interrogation INRG
S1
Retrieve Application List
S2
Application list LIST
S3
Application list LIST
S4
Request REQ
S5
Refer to file in look-up table
S6
COMMAND
S7
Execute COMMAND
S8
STATUS
S9
Response RES
S10

Figure 8a

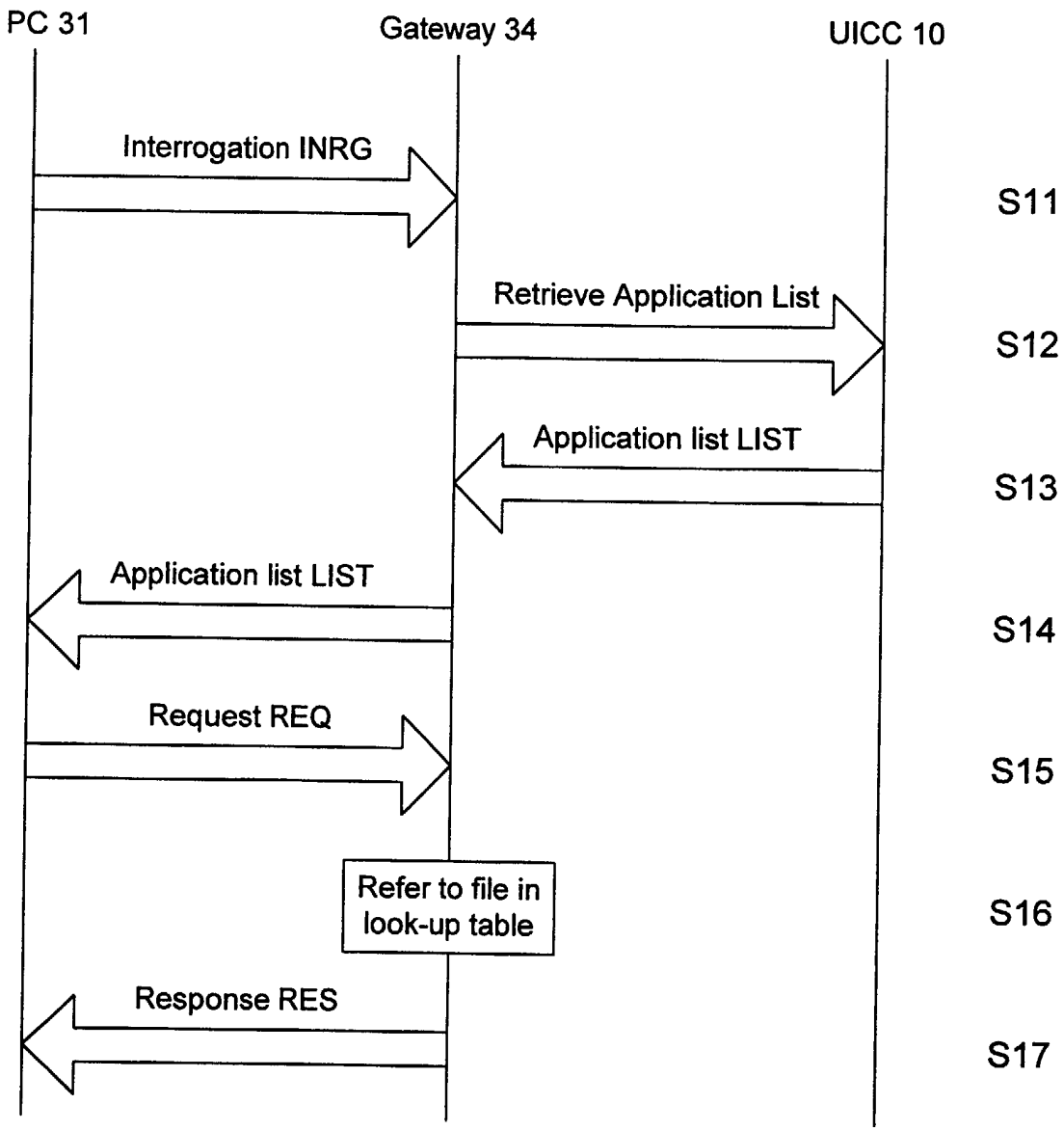
PC 31
Gateway 34
UICC 10
Interrogation INRG
S11
Retrieve Application List
S12
Application list LIST
S13
Application list LIST
S14
Request REQ
S15
Refer to file in look-up table
S16
Response RES
S17

Figure 8b

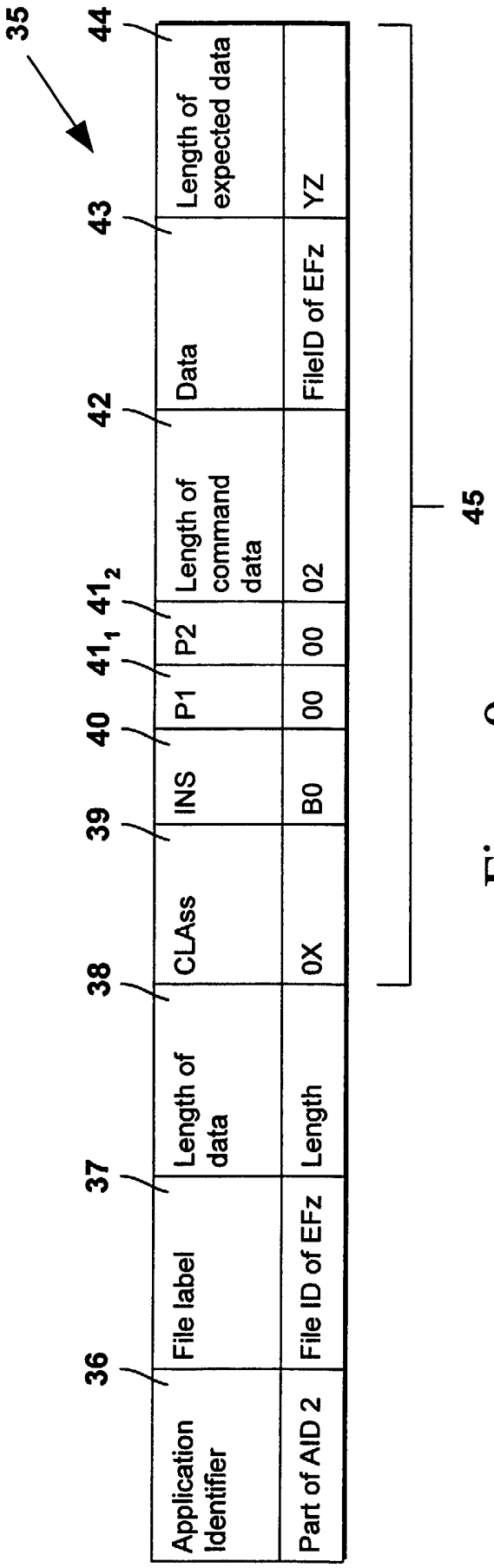


Figure 9

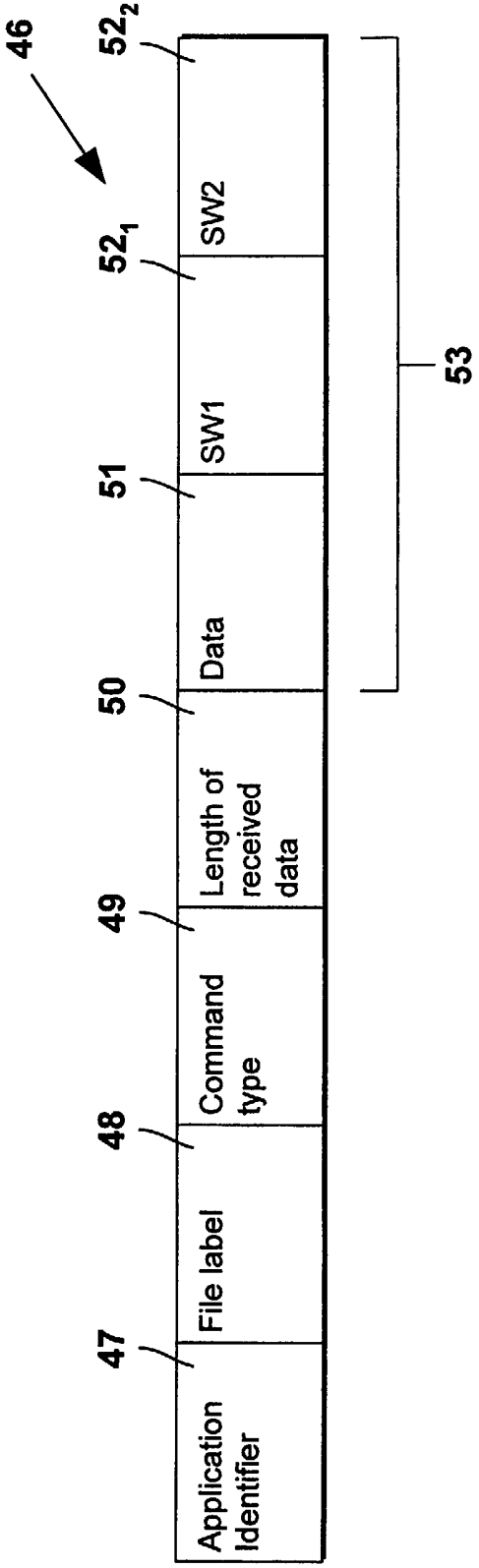


Figure 10

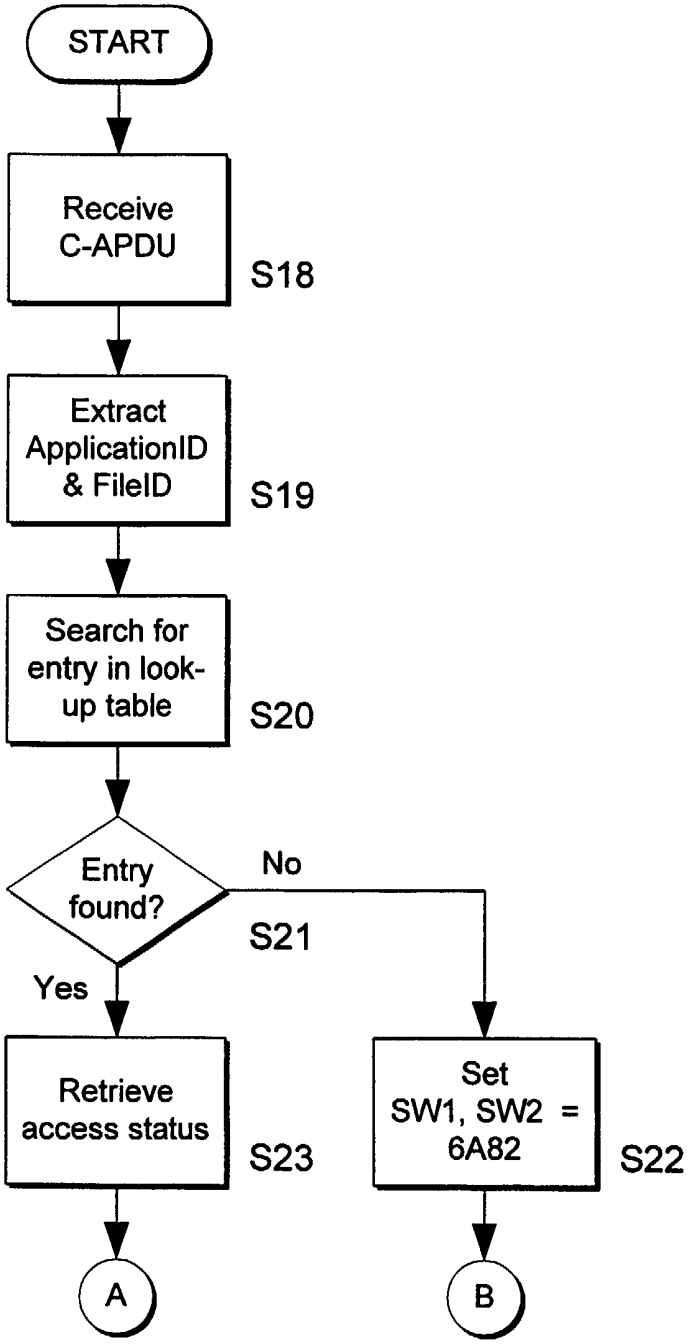
START
Receive C-APDU
S18
Extract ApplicationID & FileID
S19
Search for entry in look-up table
S20
Entry found?
No
S21
Yes
Retrieve access status
S23
Set SW1, SW2 = 6A82
S22
A
B

Figure 11

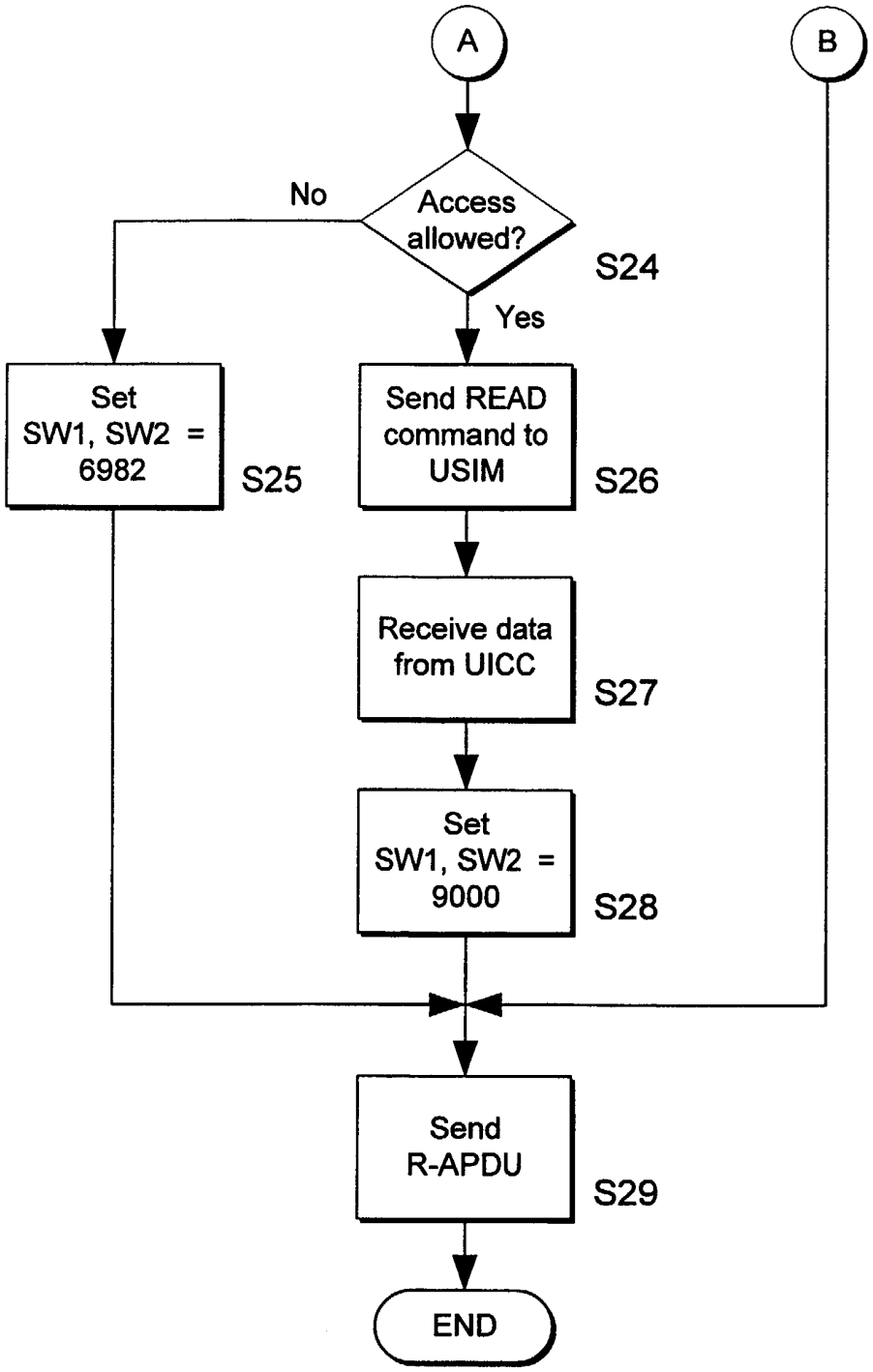
A
B
Access allowed?
S24
No
Yes
Set SW1, SW2 = 6982
S25
Send READ command to USIM
S26
Receive data from UICC
S27
Set SW1, SW2 = 9000
S28
Send R-APDU
S29
END

Figure 11

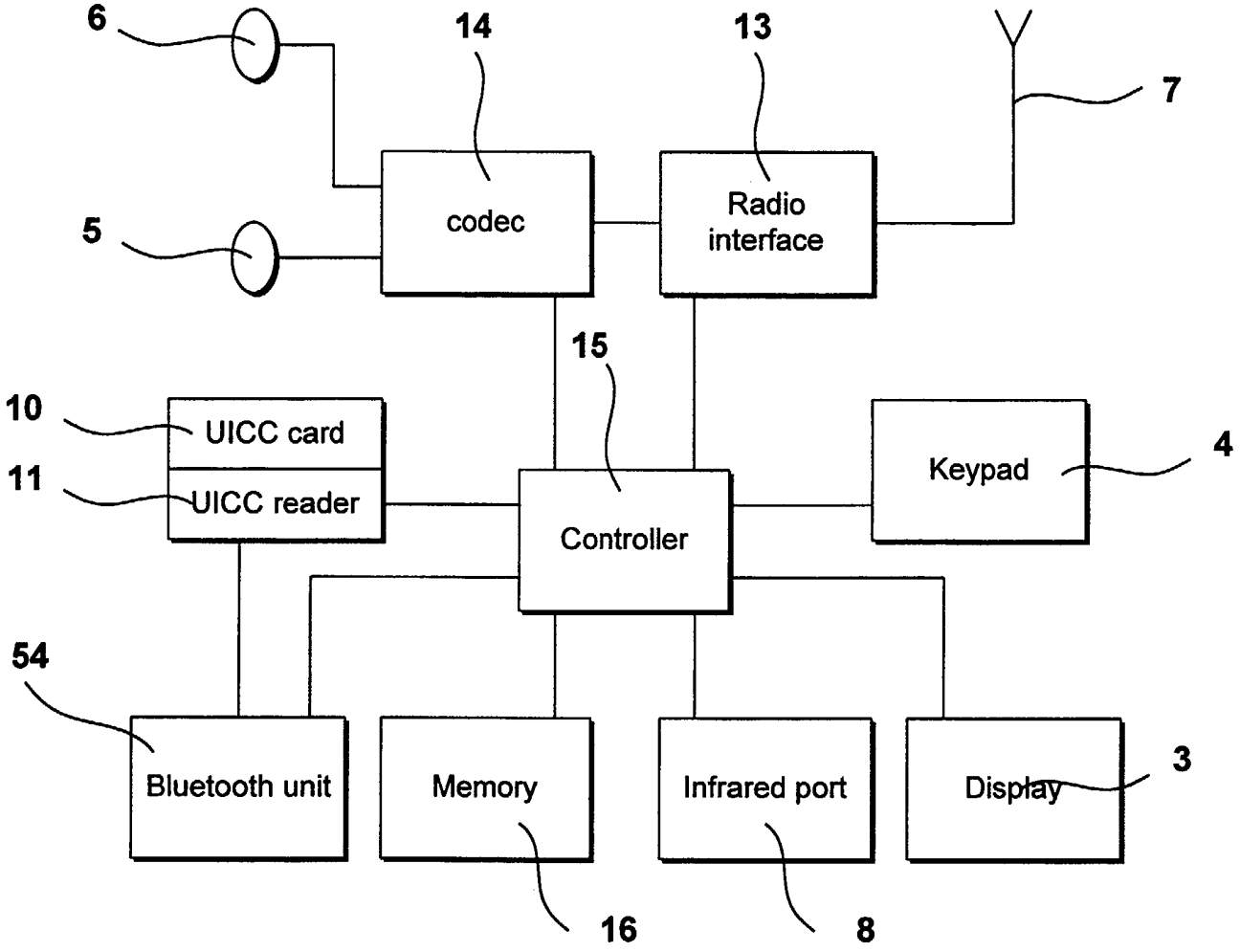


Figure 12

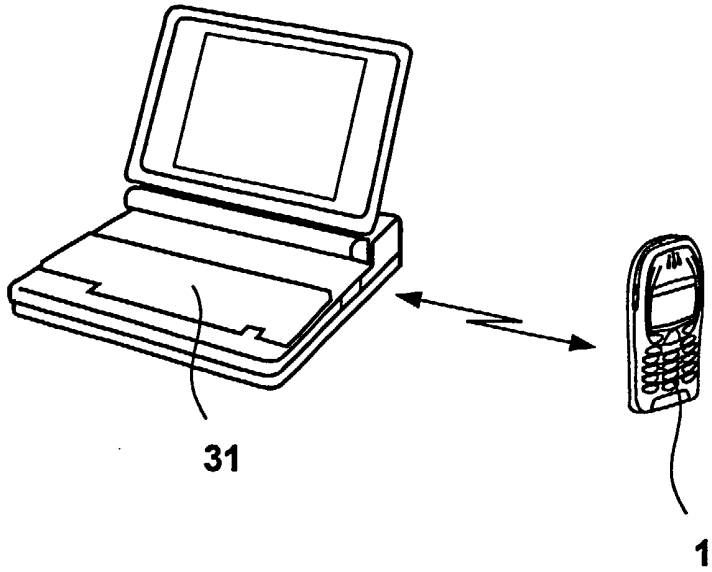


Figure 13

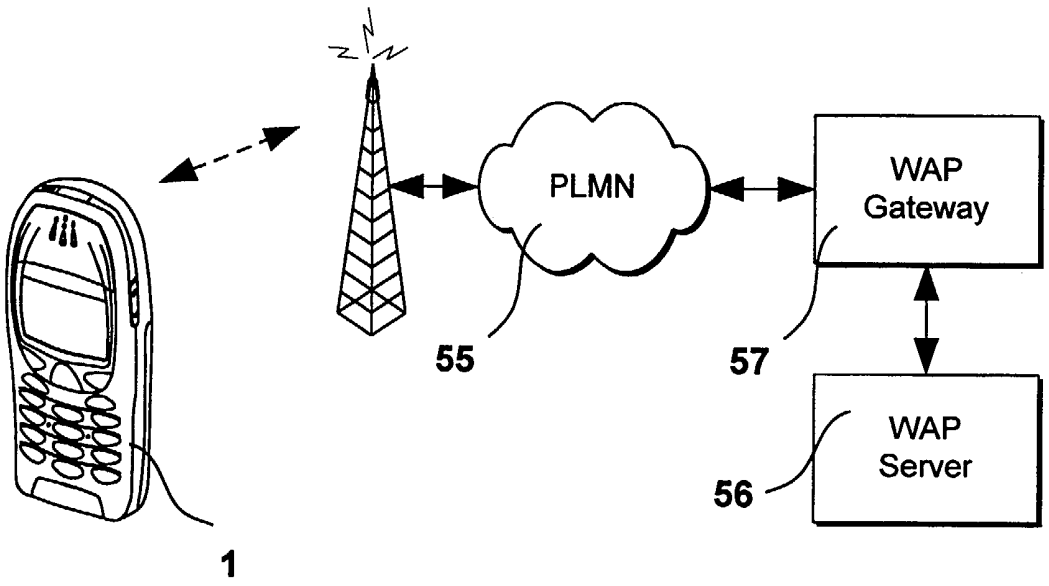


Figure 14

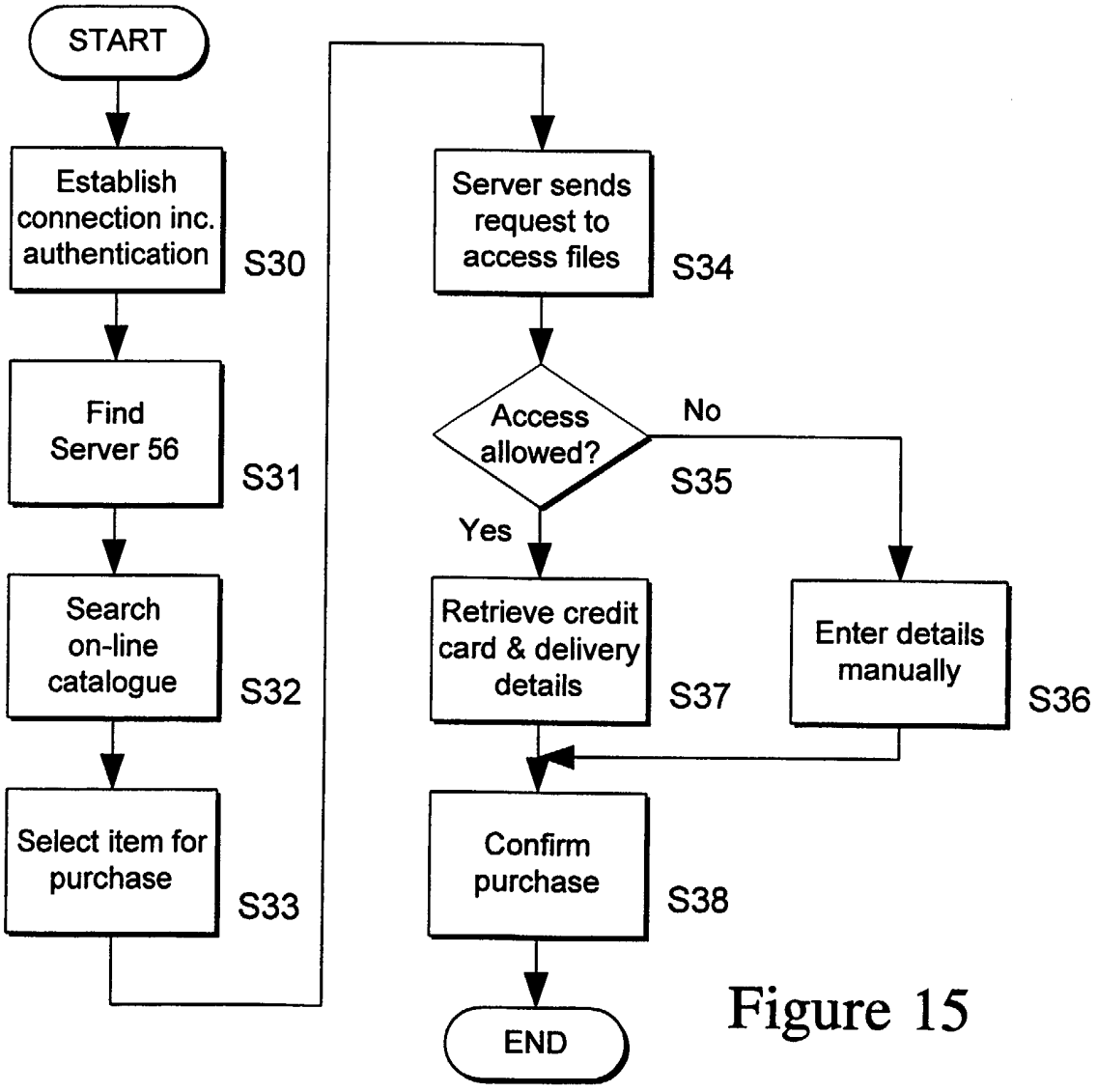


Figure 15

2370659

# Method of controlling access to a data file held by a smart card

## Description

The present invention relates to a method of controlling access to a data file held by a smart card.

Smart cards are commonly used in mobile telephone handsets, payment systems and for user identification. An overview of smart cards and their application is given in "Smart Card Handbook" by W. Rankl & W. Effing, John Riley & Sons, 2000 [ISBN 0471988758].

In mobile telephone handsets conforming to the Global System for Mobile Communications (GSM) standard, a smart card is usually referred to as a subscriber identification module (SIM) card. The SIM card holds a subscriber's identity number, security information and memory for a personal directory of telephone numbers. An overview of SIM cards is given in "The GSM System for Mobile Communications" by M. Mouly & M. B. Pautet, Sell & Sys, 1992 [ISBN 950719007], pp 67-71.

In payment systems, such as credit and debit cards and electronic money, a smart card may be used to hold a variety of different types of information and provide secure methods of payment. Payment systems employing a smart card usually conform to the Europay-Mastercard-Visa (EMV) standard and a copy of the specification may be obtained from www.emvco.com. An overview of payment systems is given in "Electronic Payment Systems", by D. O'Mahony, M. Peirce and H. Tewari, Artech House, 1997 [ISBN 08900692555] and at www.mastercard.com.

Increasingly smart cards hold many different types of information accessible to different applications such electronic payment systems and telecommunications. This is known as open access and such a smart card capable of housing different applications is a universal integrated circuit card (UICC). However, it is desirable to restrict access to some files, especially those concerned with personal and financial

information or those containing data necessary for user authentication and call encryption.

Furthermore, mobile telephones are increasingly capable of exchanging data and accessing the internet. Therefore, the opportunity arises of using the mobile telephone handset to make and pay for purchases over the internet. It is preferable that data available to different applications should be delimited in some way.

The present invention seeks to help allow open access to a smart card used by different applications.

According to the present invention there is provided a method of controlling access to a data file held by a smart card, the method comprising providing an access table including an indication whether access to said file is allowed, receiving a request for access identifying said data file, deciding whether access to said data file is allowed in dependence upon said indication and, if access is allowed, providing access to said file.

The receiving said request may include receiving an instruction to execute a command in respect of said file. Alternatively, the method may further include receiving an instruction to execute a command in respect of said file. The providing access may comprise transmitting said instruction to execute the command in respect of said file to said smart card.

The method may further comprise receiving information in relation to execution of said command from said smart card. The receiving of the information may comprise receiving confirmation that the command has been executed or data from said file.

The providing access to said file may include reading or writing to said file.

According to the present invention there is also provided a method, in a controller, of controlling access to a data file held by a smart card, the method comprising

receiving a request for access identifying said data file, deciding whether access to said file is allowed and, if access is allowed, providing access to said file.

According to the present invention there is also provided a method of programming a controller which controls access to a data file held by a smart card, the method comprising providing access data including an indication whether access to said file is allowed

According to the present invention there is also provided a computer program to be loaded on data processing apparatus to control access to a data file held by a smart card, such that the data processing means provides an access table including an indication whether access to said file is allowed, receives a request for access identifying said data file, decides whether access to said data file is allowed in dependence upon said indication and, if access is allowed, provides access to said file.

According to the present invention there is also provided a device to control access to a data file held by a smart card comprising means for providing an access table including an indication whether access to said file is allowed, means for receiving a request for access identifying said data file, means for deciding whether access to said data file is allowed in dependence upon said indication and means for providing access to said file.

According to the present invention there is also provided electronic apparatus or a mobile telephone incorporating said device.

Embodiments of the present invention will now be described, by way of example, with reference to the accompanying drawings, in which:-

Figure 1 is an exploded view of a mobile telephone according to a first embodiment of the present invention;

Figure 2 is a schematic representation of telephone circuits of the mobile telephone shown in Figure 1;

Figure 3 is a plan view of a universal integrated circuit card;

Figure 4 is a schematic representation of the circuits of the universal integrated

circuit card shown in Figure 3;

Figure 5 is schematic diagram of the memory structure held by the universal integrated circuit card shown in Figure 3;

Figure 6 shows a laptop personal computer with an infra red port exchanging information with the mobile telephone shown in Figure 1;

Figure 7 is schematic diagram of information exchange between the personal computer and the mobile telephone;

Figures 8a and 8b are sequence diagrams of the interaction between the personal computer and the mobile telephone;

Figure 9 is a schematic representation of a request message from the personal computer;

Figure 10 is a schematic representation of a response message from the mobile telephone,

Figure 11 is a process flow diagram of the response of the mobile telephone

Figure 12 is a schematic representation of telephone circuits of the mobile telephone according to a second embodiment;

Figure 13 shows a laptop personal computer with Bluetooth unit exchanging information with a mobile telephone also having a Bluetooth unit;

Figure 14 is a schematic block diagram illustrating the mobile telephone communicating through a PLMN with a WAP server and

Figure 15 is process flow diagram of making a purchase on with the mobile telephone.

## First embodiment

Referring to Figures 1 and 2, a mobile telephone 1 comprises a housing 2, a liquid crystal display 3, a keypad 4, a microphone 5, an ear-piece 6, battery 7, an infrared port 8, antenna 9, a universal integrated circuit card (UICC) 10, a UICC card reader 11 and mobile telephone circuitry 12. The mobile telephone circuitry 12 includes radio interface circuitry 13, codec circuitry 14, controller 15 and memory 16. Individual circuits and elements are of a type well known in the art, for example in the Nokia range of mobile telephones.

Referring to Figures 3 and 4, the UICC card 10 comprises a plastics card body 17 and a module 18, which comprises an integrated circuit 19 and contacts 20. The integrated circuit 19 comprises input/output circuits 21, a processor 22 and non-volatile memory 23.

The UICC card 10 conforms to International Standards Organisation/International Electrotechnical Commission (ISO/IEC) 7816. A copy of the ISO/IEC standards may be obtained from ISO at Case Postale 56, 1211 Geneva 20, Switzerland. The UICC card 10 may also conform to other standards, for example Europay-Mastercard-Visa (EMV) set of specifications which relate to standards for international debit and credit cards. A copy of the EMV standards may be obtained from Europay at 198A Chausée de Tervuren, B-1410 Waterloo, Belgium.

Referring to Figure 5, files stored in memory 23 are organised according to a hierarchical structure 24 and are grouped according to application 25. The structure 24 comprises a master file (MF) 26, dedicated files (DF) 27, application dedicated files (ADFs) 28 and elementary files (EFs) 29. An ADF 28 is a particular type of DF 27 and serves as a point of entry to EFs 29 of a particular application. A directory file 30 attached to the MF 26 is used to access ADFs 28. Usually, an external device wishes access to the contents of EFs 29.

Referring to Figure 6, the mobile terminal 1 may exchange information with an external device, for example a laptop personal computer (PC) 31 having an infrared (IR) port 32, through an IR link 33.

Referring to Figure 7, a functional representation of the interface between the mobile terminal 1 and the PC 31 is shown. Access to DFs 27, ADFs 28 and EFs 29 stored in the memory 23 of the UICC 10 is controlled by an external interface gateway 34. The gateway 34 is the implemented in software by the controller 15. The gateway 34 prevents PC 31 from having direct access to DFs 27, ADFs 28 and EFs 29. The gateway 34 has available to it the location of a file, such as a first EF $29_1$, within the hierarchical structure 24 and whether the PC 31 is allowed access to it. In this example, "access" is understood to include reading and writing to the file,

although specific types of access are defined in ISO/IEC 7816 and EMV standards. Thus, access by the PC 31 to the first EF $29_1$ is non-transparent because no path information is sent to the PC 31. The gateway 34 performs any command received from the PC 31 on its behalf. Furthermore, the gateway 34 provides a standard interface between the PC 31 and the UICC 10.

Referring to Figure 8a, a sequence diagram of the exchange of signals within the application layer between the PC 31 and the mobile telephone handset 1 is shown in which the PC 31 successfully retrieves the first EF $29_1$ from the UICC 10. A description of the signal exchanges within the physical, data link and terminal transport layers may be found in the ISO/IEC 7816 and EMV standards

The PC 31 sends an interrogation signal INRG over the IR link 33, requesting a list of applications LIST held by the card (step S1). The list of applications is held by the directory file 30. The exchange 34 retrieves the application list LIST from the directory 30 and sends it to the PC 31 over the IR link 33 (steps S2, S3 & S4). The PC 31 sends a request REQ to read the contents of a particular file, in this example the first EF $29_1$ which holds a credit card number. The first EF $29_1$ is attached to a first application AID1 $25_1$, which in this example is a banking application such as EMV, and is entered through a first ADF $28_1$ (step S5). The form and content of the request REQ will be described in more detail below. The gateway 34 checks whether the PC 31 is allowed access to the first EF $29_1$ by referring to a look-up table (not shown) (step S6). In this example, the look-up table is held in memory 16. The form and content of the table will be described in more detail later. If the PC 31 is allowed access to the first EF $29_1$, then the gateway 34 performs a command COMMAND contained in the request REQ, in this example to read the contents of the first file EF $29_1$ (step S7). The contents of the first EF $29_1$ is retrieved and a response RES sent to the PC 31 containing the contents of the first EF $29_1$ (steps S8, S9 & S10).

Referring to Figure 8b, a sequence diagram of the interaction between the PC 31 and the mobile telephone 1 is shown in which the PC 31 is unsuccessful in its attempt to retrieve a second EF $29_2$ from the UICC 10.

The PC 31 sends an interrogation signal INRG over the IR link 33, requesting a list of applications held by the card (step S11). The exchange 34 retrieves the application list LIST from the directory 30 and sends it to the PC 31 over the IR link 33 (steps S12, S13 & S14). The PC 31 sends a request REQ to read the contents of a particular file, in this example the second EF $29_2$ which holds a ciphering key used in mobile telecommunications. The second EF $29_2$ is attached to a second application AID2 $25_2$, which in this example is a telecommunication application, such as a universal subscriber identification module (USIM) and is accessed through a second ADF $28_2$ (step S15). The gateway 34 checks whether the PC 31 is allowed access to the second EF $29_2$ by referring to a look-up table (not shown) (step S16). If the PC 31 is not allowed access to the second EF $29_2$ then the gateway 34 sends a response RES to the PC 31 containing an error message indicating that the PC 31 is not allowed access (step S17). Similarly, if the PC 31 requests the contents of a file which does not exit, when the gateway 34 checks the look-up table and does not find the file, it returns an error message indicating that the file has not been found. It will be appreciated that instead of retrieving the application list LIST every time a command is sent, it may be retrieved once per card session during which many access requests are made.

Referring to Figure 9, an example of a request command REQ 35 using an ISO 7816 definition control-application protocol data unit (C-APDU) is shown together with exemplary data in the case that the PC 31 wants to read the content of the first EF $29_1$ in the application. The request 35 comprises an application identifier (AID) field 36, which identifies the application the PC 31 wishes to access. In this example, the AID 36 comprises a registered application provider identifier (RID) and a proprietary application identifier extension (PIX). The request 35 further comprises a file label field 37, which identifies the file to be accessed. The request 35 also includes a length of data string 38 and a class (CLA) byte 39, which identifies the instruction to be performed on the file. The request 35 further comprises an instruction byte (INS) 40, which identifies the type of instruction the application should perform, such as read or write and first and second parameter (P) bytes $41_1$, $41_2$, which further subdivide the operations described in the instruction byte 40. The request 35 further includes a length of command data field 42, which

indicates the number of bytes that the card 10 should expect. The request 35 also comprises a data field 43, which could for example contain data to be stored in a selected file or a path to a file to be read. The request 35 also comprises a length of expected data field 44, which indicates the number of bytes the PC 31 expects to receive from the mobile terminal 1.

In this example, the class, instruction and parameter bytes 39, 40, 41 together with the length of command, data and expected data fields 42, 43, 44 are a C-APDU string 45 which is defined in accordance with ISO 7816. It will be appreciated that these fields are conditional.

Referring to Figure 10, an example of a response RES 46 is shown. The response 46 comprises application identifier 47, file label 48 and command type fields 49 fields as described above. The response 46 further includes length of received data and data fields 50, 51 and it will be appreciated that these fields 50, 51 are conditional. The response 46 also comprises first and second status words (SWs) $52_1$, $52_2$, which indicate the status of the response.

In this example, the data field 52 and the status words $52_1$, $52_2$ are a response-application protocol data unit (R-APDU) string 53 which is defined in accordance with ISO 7816. Thus, for example, if the first and second status words $52_1$, $52_2$ contain between them "6A82", this indicates "file not found" and "6982" indicates "security status not satisfied".

Referring to Table 1 below, the look-up table comprises a list of EFs 29 together with flags indicating whether access by the PC 31 is allowed. In this example, a flag set to "1" indicates that access is allowed, while a flag set to "0" indicates that access is not permitted. The look-up table holds different types of information. For example, the DF TELECOM file 27 is point of entry for general telecommunications information such as an abbreviated dialling numbers EF. Further examples of EFs in the DF TELECOM file 27 are found in 3GPP Technical Specification 31.102. The ADFs 28 provide points of access to data related to other applications. For example, the first ADF $28_1$ is point of access to

credit card information such as card number, issue number, expiry date, card holder's name and card issuer. Each credit card, debit card and electronic cash card may be represented by a separate application 25. In this example, the second ADF $28_2$ contains USIM data, such as ciphering keys, subscription identity and memory for short message service (SMS). It will be appreciated that other applications having information stored on the card 10 may include driving licence, health details and insurance, club membership, automobile breakdown membership and library card.

TABLE 1

| File | Access |
|---|---|
| Contents of EFs 29 at the MF 26 level | |
| EFDIR | 1 |
| EFICCID (ICC Identity) | 1 |
| EFPL (Preferred Language) | 1 |
| Contents of EFs 29 at DF TELECOM level | |
| EF1 (Abreviated Dialling Number) | 0 |
| EF2 | 1 |
| Efx | 0 |
| Contents of EFs 29 at ADF1 $28_1$ level | |
| EF1 (Credit Card Number) | 1 |
| EF2 (PIN number) | 0 |
| EFy (Credit Card Expiry Date) | 1 |
| Contents of EFs 29 at ADF2 $28_2$ level | |
| EF1 (Ciphering Keys) | 0 |
| EF2 (Subscription Identity) | 0 |
| EFz (SMS storage) | 1 |

Referring to Figure 11, a process flow for operation of the gateway 34 is shown.

The gateway 34 receives the request 35 and extracts the application and file identifiers 36, 37 which identify an ADF 28 and an EF 29 respectively (steps S18 & S19) The gateway 34 searches for the EF 29 (steps S20 & S21). If it does not find the EF 29, then it sets the first and second status word $52_1$, $52_2$ to "6A82" indicating that the file has not been found (step S22). If it does find the EF 29, then retrieves the access status (step S23). The gateway 34 checks the access status (step S24). If access is denied, then it sets the first and second status word $52_1$, $52_2$ to "6982" indicating that access is denied (step S25). If access is permitted, then the gateway 24 sends a command, for example read contents of EF 29, to the UICC 10 (step 26). The gateway 34 receives the contents of the EF 29 and sets the first and

second status word $52_1$, $52_2$ to "9000" indicating that access is permitted (steps S27 & S28). Once the response 46 has been assembled, it is sent to the PC 31 (step S29).

If the command at step S26 is to write data to EF 29, then the gateway 34 sends the data to UICC 10. Once the data has been written, the UICC 10 confirms writing of the data. The gateway 34 sets the first and second status word $52_1$, $52_2$ to "9000" indicating that writing is successful.

It will be appreciated that the gateway 34 and the UICC 10 communicate using C-APDU and R-APDUs.

**Second embodiment**

Referring to Figures 1, 12 and 13, the mobile telephone handset 1 of the first embodiment of the present invention is modified to include a Bluetooth unit 54. This allows the mobile telephone handset 1 to communicate with the PC 31, which has also been modified to include a Bluetooth unit (not shown) over a short-range radio link. A Bluetooth specification (version 1.0B) and a system overview may be found on the world-wide web at www.bluetooth.com or ordered from Bluetooth SIG, c/o Daniel Edlund, Facsimile No.: +46 70 615 9049.

The exchange of information between the mobile telephone 1 and the PC 31 is similar to the that described in the first embodiment with reference to Figures 3, 4, 5, 7, 8a, 8b, 9a, 9b, 10 and 11. The gateway 34 is implemented in software by the controller 15. Alternatively, the gateway 34 may be implemented independently of the controller 15 by the Bluetooth unit 54 itself.

**Third embodiment**

Referring to Figures 1 and 14, the mobile telephone 1 according to the first embodiment of the invention is modified so as to support wireless application protocol (WAP). The mobile telephone 1 may used not only to search for an item, such a television set, on the internet but also to pay for it using a credit card application on the USIM 10.

An overview of WAP and the wireless application environment (WAE) may be found at http://www.wapforum.org/.

The mobile telephone 1 is in radio communication with a public land mobile network (PLMN) 55 through which it may exchange content with a WAP server 56 via a WAP gateway 57. The mobile telephone 1 is configured to execute browser software with which a user can access and view content provided by the server 56. In this example, a supplier of electrical goods maintains the server 56 and it is possible to browse an on-line catalogue and select and pay for a purchase.

Referring to Figure 15, a flow diagram of a purchase selection and payment process is shown. The server 56 is accessed by dialling an individual telephone number associated with the WAP gateway 57. A connection to the PLMN 55 is established, involving authentication of the user using Ki and encryption of transmission signals using Kc (steps S30). This process involves the mobile telephone 1 accessing values of Ki and Kc held by the UICC 10. Security management is described in "The GSM System for Mobile Communications" ibid., pp 477 to 492. Once a secure encrypted connection to the WAP gateway 57 has been established, the user selects a link to the server (step S31). The user searches the on-line catalogue for the television set of his choice (step 32). Once they succeed in finding their choice of television, they select a link "BUY" (step S33). The server 56 obtains delivery and payment information from the UICC 10 according to the procedure outlined in Figures 8a and 8b (step S34). For example, the server 56 sends a request for the contents of the first EF $29_1$ which contains the user's credit card number. The server 56 goes on further to request name and address of the user. If at any point the gateway 34 decides that the server 56 is not allowed to access the UICC 10, then the server 56 may request the user to enter the information on the keypad 4 (step S35 & S36). Otherwise, if the sequence of requests is successful (step S37), then the server 56 sends a message to the mobile telephone 1 that the transaction is complete (step S38).

Use of the gateway 34 has the advantage that it is possible to delimit access to different applications. In particular, even though an external agent may have access

to application data, such as credit card details, it may not have access to sensitive information, such as authentication and ciphering keys. The gateway 34 provides a means to prevent fraudulent attempts to obtain such keys and so defraud the telephone billing system. Thus, even though an external device may have successfully accessed some data on the UICC 10, it does not mean that it will have complete freedom to access all data on the UICC 10, such as files of another application.

It will be appreciated that many modifications may be made to the embodiments described above. For example, the connection between the mobile telephone and the PC need not be wireless. The exchange may be located in the smart card. A dedicated smart card reader may be used instead of a PC. The smart card may be of the contactless type. The request message may include the identity of the external device. The look-up table may list different sets of flags for different external devices. Access to the data file may be dependent upon the type of external device seeking access. Encryption may also be used, particularly encryption of a type used in SIM cards.

## Claims

1. A method of controlling access to a data file held by a smart card, the method comprising providing access data including an indication whether access to said file is allowed, receiving a request for access identifying said data file, deciding whether access to said data file is allowed in dependence upon said indication and, if access is allowed, providing access to said file.

2. A method according to claim 1 wherein the receiving of the request includes a receiving an instruction to execute a command in respect of said file.

3. A method according to claim 1 wherein the method further comprises receiving an instruction to execute a command in respect of said file.

4. A method according to either claim 2 or claim 3 wherein the providing access comprises transmitting said instruction to execute the command in respect of said file to said smart card.

5. A method according to claim 4 further comprising receiving information in relation to execution of said command from said smart card.

6. A method according to claim 5 wherein the receiving of the information comprises receiving confirmation that the command has been executed.

7. A method according to claim 5 or 6 wherein the receiving of the information comprises receiving data from said file.

8. A method according to any preceding claim wherein the providing access to said file includes reading said file.

9. A method according to any one of claims 1 to 8 wherein the providing access to said file includes writing to said file.

10. A method of controlling access to a data file held by a smart card substantially as hereinbefore described with reference to Figures 1 to 11 of the accompanying drawings.

11. A method of controlling access to a data file held by a smart card substantially as hereinbefore described with reference to Figures 1, 3 to 5 and 7 to 13 of the accompanying drawings.

12. A method, performed by a controller, of controlling access to a data file held by a smart card, the method comprising receiving a request for access identifying said data file, deciding whether access to said file is allowed and, if access is allowed, providing access to said file.

13. A method of programming a controller which controls access to a data file held by a smart card, the method comprising providing access data including an indication whether access to said file is allowed.

14. A computer program to be loaded on data processing apparatus to control access to a data file held by a smart card, such that the data processing means provides an access data including an indication whether access to said file is allowed, receives a request for access identifying said data file, decides whether access to said data file is allowed in dependence upon said indication and, if access is allowed, provides access to said file.

15. A device to control access to a data file held by a smart card comprising:

means for providing an access data including an indication whether access to said file is allowed;

means for receiving a request for access identifying said data file;

means for deciding whether access to said data file is allowed in dependence upon said indication and

means for providing access to said file.

16. A device to control access to a data file held by a smart card comprising:

memory to store an access data including an indication whether access to

said file is allowed;

receiver for receiving a request for access identifying said data file;

a controller for deciding whether access to said data file is allowed in dependence upon said indication and

a switch for providing access to said file.

17. A device to control access to a data file held by a smart card substantially as hereinbefore described with reference to Figures 1 to 11 of the accompanying drawings.

18. A device to control access to a data file held by a smart card substantially as hereinbefore described with reference to Figures 1, 3 to 5 and 7 to 13 of the accompanying drawings.

19. Electronic apparatus including a device according to any one of claims 15 to 18.

20. A mobile telephone including a device according to any one of claims 15 to 18.

21. A smart card comprising a device to control access to a data file held by the smart card comprising:

means for providing access data including an indication whether access to said file is allowed;

means for receiving a request for access identifying said data file;

means for deciding whether access to said data file is allowed in dependence upon said indication and

means for providing access to said file.

22. A smart card comprising memory to store a data file and access data including an indication whether access to said file is allowed.

**Application No:** GB 0031837.8 **Examiner:** Colin Clarke
**Claims searched:** 1-22 **Date of search:** 20 November 2001

# Patents Act 1977
# Search Report under Section 17

## Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): G4A (AAP)

Int Cl (Ed.7): G06F 1/00

Other: ONLINE: WPI, EPODOC, JAPIO

## Documents considered to be relevant:

| Category | Identity of document and relevant passage | Relevant to claims |
|---|---|---|
| X | GB 2346239 A IBM see whole document | 1, 12-16, 21 & 22 at least |
| X | GB 2331821 A NORTHERN TELECOM see claim 9 | 1,12-16,21 & 22 at least |
| X | EP 1085395 A PHONE COM INC see whole document | 1, 12-16, 21 & 22 at least |
| X | WO 00/43875 A SUN MICROSYSTEMS see claims | 1,12-16, 21 & 22 at least |
| X | Derwent Abstract 2000-024385 & DE 19816541 A ORGA | 1, 12-16, 21 & 22 |
| X | Derwent Abstract 1988-127391 & DE 3736190 A HITACHI | 1,12-16 21 & 22 |

| | | | |
|---|---|---|---|
| X | Document indicating lack of novelty or inventive step | A | Document indicating technological background and/or state of the art. |
| Y | Document indicating lack of inventive step if combined with one or more other documents of same category. | P | Document published on or after the declared priority date but before the filing date of this invention. |
| & | Member of the same patent family | E | Patent document published on or after, but with priority date earlier than, the filing date of this application. |