(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 818 761 A1

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
14.01.1998 Bulletin 1998/03

(51) Int. Cl.^{6}: **G07F 7/10**

(21) Application number: **96202832.0**

(22) Date of filing: **11.10.1996**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **12.07.1996 EP 96201967**

(71) Applicant:
Koninklijke PTT Nederland N.V.
2509 CH Den Haag (NL)

(72) Inventors:
- **Drupsteen, Michel Marco Paul**
  1816 NA Alkmaar (NL)
- **Feiken, Albertus**
  1186 TD Amstelveen (NL)

(74) Representative:
de Bruijn, Leendert C. et al
Nederlandsch Octrooibureau
P.O. Box 29720
2502 LS Den Haag (NL)

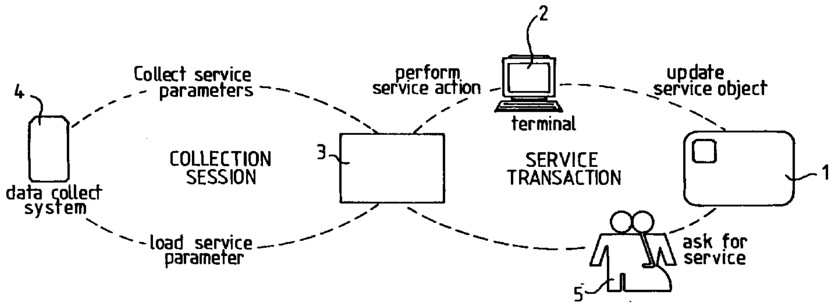
(54) Integrated circuit card, secure application module, system comprising a secure application module and a terminal and a method for controlling service actions to be carried out by the secure application module on the integrated circuit card

(57) An integrated circuit card (=ICC) with file oriented memory structure, a secure application module (=SAM) with file oriented memory structure, a system comprising a SAM and a terminal and a method for controlling service actions in a multiple service application mechanism to be carried out by the terminal on the ICC including the following steps:

a. establishing whether said terminal is allowed to carry out said service action on said integrated service card by using at least one key stored both on said ICC and on said SAM and by checking on said SAM predetermined access rights stored on said SAM, and

b. carrying out said service action on said integrated service card.

Fig-1



Description

Background of the Invention

The present invention relates to an integrated circuit card provided with memory means storing service data relating to at least one service.

Such integrated circuit cards are now widely used. The present invention is intended to be used in multiple application authorization mechanisms. Examples of multiple application authorization mechanisms have been described before in, e.g., US-A-5,473,690, WO-A-92/06451, EP-A-0,640,945, EP-A-0,644,513, WO-A-87/07060, EP-A-0,262,025 and EP-A-0,661,675.

These known multiple application authorization mechanisms share a direct memory access structure in which no directories and files are used. A common feature of the known mechanisms is to use a secret code to check whether a secure application module is allowed to access an application, indicated by a unique identifier, on the integrated circuit card. Whenever a secure application module wishes access to this application this secret code needs to be reproduced.

Since these known mechanisms do not use directories or file structures the presence of access tables on the integrated circuit cards is required. These access tables comprise several entries constituted of the secret code for a predetermined application, the related memory locations on the integrated circuit card used for this application and the related access rights associated with this application like read/write rights, PIN, etc.. Mostly, a secret key is required to avoid disclosure of the secret code.

A disadvantage of the known mechanisms referred to above is that the access tables on the integrated circuit card occupy memory locations. Since nowadays an integrated circuit card only has about 8 kilobits memory space available this is a serious disadvantage.

Summary of the invention

The object of the present invention is to provide an integrated circuit card having its memory organized in a directory and file structure and in which memory space is saved by reducing the overhead data on the integrated circuit card per application.

To obtain this object the present invention provides an integrated circuit card as defined in the preamble of claim 1 which is characterized in that at least part of the memory means comprises service data in file structures within one directory comprising a first file and a second file, service data being grouped together in service slots, any service slot being divided into a profile part and a data part, any profile part having a slot number, and being stored in the first file and comprising a unique application identifier and any data part being stored in the second file and comprising data relating to the service, the memory means storing at least one key to protect write access to the first and second files.

By means of a memory on the integrated circuit card structured as defined above it is enough to store only one or two keys on the card which are common to several service applications. Thus, less overhead data relating to any of the service applications on the card is required and more service applications can be supported by the integrated circuit card.

In one embodiment, at least one profile part also comprises data relating to an expiry date of the service slot concerned. Such data relating to an expiry date may be checked by the secure application module which is communicating with the integrated circuit card. If it is established that the date has already expired the service slot concerned is available to any other new service application. Thus, no complicated arrangements have to be provided for between the hardware provider, the provider of the software and the party who is providing the service to the user of the integrated circuit card. The availability of a service slot of which the expiry date has expired can be checked automatically.

When there are different application providers of the software related to several services the service slots are preferably structured such that they comprise their own profile part and their own data part, the profile parts being implemented as records of the first file and the data parts being implemented as records of the second file, the memory means storing a further key to protect access to the first file. In such a case these service slots may be called "generic service slots".

However, when there is only one application provider of the software for several services, preferably the implemented service slots share one common profile part but any service slot comprises its own data part, the common profile part being implemented as one record of the first file and the data parts being implemented as separate records of the second file. These service slots may be called "dedicated service slots". In such a case, the first file only comprises one record, thus saving required memory space for the profile part data.

The directory of the integrated circuit card may be extended by a third file such that at least one service slot comprises an additional data part in the third file for storing additional data. Some service applications need a lot of additional data which may be stored in such an additional data part.

The present invention also relates to a secure application module equipped to communicate with an integrated circuit card according to any of the claims 1 through 7, provided with memory means storing service data relating to at least one service, characterised in that at least part of the memory means comprises service data in file structures within one directory, the directory comprising at least one file, the at least one file storing service data relating to one single service grouped together into.

- application/service definition data comprising a unique service identifier and data indicating a service type;
- at least two application counters for administrating the number of allocations and for generating a unique record transaction number;
- a service sequence counter for generating a unique object number and administrating the number of created service objects;
- a service float for administrating the number of either issued or received value units and
- data relating to access rights defining service actions allowed to be performed by predefined terminals,

  and in that the memory means comprises at least a first key and a second key for protecting any data communication with an integrated circuit card.

The service definition data and the keys on the secure application module are used for the management of the service application, which was controlled by access tables on the integrated circuit card in the mechanisms according to the prior art. Thus, management control data is now stored on the secure application module instead of on the integrated circuit card. However, this is no serious disadvantage since the available memory space on the secure application module is less critical than on the integrated circuit card itself. Moreover, such a construction has several advantages.

First of all, the management of the applications may be realized more easily since the issuer of the integrated circuit cards is always able to establish a direct link between the secure application module and a central data collect system which is more difficult between the integrated circuit cards and the central data collect system.

Secondly, different service acceptants, i.e. parties which establish direct links between integrated circuit cards and the secure application module to facilitate a service, may be authorized to different access rights. The secure application module can easily check which service actions are allowed to a service acceptant to be carried out on an integrated circuit card, e.g. adding loyalty points, subtracting loyalty points, or only displaying a total number of loyalty points present on the integrated circuit card.

By using records within the file structure of the service slot mechanism, the use of access tables on the integrated circuit cards is avoided. The secure application module will always only allow use of a specified record number that has been read in a secured way.

The present invention also relates to a system comprising a secure application module according to the invention and at least one terminal coupled to the secure application module, the terminal being equipped to communicate with the secure application module and with at least one integrated circuit according to the invention in order to control a service carried out on the at least one integrated circuit card.

Moreover, the present invention relates to a method for controlling a service action to be carried out by a terminal on an integrated circuit card according to any of the claims 1 through 7, the terminal being coupled to both a secure application module according to any of the claims 8 or 9 and to the integrated circuit card, including the following steps:

a. establishing whether the terminal is allowed to carry out the service action on the integrated service card by using at least one code and at least one secret key, both the at least one code and the at least one key being stored on both the integrated circuit card and the secure application module and by checking predetermined access rights, and
b. carrying out the service action on the integrated service card;
c. checking step b. on the terminal,
<u>characterised in that</u>:
the checking predetermined access rights in step a is carried out on the secure application module using the data relating to access rights stored on the secure application module and the at least one code.

Thus, in the method according to the invention more steps of the application mechanism are carried out on the secure application module than in methods according to the prior art. This saves memory space on the integrated circuit cards and simplifies management of multiple applications on integrated circuit cards.

Since the available memory space in secure application modules is less critical than on integrated circuit cards the number of possible access rights may be rather large. Access rights may be defined in more ways than only read or write. In accordance with the invention access rights may relate to creating, erasing, increasing, decreasing, validating, marking, and verifying service slots on the integrated circuit card and to modifying additional data parts if present. These are only examples: other types of access rights may be implemented on the secure application module.

In an alternative embodiment the method defined above is characterised by the following step prior to the step of checking predetermined access rights in step a: reading out service data from the service slot and storing in the secure application module a predetermined data part of the data which has to remain unchanged; and by the step of carrying out step b. without changing the predetermined part of the data on the integrated circuit card.

<u>Brief description of the Drawings</u>

The present invention will be explained below with reference to some drawings. These drawings are only meant to illustrate the present invention and not to limit its scope.

Figure 1 shows processes to support integrated circuit card services like an "electronic purse" facility;
figure 2 shows a schematic flow diagram of method steps carried out in an integrated circuit card, a terminal, and a secure application module, respectively, to support such a service in accordance with the prior art;
figure 3 shows a structure for several secure application module facilities;
figure 4 shows a service application environment on an integrated circuit card which may be used for services of the same type, originating from different application providers (generic service slots);
figure 5 shows a structure of an alternative service application environment for services of different types, originating from one application provider only (dedicated service slots);
figure 6 shows a structure of a service application environment of a secure application module in accordance with the present invention;
figure 7 shows a secure application module and its relation between several parties involved for providing and facilitating a service;
figure 8a shows a schematic flow diagram of method steps carried out on an integrated circuit card, a terminal and a secure application module, respectively, for carrying out one of the following service actions: creating, erasing, or modifying a service object;
figure 8b shows an amended flow diagram of the one shown in figure 8a, which illustrates steps for carrying out one of the following service actions: increasing, decreasing, validating, and marking an existing service object;
figure 9 shows an example of the exact structure of a service slot.

Detailed description of the embodiments

As shown in figure 1, in accordance with the state of the art, an integrated circuit card 1 may be loaded with one or more services, like an "electronic purse" facility. A user 5 may insert the integrated circuit card 1 into suitable connection means (not shown) of a terminal 2. The terminal 2 is coupled to a secure application module 3. A data collect system 4 is coupled to the secure application module 3 via the terminal interface. The connections between the terminal 2, the secure application module 3, the data collect system 4, and the integrated circuit card 1, respectively, may be either by conventional wires, optical fibres or by any wireless transmission technique.

The terminal 2 operates as an interface between the integrated circuit card 1 and the secure application module 3.

In order to facilitate the description, several definitions used will be stated firstly.

Service type: the type of card-related service to be used by a card holder 5. Examples of service types are the electronic purse, loyalty counters, loyalty coupons, identifiers, subscriptions, tickets, e.g. to be used for parking, public transport, cinema, concerts, etc..

Service application: the set of necessary service objects to be stored on the integrated circuit card 1 and on the secure application module 3, to be used for the exploitation of the service. Examples of service objects are: loyalty points, tickets, subscriptions, etc..

Service parameter: a service object that is necessary for the secure application module 3 in order to facilitate a service application, e.g., the application identifier, service identifier, service access rights, etc..

Service action: the (authorized) execution of one or more software routines which results in the modification, creation or elimination of the service object, for example, the creation or verification of a ticket or the increase or decrease of loyalty points on a loyalty coupon.

Service access rights: a defined authorization rule for the use of a certain service action by a predetermined terminal; some terminals may, for example, only have the right to read the number of loyalty points on a integrated circuit card 1, whereas others may have the authorization to modify this number of loyalty points.

Service object: the service related data structure that is securely stored on the integrated circuit card and which can be modified by a service (object) action (e.g. tickets, coupons, loyalty counters).

Hardware provider: the party which provides the integrated circuit card 1 to the card issuers and the secure application module 3 to the card acceptants. These integrated circuit cards 1 and secure application modules 3 will be provided with basic applications for the use of, for instance, the electronic purse. Part of the memory of the provided integrated circuit cards 1 and the secure application modules can be used for the storage of further applications to be determined by the card issuer/card acceptant.

Card issuer: the party which issues the integrated circuit card 1 to customers. This party determines the optional applications on the integrated circuit cards 1, usually after a legal agreement with the hardware provider.

Card acceptant: the party which buys the necessary secure application modules 3 from the hardware provider in order to offer several card-related services to the card holders 5. These secure application modules 3 must be linked to the terminal(s) 2 of the card acceptant. The card acceptant determines the optional applications on the secure application module 3, usually after a legal agreement with the hardware provider.

Application provider: the party which facilitates these card-related services, by means of storing service application modules on the integrated circuit card 1 and on the secure application modules 3. This party must also provide the necessary terminal software to be stored in the terminal(s) 2 of the card acceptant.

Service provider: the party which (financially) exploits the card-related service offered by a card acceptant and facilitated by an application provider.

Service acceptant: the party which establishes the direct link between the card holder 5 and a certain service via an on-line service host or via an off-line service terminal 2. This party performs the service actions on the stored service object, for which it is allowed to use.

Card holder 5: the customer who uses the integrated circuit card 1 for several services by means of establishing the necessary link between the integrated circuit card 1 and the terminal 2, e.g., by inserting the Chipper in a retailer's reader or by communicating via a Tele-Chipper®.

As shown in figure 1, the terminal 2 controls any service transaction after a customer 5 has connected his integrated circuit card 1 to the terminal 2. The terminal 2 performs any service action to be made and updates the service object on the integrated circuit card 1. At the same time, the terminal 2 performs the necessary actions on the secure application module 3.

The data collect system 4 collects service parameters from and loads service parameters on the secure application module 3 in a collection session.

The collection session as indicated in figure 1 is known to persons skilled in the art and is not explained in detail here.

As indicated above, several multiple application authorization mechanisms have been described before, like in US-A-5.473.690, WO-A-92/06451, EP-A-0.640.945, EP-A-0.644.513, WO-A-87/07060, and EP-A-0.262.025 and EP-A-0.661.675. These known multiple application authorization mechanisms share a direct memory access structure, i.e., without directories and files structures. A secret code C is used for accessing the application with an identifier I on the integrated circuit card 1. Whenever a secure application module 3 wishes to access this application it must be able to generate this secret code C. This secret code C may be encrypted when it is supplied to the integrated circuit card 1 to avoid its disclosure to the outside world. Alternatively, this code C may be processed with a message authentication code (MAC) in order to avoid any modification by the outside world. As a further alternative, this code C may be supplied directly. A control mechanism on the integrated circuit card 1 may count how many times a wrong code C is supplied.

A second feature of all these known mechanisms is the presence of an access table on the integrated circuit card 1. Mostly, such a table comprises a plurality of entries consisting of 1) the secret code C for a specific application, 2) related memory locations M on the integrated circuit card 1 used by that application (e.g. referring to zones, number of bytes, offsets, records, etc.) and 3) related access rights A applicable to this application (e.g. read/write rights, PIN, etc.). When either option 1 or option 2 is used a secret key Ks is required.

Figure 2 shows a schematic flow diagram broadly summarizing the mechanism according to the prior art when writing data D on a memory location M of the application related to the code C. Four phases can be distinguished: the initialization phase in which several parameters are stored in the integrated circuit card (ICC) 1 and the secure application module (SAM) 3, the application access phase in which the integrated circuit card 1 checks whether the secret code C as supplied is correct, the application request phase in which the request to write data D on the memory location M is made, and the request authorization execution phase in which the terminal is authorized to write data on memory location M given access rights A and code C. The use of random numbers RND is optional but is required to avoid so-called "replay attacks". A random number RND is used by the secure application module 3 to encrypt the code C when the secret code C is to be transferred from the secure application module 3 to the integrated circuit card 1. The integrated circuit card 1 is equipped to decode the encoded secret code C. Thus, the terminal 2 when transferring the encrypted secret code C from the secure application module 3 to the integrated circuit card 1 does not know the value of the secret code C and will not be able to carry out any further action on the integrated circuit card 1 without being authorized.

The flow diagram of figure 2 is separated into three parts relating to the integrated circuit card (ICC) 1, the terminal 2, and the secure application module (SAM) 3, respectively.

In step 201, the integrated circuit card 1 stores the following set of parameters for an application: an identifier I, a secret code C, a memory location M, and access rights A.

In step 202, the integrated circuit card 1 stores a secret key Ks.

In the initialization phase, in step 203, the secure application module 3 stores an application identifier I' and a secret code C'. In step 204, the secure application module stores the secret key Ks.

For the same application, it is required that $I = I'$ and $C = C'$.

In the application access phase the following steps are carried out.

In step 205 the integrated circuit card 1 generates a random number RND which is stored in step 206.

In step 207, the random number RND is transmitted to the terminal 2.

Step 208 indicates that the terminal 2 is waiting for receipt of the random number RND. As long as the random number RND has not been received the terminal 2 remains waiting.

As soon as the terminal 2 has received the random number RND it transfers the random number RND, in step 209, to the secure application module 3.

Step 210 indicates that in the application access

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**