(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 October 2017 (05.10.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/167408 A1

(51) International Patent Classification:
H04W 4/00 (2009.01) *H04W 12/06* (2009.01)
G06F 9/54 (2006.01)

(21) International Application Number:
PCT/EP2016/068451

(22) International Filing Date:
2 August 2016 (02.08.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201610186686.7 29 March 2016 (29.03.2016) CN

(71) Applicant: **GEMALTO SA** [FR/FR]; 6 rue de la Verrerie, 92190 Meudon (FR).

(72) Inventors: **SUN, Yanjing**; Gemalto SA, Intellectual Property Department, 6 rue de la Verrerie, 92190 Meudon (FR). **ZHOU, Yuexin**; Gemalto SA, Intellectual Property Department, 6 rue de la Verrerie, 92190 Meudon (FR). **KAN, Zheng**; Gemalto SA, Intellectual Property Department, 6 rue de la Verrerie, 92190 Meudon (FR).

(74) Agent: **LOTAUT, Yacine**; Gemalto SA, Intellectual Property Department, 6 rue de la Verrerie, 92190 Meudon (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH,

[Continued on next page]

(54) Title: METHOD AND DEVICE FOR COMMUNICATION BETWEEN A MOBILE DEVICE AND A SECURE ELEMENT

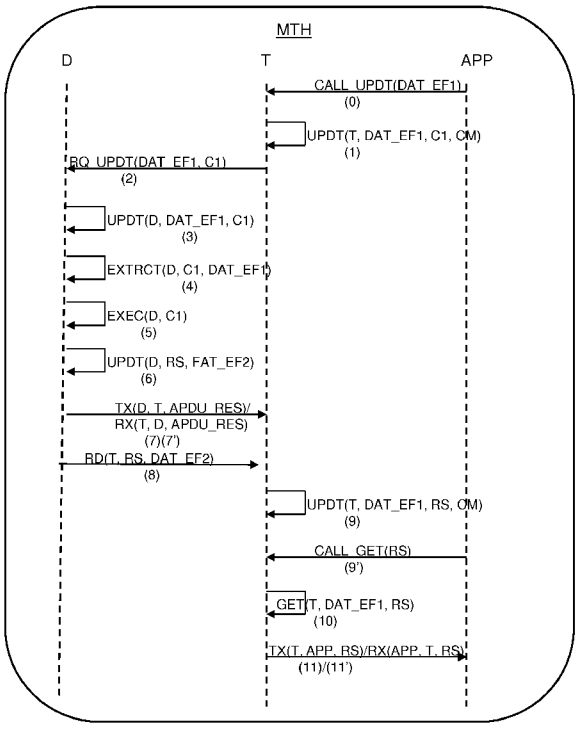

Fig. 1

(57) Abstract: The present invention relates to a method for communication between a secure element (D) of a mobile device (T) and said mobile device (T), said secure element (D) comprising a first data file (DAT_EF1) and said mobile device (T) comprising a corresponding first data file (DAT_EF1). The method comprises: updating said first data file (DAT_EF1) of said mobile device (T) with a command (C1); requesting by said mobile device (T) to said secure element (D) to update the corresponding first data file (DAT_EF1) with said command (C1); extracting and executing by said secure element (D) the command (C1) within the updated first data file (DAT_EF1) of said secure element (D); updating by said secure element (D) a second data file (DAT_EF2, DAT_F2) with a result (RS) of the execution; re-updating by said mobile device (T) the corresponding first data file (DAT_EF1) of said mobile device (T) with the result.

WO 2017/167408 A1

GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

METHOD AND DEVICE FOR COMMUNICATION BETWEEN A MOBILE DEVICE AND A SECURE ELEMENT

TECHNICAL FIELD

The present invention relates to a method for communication between a mobile device and a secure element of said mobile device. The invention also relates to an associated mobile device.

BACKGROUND OF THE INVENTION

A standard of communication such as the Open Mobile API standard (referred as OMAPI) of the SIMAlliance permits a mobile device to communicate with a secure element of said mobile device. Said secure element is for example a SIM ("Subscriber Identity Module") card or a USIM ("Universal Subscriber identity Module") card, said mobile device being a NFC ("Near Field Communication") mobile phone. The standard of communication permits in particular to send from said mobile phone some commands to said secure element and to receive by said mobile phone some responses from said secure element.

One problem of this prior art is that this standard of communication is complex to implement and is only dedicated to NFC mobile devices.

SUMMARY OF THE INVENTION

It is an object of the invention to provide a method for communication between a mobile device and a secure element of said mobile device which permits said mobile device to easily communicate with its secure element, and this for any type of mobile device, NFC or not.

To this end, there is provided a method for communication between a secure element of a mobile device and said mobile device, said secure element comprising at least a first data file and said mobile device comprising a corresponding first data file, wherein said method for communication comprises:

- updating by said mobile device said first data file of said mobile device with at least one command to be executed by said secure element;

- requesting by said mobile device to said secure element to update the corresponding first data file of said secure element with said at least one command;
- updating by said secure element the corresponding first data file of said secure element with said at least one command;
- extracting by said secure element the at least one command within the updated first data file of said secure element;
- executing by said secure element the at least one command;
- updating by said secure element a second data file with a result of the execution of said at least one command;
- reading by said mobile device from said secure element the result from said second data file;
- re-updating by said mobile device the corresponding first data file of said mobile device with the result read;
- getting by said mobile device the result of the execution of said at least one command from said re-updated first data file.

Hence, as will be described in detailed, one uses data files which are common to the mobile device and to the secure element to send a command from said mobile device to the secure element and to receive by said mobile device a response of the execution of said command from said secure element. It doesn't need any complex standard of communication. It may be applied to any type of mobile device. Moreover, the invention permits a mobile device to know when an update in a data file of said secure element takes place, and to update accordingly a data file in its own memory, which corresponds to the secure element's updated data file.

According to non-limitative embodiments of the invention, the method for communication in accordance with the invention further comprises the following characteristics.

In a non-limitative embodiment, the command to be executed by said secure element is an APDU command.

In a non-limitative embodiment, the first data file is an elementary file.

In a non-limitative embodiment, the first data file and the second data file are:

- an ADN file; or
- an SMS file; or
- an ICCID file; or
- an MSISDN file; or
- an IMSI file.

In a non-limitative embodiment, the second data file is a data file which is smaller than the first data file.

In a non-limitative embodiment, said method for communication further comprises switching by said secure element of the file identifications between an elementary file of said secure element and said smaller data file.

In a non-limitative embodiment, said method for communication further comprises:

- switching back by said secure element of the file identifications between an elementary file of said secure element and said smaller data file;
- reading by said mobile device from said secure element some data of said elementary file;
- updating by said mobile device the first data file of said mobile device with the data read.

In a non-limitative embodiment, said method for communication further comprises:

- receiving by said mobile device a request from a user for reading some data of said first data file;
- getting by said mobile device the requested data;
- displaying by said mobile device said requested data.

In a non-limitative embodiment, said secure element is a SIM card, USIM card, an eSE, a micro-SD, an UICC, or an embedded UICC.

In a non-limitative embodiment, said mobile device is a mobile phone.

In a non-limitative embodiment, said mobile device is an Android™ device.

In a non-limitative embodiment, in order to indicate the mobile device to read some data in a second data file of said secure element, said method communication further comprises sending by said secure element to said mobile device a proactive refresh command comprising a file identification of said second data file to be read.

In a non-limitative embodiment, said mobile device comprises an operating system which is adapted to perform the steps performed by said mobile device.

In a non-limitative embodiment, said mobile device further comprises an application and said method for communication further comprises:

- a launch by said application of the update by said mobile device of said first data file of said mobile device with at least one command;
- a launch by said application of the getting by said mobile device of the result of the execution of said at least one command.

In addition, there is provided a mobile device for communicating with a secure element of said mobile device, said secure element comprising at least a first data file and said mobile device comprising a corresponding first data file, wherein said mobile device is adapted to:

- update said first data file of said mobile device with at least one command to be executed by said secure element;
- request to said secure element to update the corresponding first data file of said secure element with said at least one command;
- update by said secure element the corresponding first data file of said secure element with said at least one command;
- extract by said secure element the at least one command within the updated first data file of said secure element;
- execute by said secure element the at least one command;

- update by said secure element a second data file with a result of the execution of said at least one command;
- read from said secure element the result from said second data file;
- re-update the corresponding first data file of said mobile device with the result read;
- get the result of the execution of said at least one command from said re-updated first data file.

BRIEF DESCRIPTION OF THE FIGURES

Some embodiments of methods and/or apparatus in accordance with embodiments of the present invention are now described, by way of example only, and with reference to the accompanying drawings, in which:

- Fig. 1 illustrates a schematic organization chart of a method for communication according to a first non-limitative embodiment of the invention;
- Fig. 2 illustrates a schematic organization chart of a method for communication according to a second non-limitative embodiment of the invention;
- Fig. 3 illustrates some further steps of the method for communication of Fig. 6;
- Fig. 4 illustrates a mobile device which is adapted to carry out the method for communication of Fig. 1 to 3.

DESCRIPTION OF EMBODIMENTS OF THE INVENTION

In the following description, well-known functions or constructions by the man skilled in the art are not described in detail since they would obscure the invention in unnecessary detail.

The present invention relates to a method for communication MTH between a mobile device T and a secure element D of said mobile device T.

The mobile device T illustrated in Fig. 4 comprises :

- the secure element D;
- an operating system OS; and

- an application APP.

The operating system OS is adapted to communicate with the secure element D and with the application APP.

It is to be noted that an application refers to a set of one or more programs designed to carry out a set of operations sequences to perform specific tasks.

In a non-limitative embodiment, the mobile device T is a mobile phone.

In a non-limitative embodiment, the mobile device T is an Android™ device.

In a non-limitative embodiment, the mobile device T is a NFC ("Near Filed Communication") mobile device T or not.

The mobile device T comprises :

- a cache memory CM ;
- a plurality of data files, which comprises some elementary files, referred as EF files. Said EF files are stored in said cache memory CM.

These EF files being well-known by the man skilled in the art, there are not described here.

In non-limitative examples, said EF files are:

- ICCID file ("Integrated Circuit Card ID") referred as ICCID_EF;
- IMSI file ("International Mobile Subscriber Identity") referred as IMSI_EF;
- MSISDN file ("Mobile Station International Subscriber Directory Number ») referred as MSISDN_EF;
- ADN file ("Abbreviated Dialing Number") referred as ADN_EF; and
- SMS file ("Short Message Service") referred as SMS_EF.

The mobile device T comprises at least one first data file DAT_EF1. Said first data file DAT_EF1 is in a non-limitative embodiment an EF file. As will be described hereinafter, said first data file DAT_EF1 will be used to receive a command C1 from said application APP or a result RS of the

execution of said command C1 from said secure element D.

A secure element D is a secured component which may perform cryptographic functionalities and is adapted to store a secret data.

In a non-limitative embodiment, the secure element D is a smart card. In non-limitative examples, the smart card is a SIM card or an USIM card.

In other non-limitative embodiments, the secure element D is an eSE (embedded secure element), a micro-SD, an UICC.

In the non-limitative embodiment of the secure element D which is a smart card, communication is performed with the operating system OS of the mobile device T by means of APDU (Application Protocol Data Unit).

Hence, in a non-limitative embodiment, said command C1 is an APDU command and said response RS is an APDU response. Of course, other formats different from an APDU command/response (recognized by the secure element D and the application APP) may be used.

In a non-limitative embodiment, the secure element D comprises a plurality of files, which comprises also some elementary files EF.

Some of these EF files are common to the ones of said mobile device T.

In non-limitative examples, the EF files in common are:

- ICCID file (“Integrated Circuit Card ID”) referred as ICCID_EF;
- IMSI file (“International Mobile Subscriber Identity”) referred as IMSI_EF;
- MSISDN file (“Mobile Station International Subscriber Directory Number ») referred as MSISDN_EF;
- ADN file (“Abbreviated Dialing Number”) referred as ADN_EF; and
- SMS file (“Short Message Service”) referred as SMS_EF.

The secure element D comprises at least one first data file DAT_EF1 which corresponds to the first data file of the mobile device T. Said first data file DAT_EF1 is in a non-limitative embodiment an EF file. As will be described hereinafter, said first data file DAT_EF1 will be used to receive the command C1 from said mobile device T.

The secure element D comprises at least one second data file DAT_EF2, DAT_F2. As will be described hereinafter, said second data file DAT_EF2, DAT_F2 will be used to save the result RS of the execution of said command C1.

In a non-limitative embodiment, the secure element D further comprises a secret password PIN1 also referred as stored PIN1. In a non-limitative example, said secret password is a short secret password, such as a PIN (Password Identification Number"). In another non-limitative embodiment, the secret password is a passphrase.

The short secret password will be taken in the following as a non-limitative example.

As will be described hereinafter, the method for communication MTH between the mobile device T and the secure element D will permit data exchange, such as a command C1 and a response RS, between the secure element D and the application APP, via the operating system OS.

Moreover, the method for communication MTH permits to transfer some data from said secure element D to said application APP on the mobile device T by updating an element file EF. In order for said mobile device T to know that an element file EF of said secure element D has been updated, said secure element D will send a proactive refresh command APDU_RES to said mobile device T, that is related to the updated element file EF. Then said mobile device T will read the element file EF and updates the image of said element file EF in the cache memory.

In a non-limitative embodiment, said proactive refresh command ADPU_RES is a proactive REFRESH ADPU command with a mode "file change notification". Of course, other formats different from an APDU command may be used for such proactive refresh command APDU_RES.

This mode advises the mobile device T of the identity of the elementary file DAT_EF2 that has been changed (in structure and/or contents) in the secure element D. This information may be used by the

mobile device T if there is an image of said elementary file (e.g. the ADN file) in the mobile device's memory, to determine whether it needs to update this image, DAT_EF1 in this case.

It is to be noted that a proactive command is used by the secure element D to instruct the mobile device T to do different tasks. In the case of the proactive refresh command, the secure element D notifies the mobile device T to read one of its elementary file DAT_EF2, DAT_F2 in order to update its corresponding elementary file DAT_EF1.

In a non-limitative example, the application APP is an application which permits an authentication of a user U of the mobile device D to a remote server (not illustrated) via said mobile device T. Thanks to this application APP, the user U enters a short secret password referred as PIN2 on the mobile device T. Said PIN2 is then verified by the secure element D. The result of the verification is then sent to the remote server.

In this case, the data exchanged between the application APP and the secure element D will be:

- a verify short secret password command C1, which will be transferred from the application APP to the USIM card D, via the operating system OS of the mobile device T;
- a result RS of the verification of said short secret password, which will be transferred from the USIM card D to the application APP, via the operating system OS of the mobile device T.

This non-limitative example of application APP will be taken in the following description. Furthermore, in a non-limitative example, the first data file DAT_EF1 of said mobile device T is an ADN file.

The method for communication MTH between the mobile device T and the secure element D is illustrated in Fig. 1 according to a first non-limitative embodiment, and in Fig. 2 and 3 according to a second non-limitative embodiment.

The USIM card will be taken in the following as a non-limitative example.

These non-limitative embodiments are described hereinafter.

- First embodiment

When the application APP for authenticating the user U to a remote server is open and launched (by the user of the mobile device D for example), said application APP launches (**step 0** illustrated in Fig. 1 CALL_UPDT(DAT_EF1)) the update of a first data file DAT_EF1 of said mobile device T with the command C1 to be executed.

Hence, **in step 1)** illustrated in Fig. 1 UPDT(T, DAT_EF1, C1, CM), said mobile device T updates its first data file DAT_EF1 with at least said one command C1 to be executed by said USIM card D.

In the non-limitative given example, the ADN file in the cache memory CM of said mobile device T is therefore updated with the verify short secret password command C1, said command C1 comprising the PIN2 entered by the user U of the mobile phone T.

In step 2) illustrated in Fig. 1 RQ_UPDT(DAT_EF1, C1), said mobile device T requests said USIM card D to update its corresponding first data file DAT_EF1 with said at least one command C1.

Hence, it request the USIM card D to update its own ADN file with the verify short secret password command C1.

In step 3) illustrated in Fig. 1 UPDT(D, DAT_EF1, C1), said USIM card D updates its corresponding first data file DAT_EF1 with said at least one command C1.

Hence, the ADN file of said USIM card D is updated with the verify short secret password command C1, said verify short secret password command comprising the PIN2 entered by the user.

In step 4) illustrated in Fig. 1 EXTRCT(D, C1, DAT_EF1), said USIM card D extracts the at least one command C1 within the updated first data file DAT_EF1.

In order to read the verify short secret password command C1 and therefore here the PIN2, the USIM card D extracts it from its ADN file.

In step 5) illustrated in Fig. 1 EXEC(D, C1), said USIM card D executes the at least one command C1.

In the non-limitative given example, the USIM card D executes the verify short secret password command: it checks if the short secret password PIN2 entered is equal to its own stored PIN1.

If it is the case, the USIM card D generates a result RS which is “PIN correct”, in the other case, the results RS is “PIN wrong”. In a non-limitative example, the result RS equal to 1 when the short secret password PIN2 is correct, and equal to 0 when the short secret password PIN2 is wrong.

In the given example, PIN2 is equal to PIN1, and the result RS is = 1.

In step 6) illustrated in Fig. 1 UPDT(D, RS, DAT_EF2), said USIM card D updates a second data file DAT_EF2 with said result RS of the execution of said at least one command C1.

In a non-limitative embodiment, said second data file DAT_EF2 is an elementary file EF.

In a non-limitative embodiment, said second data file DAT_EF2 may be the same as the first data file DAT_EF1 which has been updated with the command C1, here the ADN file, or may be another EF file, for example the SMS file.

In other non-limitative examples, these other EF files may be used as a second data file DAT_EF2 to store the result RS:

- ICCID file ;
- IMSI file ;
- MSISDN file.

Said mobile device T will then be able to read said result RS from said second data file DAT_EF2.

It is to be noted that in order to make the mobile device T read some data from said second data file DAT_EF2 of said USIM card D, **in step 7)** illustrated in Fig. 1 TX(D, T, APDU_RES), the USIM card D sends to said mobile device T a proactive refresh command ADPU_RES comprising the file identification ID2 of said second data file DAT_EF2 to be read.

In step 7') illustrated in Fig. 1 RX(T, D, APDU_RES), said mobile device T receives said proactive refresh command APDU_RES.

In step 8) illustrated in Fig. 1 RD(T, RS, DAT_EF2), said mobile device T reads from said USIM card D the result RS from said second data file DAT_EF2.

Hence, the mobile device T reads, in the ADN file of the USM card D, the result RS which is equal to 1.

Therefore, the mobile phone T is able to retrieve the data which has been updated in the USIM card (in particular in the ADN file in the given example), that is to say, here in non-limitative given example, the result RS.

In step 9) illustrated in Fig. 1 UPDT(T, DAT_EF1, RS, CM), said mobile device T re-updates its corresponding first data file DAT_EF1 with said result read RS.

Hence it updates its own ADN file in the cache memory CM with the result RS equal to 1.

In step 10) illustrated in Fig. 1 GT(T, DAT_EF1, RS), said mobile device T gets the result RS of the execution of said at least one command C1 from said re-updated first data file DAT_EF1.

Hence, the result RS that is to say the value 1 in the non-limitative given example, is read from the ADN file in the cache memory CM.

It is to be noted that the application APP is adapted to launch (**step 9'** illustrated in Fig. 1 CALL_GT(RS) the getting by the mobile device T of the result RS of the execution of said at least one command C1 from said re-updated first data file DAT_EF1.

In step 11) illustrated in Fig. 1 TX(T, APP, RS), said mobile device T sends the result RS to the application APP which receives it **in step 11')** illustrated in Fig. 1 (RX(APP, T, RS).

Hence, the result "PIN2 correct" is sent and received.

It is to be noted that all the steps above-described performed by the mobile device T, are performed by the operating system OS of said mobile device T.

Hence, when receiving this result RS which indicates that the short secret password PIN2 entered by the user U is correct, the application APP is able to sends a response to the remote server to acknowledge that the short secret password PIN2 is correct, in this case, and to display a message related to the result RS of the command executed for the user.

The application APP is thereafter closed.

Hence, thanks to this first embodiment, a command C1 is transmitted via data files which are common to the mobile device T and the secure element D, and which are here standard EF files. The result RS is transmitted via a data file which already exists in the secure element D, which is here a standard EF file.

It is to be noted that the first data file DAT_EF1 and the second data file DAT_EF2 which are standard EF files usually comprise a huge size (for example 250 records for an ADN file).

Hence, after receiving the proactive refresh command ADPU_RES, the reading of an EF file in the USIM card D and the updating of its cache memory CM will take a long time for the mobile device T to perform.

So, if an EF file such as ADN file or SMS file is used for the data exchange, the application APP may have to wait a long time for getting the data updated in the USIM card D, here the result RS. In a non-limitative embodiment, the application APP will have to wait up to 23 seconds, which is too long.

Hence, as will be described in the second non-limitative embodiment illustrated in Fig. 2 and 3, a data file, called ghost file, may be used as a second data file for exchanging data between the USIM card D and the application APP. Said ghost data file referred as DAT_F2 comprises a structure which is smaller than a standard EF file. It comprises less records than the first data file DAT_EF1. Hence, when the mobile device T will read said ghost data file DAT_F2, it will be quicker, because its file size is smaller.

- Second embodiment

The five first **steps 1 to 5** above-described for the first embodiment are the same for said second embodiment.

As explained above, the second data file which will be updated will be the ghost data file DAT_F2.

Hence, instead of the second data file referred as DAT_EF2 (here, the standard ADN file) corresponding to the first data file DAT_EF1 of the mobile device T, the USIM card D selects the ghost data file DAT_F2 as the second data file to be updated with the result RS, and update it as described in the **step 6)** in the first embodiment (step 6 illustrated in Fig. 2 UPDT(D, RS, DAT_F2)) .

It is to be noted a second data file which is either a standard EF file (in the first embodiment) or the ghost data file DAT_F2 (in these second embodiment) comprises a file identification, here ID2 for the standard EF file DAT_EF2, and ID2' for the ghost data file DAT_F2.

In step 7) illustrated in Fig. 2 SWP(D, ID2, ID2', DAT_EF2, DAT_F2) the USIM card D switch (also called swap) the file identifications ID2, ID2' between the EF file DAT_EF2 and said second ghost data file DAT_F2.

Hence, in the non-limitative given example, the file identification ID2 of the standard ADN file will be associated with the ghost data file DAT_F2, and the file identification ID2' of the ghost data file DAT_F2 will be associated to the ADN file.

It permits the mobile device T to read said ghost data file DAT_F2 instead of the standard ADN file.

Then, in order to make the mobile device T read some data from said ghost data file DAT_F2 of said USIM card D, **in step 8)** illustrated in Fig. 2 TX(D, T, APDU_RES), the USIM card D send a proactive refresh command APDU_RES. Said proactive refresh command APDU_RES comprises the file identification ID2 of said ADN file.

In step 8'), said mobile device T receives said proactive refresh command APDU_RES as illustrated in Fig. 2 RX(T, D, APDU_RES).

Consequently, **in step 9)**, illustrated in Fig. 2 RD(T, RS, DAT_F2), the mobile device T will read the result RS from said ghost data file DAT_F2 thinking that it reads a standard EF file (as it is described **in step 8)** of the first embodiment).

As, in the non-limitative given example, the mobile device T only recognizes the file identification ID2 of the standard ADN file, it thinks that it reads its content while reading the content of the ghost data file DAT_F2. This is the reason why this smaller data file DAT_F2 is called ghost.

As the file size of the ghost data file DAT_F2 is smaller than the one of the standard ADN file, the reading is faster.

The **steps 10, 10', 11, 12 and 12'** are respectively the same as the **steps 9, 9', 10, 11 and 11'** described in the first embodiment.

It is to be noted that all the steps above-described performed by the mobile device T, are performed by the operating system OS of said mobile device T.

Hence, as in the first embodiment, when receiving this result RS which indicates that the short secret password PIN2 entered by the user U is correct, the application APP is able to sends a response to the remote server to acknowledge that the short secret password PIN2 is correct, in this case,

and to display a message related to the result RS of the command executed for the user.

The application APP is thereafter closed.

Hence, thanks to this second embodiment, a command C1 is transmitted via data files which are common to the mobile device T and the secure element D, and which are here standard EF files. The result RS is transmitted via a data file which is smaller than a standard EF file.

Hence, thanks to this method for communication (first and second non-limitative embodiments), some data (here the command C1 and the result RS) may be transferred from the application APP to the secure element D of said mobile phone, and vice versa, without need of any dedicated or standard protocol communication between an APP and the secure element D. Only the protocol communication already used between the operating system OS of the mobile phone and its secure element D is used.

It is to be noted that if the user U of the mobile device T wants to get some data from the second data file, such as some abbreviated dialed numbers in the ADN file for example, the previously file identification ID2 should be associated to the ADN file, which is not the case as it has been associated to the ghost data file DAT_F2, and the corresponding first data file DAT_EF1 of said mobile device T should contain the content of said ADN file, that is to say the abbreviated dialed numbers.

Therefore, after the application APP is closed, **in step 13)** illustrated in Fig. 3 RQ_SWPB (T, D, ID2, ID2', DAT_EF2, DAT_F2), the mobile device T requests the USIM card D to switch back the file identifications ID2, ID2'. In a non-limitative embodiment, for said request, the mobile device T sends an APDU status command.

In step 14), illustrated in Fig. 3 SWPB(D, ID2, ID2', DAT_EF2, DAT_F2), the USIM card D switch back the file identifications ID2, ID2' between the elementary file DAT_EF2 of said USIM card D corresponding to

the first data file DAT_EF1 of said mobile device T and said second ghost data file DAT_F2.

The file identification ID2 is therefore again associated to the standard ADN file and the file identification ID2' to the ghost data file DAT_F2.

In step 15) illustrated in Fig. 3 TX(D, T, APDU_RES), the USIM card D sends to the mobile device D a proactive refresh command APDU_RES with the file identification ID2 of the elementary file DAT_EF2 to be read.

Hence, in the non-limitative given example, the proactive refresh command APDU_RES comprises the file identification ID2 of the standard ADN file.

Said mobile device T receives said proactive refresh command APDU-RES **in step 15')** illustrated RX(T, D, APDU_RES).

The normal ADN file will be read by the mobile device T instead of the ghost data file DAT_F2.

In step 16) illustrated in Fig. 3 RD(T, DAT2, DAT_F2), the mobile device T reads the data DAT2 from said elementary file DAT_EF2 of said USIM card D.

In the non-limitative given example, it reads the records of the ADN file, which are the abbreviated dialed numbers which are recorded in the USIM card D.

In step 17) illustrated in Fig. 3 UPDT(T, DAT_EF1, DAT2, CM), the mobile device T updates with the data read DAT2 the corresponding first data file DAT_EF1 in the cache memory CM.

Hence, the previously data which have been recorded in the cache memory CM, that is to say the data of the ghost file DAT_F2 and in particular the result RS, are erased by the data of said elementary file, here by the ADN records.

Hence, later, when **in step 18)** illustrated in Fig. 3 RX(T, U, RQ,

DAT1, DAT_EF1), the mobile device T receives a request RQ from a user U for reading some data DAT1, for example a selected abbreviated dialed number, of said first data file DAT_EF1, here of the ADN file in the cache memory CM, **in step 19)** illustrated in Fig. 3 GT(T, DAT_EF1, DAT1), the mobile device T gets the requesting data DAT1 from said first data file DAT_EF1, here, the requested abbreviated dialed number, and **in step 20)** illustrated in Fig. 3 DISP(T, DAT1, DAT_EF1), the mobile device T displays said requested data DAT1 to said user, for example on a screen.

Hence, the mobile device T is adapted to carry out a method MTH for performing a communication with its secure element D. The mobile device T is illustrated in Fig. 4. It comprises said secure element D, the operating system OS and the application APP.

As above-described, the mobile device T comprises at least one first data file DAT_EF1 in a cache memory CM and the secure element D comprises a corresponding first data file DAT_EF1 in its own memory. Said memory is for example a non-volatile memory such as an EEPROM. It is to be noted that the same reference is used for the first data file DAT_EF1 in the mobile device T and the one in the secure element D, although they are different data files.

The operating system OS of said mobile device T is adapted to:

- update said first data file DAT_EF1 with at least one command C1 to be executed by said secure element D (function illustrated in Fig. 4 UPDT(T, DAT_EF1, C1, CM));
- request to said secure element D to update the corresponding first data file DAT_EF1 of said secure element D with said at least one command C1 (function illustrated in Fig. 4 RQ_APDT(DAT_EF1, C1));
- read from said secure element D the result RS from said second data file DAT_EF2, DAT_F2 (function illustrated in Fig. 4 RD(T, RS, DAT_EF2));

- re-update the corresponding first data file DAT_EF1 of said mobile device T with the result read RS (function illustrated in Fig. 4 UPDT(T, DAT_EF1, RS, CM));
- get the result RS of the execution of said at least one command C1 from said re-updated first data file DAT_EF1 (function illustrated in Fig. 4 GT(T, DAT_EF1, RS));
- transmit to said application APP the results RS of the execution of aid command C1 ((function illustrated in Fig. 4 TX(T, APP, RS)).

The secure element D of said mobile device T is adapted to:

- update the corresponding first data file DAT_EF1 of said secure element D with said at least one command C1 (function illustrated in Fig. 4 UPDT(D, DAT_EF1, C1);
- extract the at least one command C1 within the updated first data file DAT_EF1 of said secure element D (function illustrated in Fig. 4 EXTRCT(D, C1, DAT_EF1));
- execute the at least one command C1 (function illustrated in Fig. 4 EXEC(D, C1));
- update a second data file DAT_EF2, DAT_F2 with a result RS of the execution of said at least one command ADPU_C1 (function illustrated in Fig. 4 UPDT(D, RS, DAT_EF2)).

When a smaller data file DAT_F2 (called ghost data file) is used as the second data file, in a non-limitative embodiment, the secure element D of said mobile device T is further adapted to:

- switch the file identifications ID2, ID2' between an elementary file DAT_EF2 of said secure element D and said smaller data file DAT_F2 (function illustrated in Fig. 4 SWP(D, ID2, ID2', DAT_EF2, DAT_F2));
- switch back the file identifications ID2, ID2' between an elementary file DAT_EF2 of said secure element D and said smaller data file DAT_F2 (function illustrated in Fig. 4 SWP(D, ID2, ID2', DAT_EF2, DAT_F2)).

In this case, in a non-limitative embodiment, the operating system OS of said mobile device T is further adapted to:

- request the switching back of said file identifications ID2, ID2' between said elementary file DAT_EF2 of said secure element D and said smaller data file DAT_F2 (function illustrated in Fig. 4 RQ_SWPB(T, ID2, ID2', DAT_EF2, DAT_F2));
- read from said secure element D some data DAT2 of said elementary file DAT_EF2 (which is the ghost data file) (function illustrated in Fig. 4 RD(T, DAT2, DAT_F2);
- update the first data file DAT_EF1 of said mobile device T with the data read DAT2 (function illustrated in Fig. 4 UPDT(T, DAT_EF1, DAT2, CM)).

In a non-limitative embodiment, in order to indicate the mobile device T to read some data DAT2, RS in a second data file DAT_EF2, DAT_F2 of said secure element D, the secure element D of said mobile device T is further adapted to send to said mobile device T a proactive refresh command APDU_RES comprising a file identification ID2 of said second data file DAT_EF2, DAT_F2 to be read (function illustrated in Fig. 4 TX(D, T, APDU_RES)), said operating system OS of said mobile device T being adapted to receive said proactive refresh command APDU_RES (function illustrated in Fig. 4 TX(T, D, APDU_RES)).

In a non-limitative embodiment, the operating system OS of said mobile device T is further adapted to

- receive a request RQ from a user U for reading some data DAT1 of said first data file DAT_EF1 (function illustrated in Fig. 4 RX(T, U, RQ, DAT1, DAT_EF1));
- get the requested data DAT1 (function illustrated in Fig. 4 GT(T, DAT_EF1, DAT1));
- display said requested data DAT1 (function illustrated in Fig. 4 DISP(T, DAT1, DAT_EF1)).

In a non-limitative embodiment, the application APP of said mobile device T is adapted to:

- a launch of the update by said mobile device T of said first data file DAT_EF1 of said mobile device T with at least one command C1 (function illustrated in Fig. 4 CALL_UPDT(DAT_EF1));
- a launch of the getting by said mobile device T of the result RS of the execution of said at least one command C1 (function illustrated in Fig. 4 CALL_GT(RS));
- receive from the mobile device T the results RS of the execution of aid command C1 ((function illustrated in Fig. 4 RX(APP, T, RS)).

It is to be understood that the present invention is not limited to the aforementioned embodiments.

The non-limitative given example deals with the secure element D which may be used to provide an identity service as the secure element D stores the secret password PIN1. In a non-limitative embodiment, the secure element D may further store a user identification.

In another non-limitative embodiment, the secure element D may be used to provide email encryption/decryption for a mailbox on the mobile device T.

Hence, some embodiments of the invention may comprise one or a plurality of the following advantages:

- it permits to send some commands from the mobile device T to the secure element D and to receive by said mobile device T a response from said mobile device T without a complex standard of communication;
- it permits a secure element D to transfer data to an application APP of said mobile device T;
- it permits a mobile data T to know that an elementary file of said secure element D has been updated and to recover the data updated and to update the image of said updated elementary file in its own memory ;
- it uses only standard data files which are common to the mobile device T and to the secure element D to transmit/receive the command C1/result RS;
- thanks to the ghost file, it permits to decrease the time for:
- reading the result RS of the execution of the command C1 by the mobile device T;

- updating the first data file DAT_EF in the cache memory CM by the mobile device T.
- it therefore permits to decrease the time of the response displayed to the user or sent by the application APP to a remote server ;
- it provides a simple solution to exchange data between a secure element D of a mobile device T and an application APP of said mobile device T and this for any kind of mobile devices T, which are NFC ("Near Filed Communication") or not;
- after the power-on session of the mobile device T, the mobile device T is able to get the latest file content of the secure element D, if those files are updated in the secure element D, by the user of said mobile device for example ;
- it avoids adding a supplementary implementation layer in the secure element D and in the mobile device T as it is the case when using a standard of communication such as the SIMAlliance's standard.

CLAIMS

1- Method for communication (MTH) between a secure element (D) of a mobile device (T) and said mobile device (T), said secure element (D) comprising at least a first data file (DAT_EF1) and said mobile device (T) comprising a corresponding first data file (DAT_EF1), wherein said method for communication (MTH) comprises :

- updating by said mobile device (T) said first data file (DAT_EF1) of said mobile device (T) with at least one command (C1) to be executed by said secure element (D);
- requesting by said mobile device (T) to said secure element (D) to update the corresponding first data file (DAT_EF1) of said secure element (D) with said at least one command (C1);
- updating by said secure element (D) the corresponding first data file (DAT_EF1) of said secure element (D) with said at least one command (C1);
- extracting by said secure element (D) the at least one command (C1) within the updated first data file (DAT_EF1) of said secure element (D);
- executing by said secure element (D) the at least one command (C1);
- updating by said secure element (D) a second data file (DAT_EF2, DAT_F2) with a result (RS) of the execution of said at least one command (ADPU_C1);
- reading by said mobile device (T) from said secure element (D) the result (RS) from said second data file (DAT_EF2, DAT_F2);
- re-updating by said mobile device (T) the corresponding first data file (DAT_EF1) of said mobile device (T) with the result read (RS);
- getting by said mobile device (T) the result (RS) of the execution of said at least one command (C1) from said re-updated first data file (DAT_EF1).

2- Method for communication (MTH) according to claim 1, wherein the command (C1) to be executed by said secure element (D) is an APDU command.

3- Method for communication (MTH) according to claim 1 or claim 2, wherein the first data file (DAT_EF1) is an elementary file (EF).

4- Method for communication (MTH) according to any one of the previous claims 1 to 3, wherein the first data file (DAT_EF1) and the second data file (DAT_EF2) are:

- an ADN file; or
- an SMS file; or
- an ICCID file; or
- an MSISDN file; or
- an IMSI file.

5- Method for communication (MTH) according to any one of the previous claims 1 to 4, wherein the second data file (DAT_F2) is a data file which is smaller than the first data file (DAT_EF1).

6- Method for communication (MTH) according to the previous claim 5, wherein said method for communication (MTH) further comprises switching by said secure element (D) of the file identifications (ID2, ID2') between an elementary file (DAT_EF2) of said secure element (D) and said smaller data file (DAT_F2).

7- Method for communication (MTH) according to claim 6, wherein said method for communication (MTH) further comprises:

- switching back by said secure element (D) of the file identifications (ID2, ID2') between an elementary file (DAT_EF2) of said secure element (D) and said smaller data file (DAT_F2);
- reading by said mobile device (T) from said secure element (D) some data (DAT2) of said elementary file (DAT_F2);
- updating by said mobile device (T) the first data file (DAT_EF1) of said mobile device (T) with the data read (DAT2).

8- Method for communication (MTH) according to any one of the previous claims 1 to 7, wherein said method for communication (MTH) further comprises:

- receiving by said mobile device (T) a request (RQ) from a user (U) for reading some data (DAT1) of said first data file (DAT_EF1);
- getting by said mobile device (T) the requested data (DAT1);
- displaying by said mobile device (T) said requested data (DAT1).

9- Method for communication (MTH) according to any one of the previous claims 1 to 8, wherein said secure element is a SIM card, USIM card, an eSE, a micro-SD, an UICC, or an embedded UICC.

10- Method for communication (MTH) according to any one of the previous claims 1 to 9, wherein said mobile device (T) is a mobile phone.

11- Method for communication (MTH) according to any one of the previous claims 1 to 10, wherein said mobile device (T) is an Android™ device.

12- Method for communication (MTH) according to any one of the previous claims 1 to 11, wherein in order to indicate the mobile device (T) to read some data (DAT2, RS) in a second data file (DAT_EF2, DAT_F2) of said secure element (D), said method communication (MTH) further comprises sending by said secure element (D) to said mobile device (T) a proactive refresh command (APDU_RES) comprising a file identification (ID2) of said second data file (DAT_EF2, DAT_F2) to be read.

13- Method for communication (MTH) according to any one of the previous claims 1 to 12, wherein said mobile device (T) comprises an operating system (OS) which is adapted to perform the steps performed by said mobile device (T).

14- Method for communication (MTH) according to any one of the previous claims 1 to 12, wherein said mobile device (T) further comprises an application (APP) and said method for communication (MTH) further comprises:

- a launch by said application (APP) of the update by said mobile device (T) of said first data file (DAT_EF1) of said mobile device (T) with at least one command (C1);
- a launch by said application (APP) of the getting by said mobile device (T) of the result (RS) of the execution of said at least one command (C1).

15- Mobile device (T) for communicating with a secure element (D) of said mobile device (T), said secure element (D) comprising at least a first data file (DAT_EF1) and said mobile device (T) comprising a corresponding first data file (DAT_EF1), wherein said mobile device (T) is adapted to:

- update said first data file (DAT_EF1) of said mobile device (T) with at least one command (C1) to be executed by said secure element (D);
- request to said secure element (D) to update the corresponding first data file (DAT_EF1) of said secure element (D) with said at least one command (C1);
- update by said secure element (D) the corresponding first data file (DAT_EF1) of said secure element (D) with said at least one command (C1);
- extract by said secure element (D) the at least one command (C1) within the updated first data file (DAT_EF1) of said secure element (D);
- execute by said secure element (D) the at least one command (C1);
- update by said secure element (D) a second data file (DAT_EF2, DAT_F2) with a result (RS) of the execution of said at least one command (ADPU_C1);
- read from said secure element (D) the result (RS) from said second data file (DAT_EF2, DAT_F2);
- re-update the corresponding first data file (DAT_EF1) of said mobile device (T) with the result read (RS);

- get the result (RS) of the execution of said at least one command (C1) from said re-updated first data file (DAT_EF1).

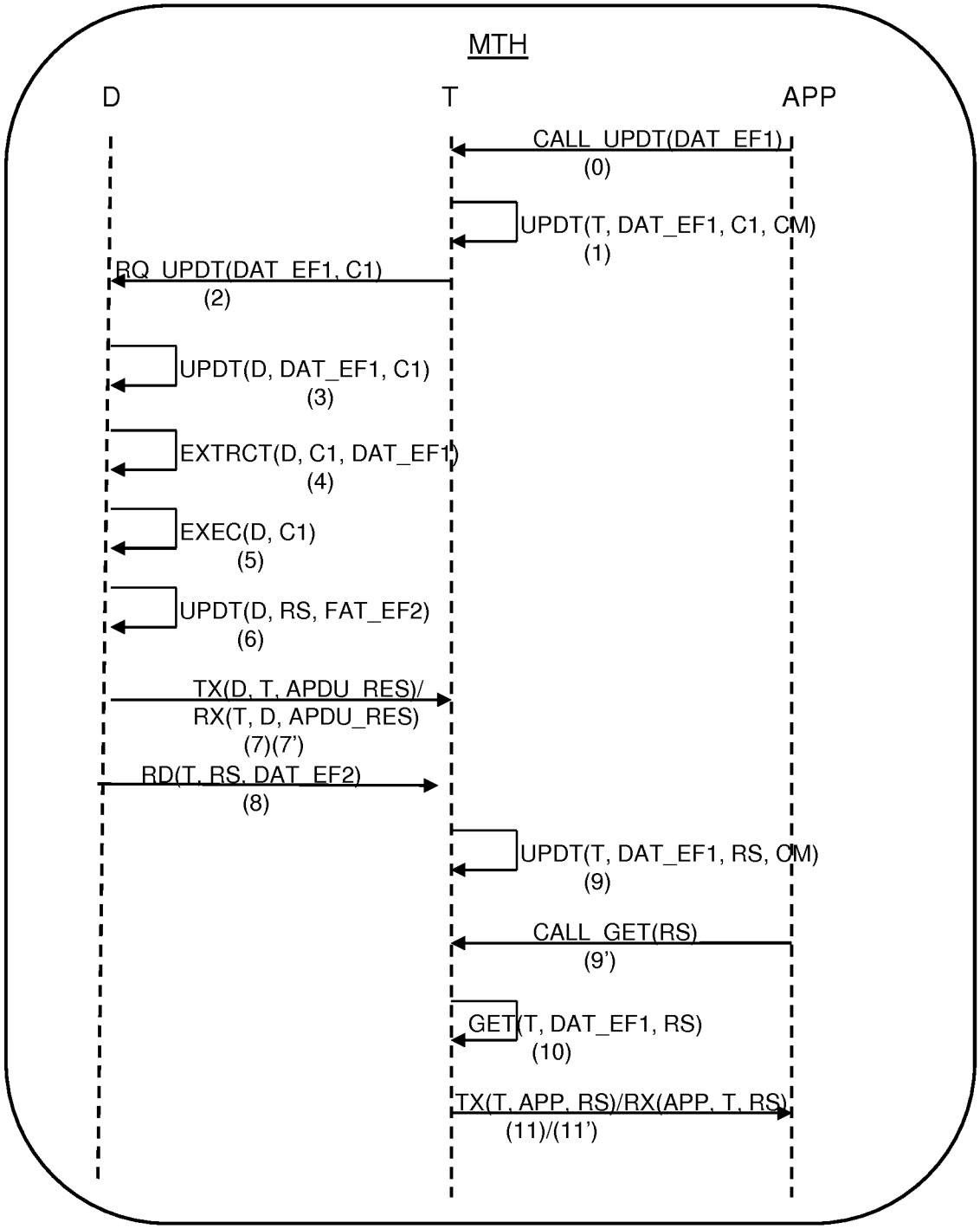
MTH
D
T
APP
CALL_UPDT(DAT_EF1)
(0)
UPDT(T, DAT_EF1, C1, CM)
(1)
RQ_UPDT(DAT_EF1, C1)
(2)
UPDT(D, DAT_EF1, C1)
(3)
EXTRCT(D, C1, DAT_EF1)
(4)
EXEC(D, C1)
(5)
UPDT(D, RS, FAT_EF2)
(6)
TX(D, T, APDU_RES)/
RX(T, D, APDU_RES)
(7)(7')
RD(T, RS, DAT_EF2)
(8)
UPDT(T, DAT_EF1, RS, CM)
(9)
CALL_GET(RS)
(9')
GET(T, DAT_EF1, RS)
(10)
TX(T, APP, RS)/RX(APP, T, RS)
(11)/(11')

Fig. 1

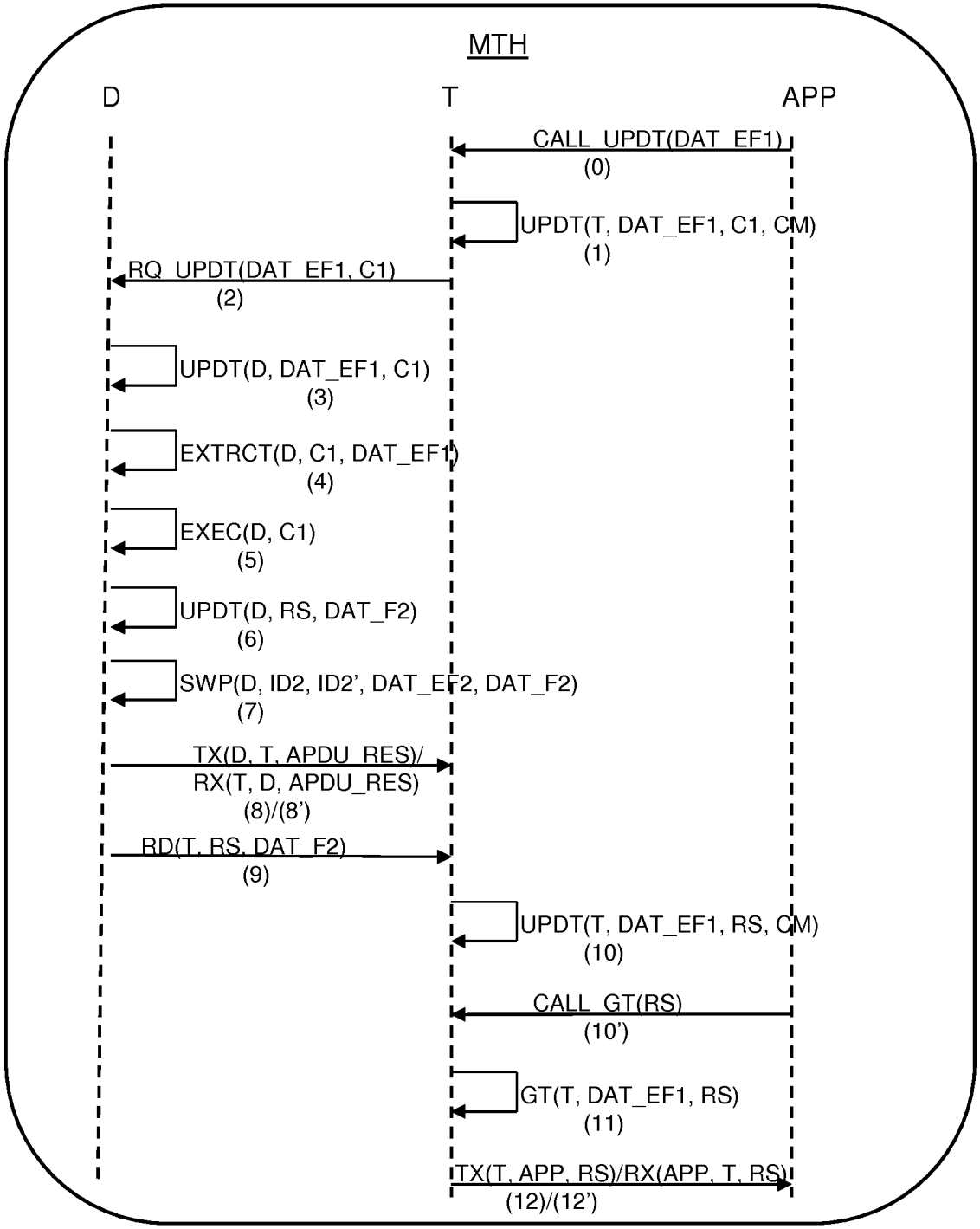
MTH
D
T
APP
CALL_UPDT(DAT_EF1)
(0)
UPDT(T, DAT_EF1, C1, CM)
(1)
RQ_UPDT(DAT_EF1, C1)
(2)
UPDT(D, DAT_EF1, C1)
(3)
EXTRCT(D, C1, DAT_EF1)
(4)
EXEC(D, C1)
(5)
UPDT(D, RS, DAT_F2)
(6)
SWP(D, ID2, ID2', DAT_EF2, DAT_F2)
(7)
TX(D, T, APDU_RES)/
RX(T, D, APDU_RES)
(8)/(8')
RD(T, RS, DAT_F2)
(9)
UPDT(T, DAT_EF1, RS, CM)
(10)
CALL_GT(RS)
(10')
GT(T, DAT_EF1, RS)
(11)
TX(T, APP, RS)/RX(APP, T, RS)
(12)/(12')

Fig. 2

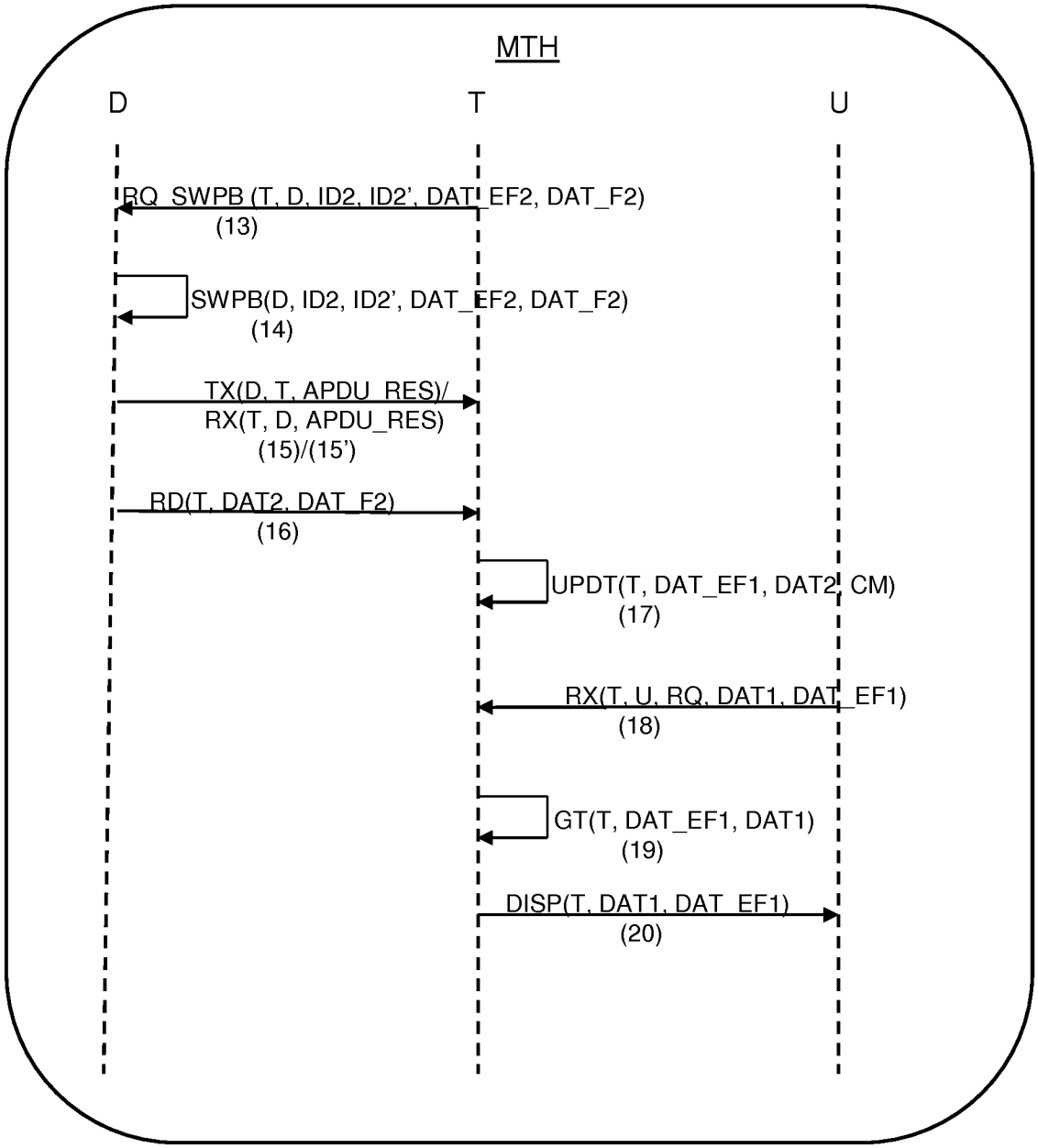
MTH
D
T
U
RQ_SWPB (T, D, ID2, ID2', DAT_EF2, DAT_F2)
(13)
SWPB(D, ID2, ID2', DAT_EF2, DAT_F2)
(14)
TX(D, T, APDU_RES)/
RX(T, D, APDU_RES)
(15)/(15')
RD(T, DAT2, DAT_F2)
(16)
UPDT(T, DAT_EF1, DAT2, CM)
(17)
RX(T, U, RQ, DAT1, DAT_EF1)
(18)
GT(T, DAT_EF1, DAT1)
(19)
DISP(T, DAT1, DAT_EF1)
(20)

Fig. 3

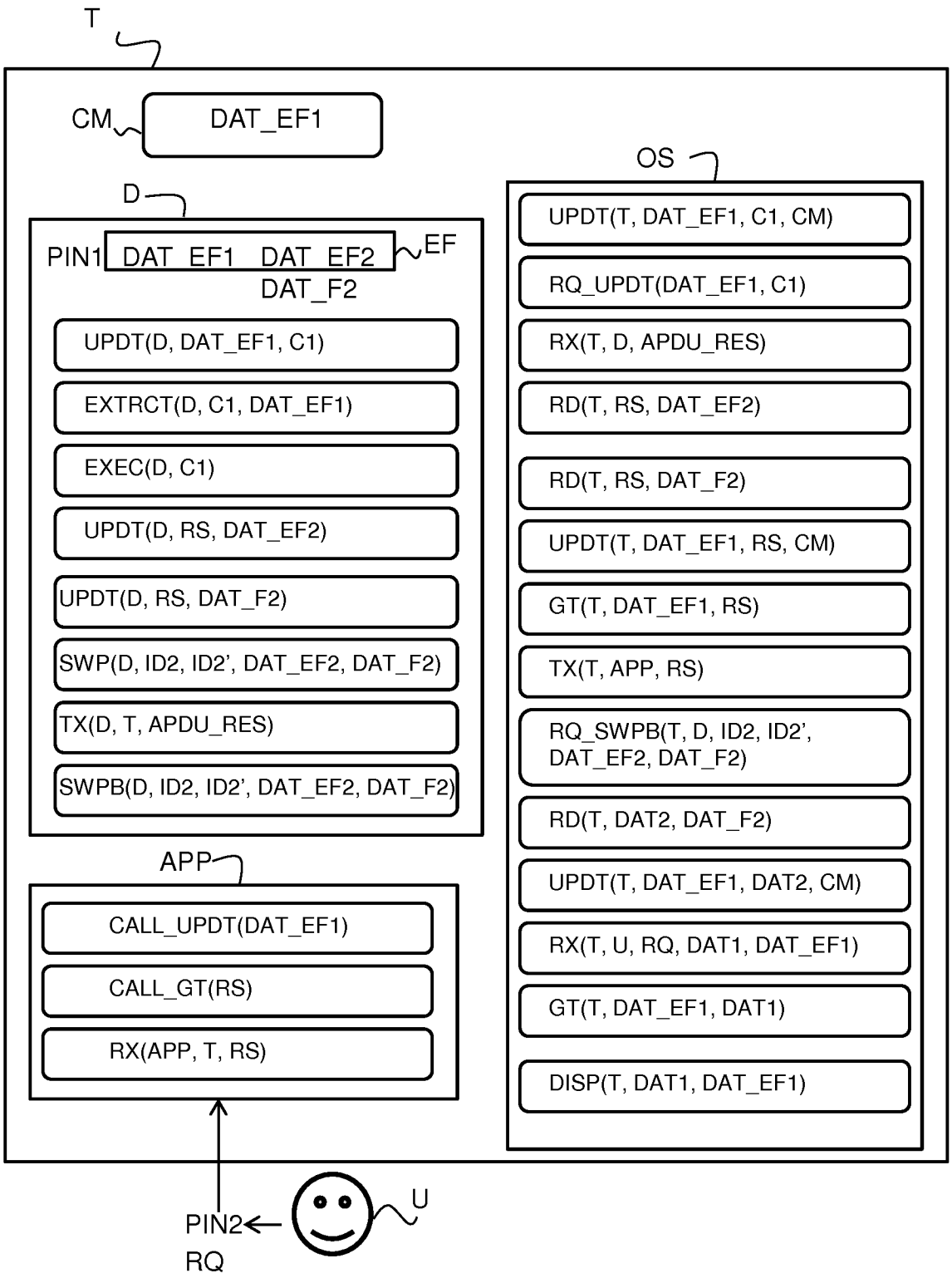
T
CM
DAT_EF1
D
PIN1
DAT_EF1
DAT_EF2
DAT_F2
EF
UPDT(D, DAT_EF1, C1)
EXTRCT(D, C1, DAT_EF1)
EXEC(D, C1)
UPDT(D, RS, DAT_EF2)
UPDT(D, RS, DAT_F2)
SWP(D, ID2, ID2', DAT_EF2, DAT_F2)
TX(D, T, APDU_RES)
SWPB(D, ID2, ID2', DAT_EF2, DAT_F2)
APP
CALL_UPDT(DAT_EF1)
CALL_GT(RS)
RX(APP, T, RS)
OS
UPDT(T, DAT_EF1, C1, CM)
RQ_UPDT(DAT_EF1, C1)
RX(T, D, APDU_RES)
RD(T, RS, DAT_EF2)
RD(T, RS, DAT_F2)
UPDT(T, DAT_EF1, RS, CM)
GT(T, DAT_EF1, RS)
TX(T, APP, RS)
RQ_SWPB(T, D, ID2, ID2', DAT_EF2, DAT_F2)
RD(T, DAT2, DAT_F2)
UPDT(T, DAT_EF1, DAT2, CM)
RX(T, U, RQ, DAT1, DAT_EF1)
GT(T, DAT_EF1, DAT1)
DISP(T, DAT1, DAT_EF1)
PIN2
RQ
U

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/068451

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W4/00 G06F9/54
ADD. H04W12/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014/165170 A1 (DMITRIEV ANDREY [RU] ET AL) 12 June 2014 (2014-06-12) paragraph [0001] - paragraph [0010] figures 1,5	1-15
A	EP 1 965 596 A1 (GEMPLUS CARD INT [FR]) 3 September 2008 (2008-09-03) paragraph [0030] - paragraph [0051]	1-15
A	"Smart Cards; Card Application Toolkit (CAT) (Release 13)", TECHNICAL SPECIFICATION, EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI), 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS ; FRANCE, vol. SCP TEC, no. V13.0.0, March 2015 (2015-03), XP014248245, page 33 - page 108	1-15

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 October 2016	31/10/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ströbeck, Anders

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/068451

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 11)", TECHNICAL SPECIFICATION, EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI), 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS ; FRANCE, vol. SCP TEC, no. V11.1.0, November 2013 (2013-11), XP014180137, page 79 - page 131 -----	1-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/068451

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014165170 A1	12-06-2014	NONE	
EP 1965596 A1	03-09-2008	BR PI0807906 A2	17-06-2014
		EP 1965596 A1	03-09-2008
		EP 2116077 A1	11-11-2009
		US 2010178945 A1	15-07-2010
		WO 2008104515 A1	04-09-2008