US 20120123945A1

(19) **United States**

(12) **Patent Application Publication**

CHARRAT

(10) **Pub. No.: US 2012/0123945 A1**

(43) **Pub. Date: May 17, 2012**

(54) **NFC TRANSACTION METHOD AND SYSTEM**

(75) Inventor: **Bruno CHARRAT**, Aix-en-Provence (FR)

(73) Assignee: **INSIDE SECURE**, Aix-en-Provence (FR)

(21) Appl. No.: **13/297,323**

(22) Filed: **Nov. 16, 2011**

(30) **Foreign Application Priority Data**

Nov. 17, 2010	(FR)	10 04473
Nov. 17, 2010	(FR)	10 04475

Publication Classification

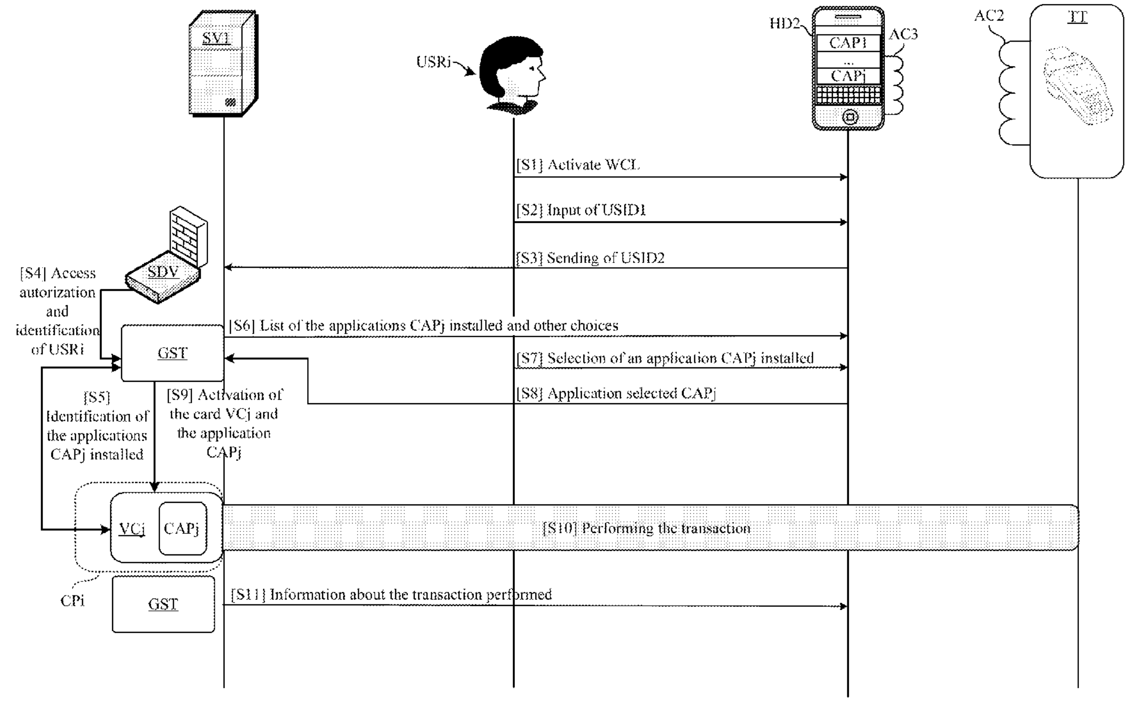
(51) **Int. Cl.**

G06Q 30/06	(2012.01)
H04L 9/28	(2006.01)

(52) **U.S. Cl.** **705/50**; 705/26.1

(57) **ABSTRACT**

A method for performing a transaction between a portable device and a transaction device includes: providing at least one transaction server having at least one application program configured to receive, process and emit application data, establishing at least one data link between the portable device and the transaction server, establishing a near field communication channel between the portable device and the transaction device, and, via the portable device, transferring to the application program of the server application data sent by the transaction device, and receiving application data sent by the application program of the server and transferring them to the transaction device.


SV1
USRi
HD2
CAP1
...
CAPj
AC3
AC2
TT
[S1] Activate WCL
[S2] Input of USID1
[S3] Sending of USID2
[S4] Access autorization and identification of USRi
SDV
GST
[S6] List of the applications CAPj installed and other choices
[S7] Selection of an application CAPj installed
[S8] Application selected CAPj
[S5] Identification of the applications CAPj installed
[S9] Activation of the card VCj and the application CAPj
VCj
CAPj
[S10] Performing the transaction
CPi
GST
[S11] Information about the transaction performed

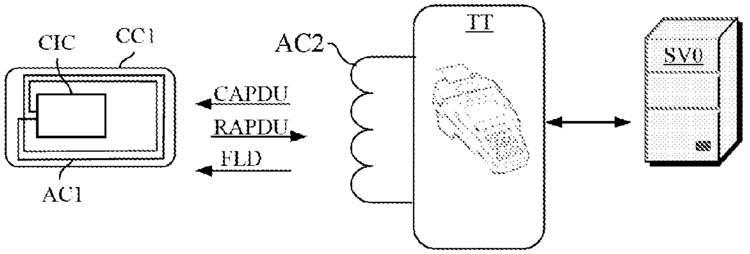


Fig. 1
(Prior Art)

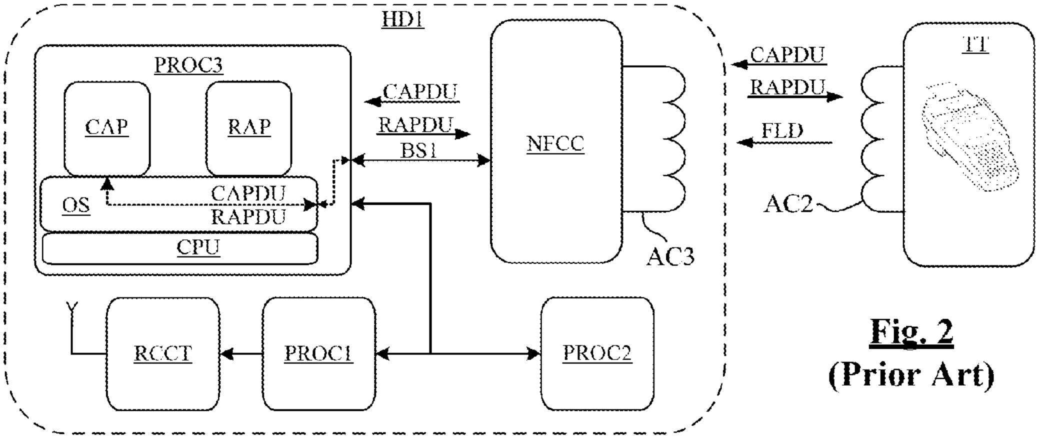


Fig. 2
(Prior Art)

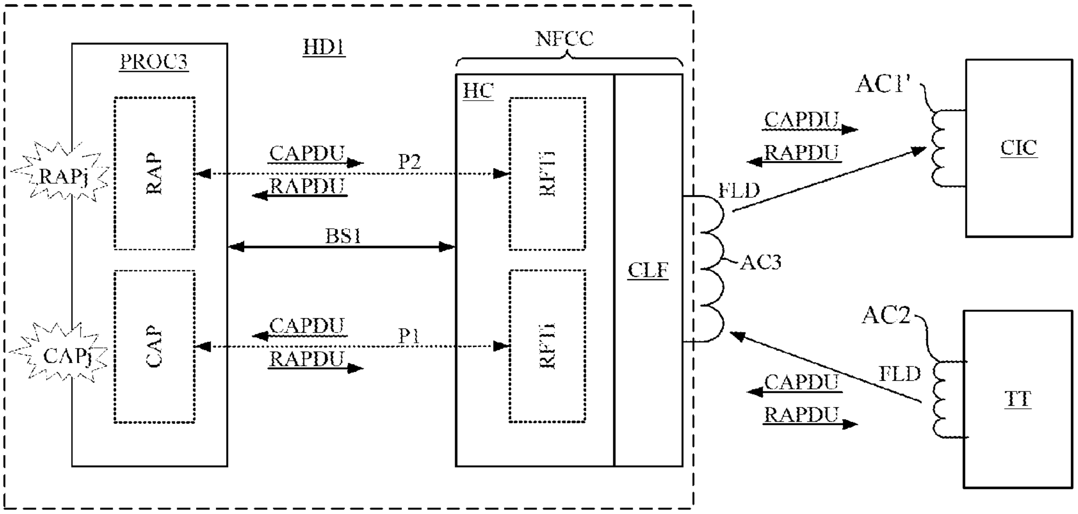


Fig. 3
(Prior Art)

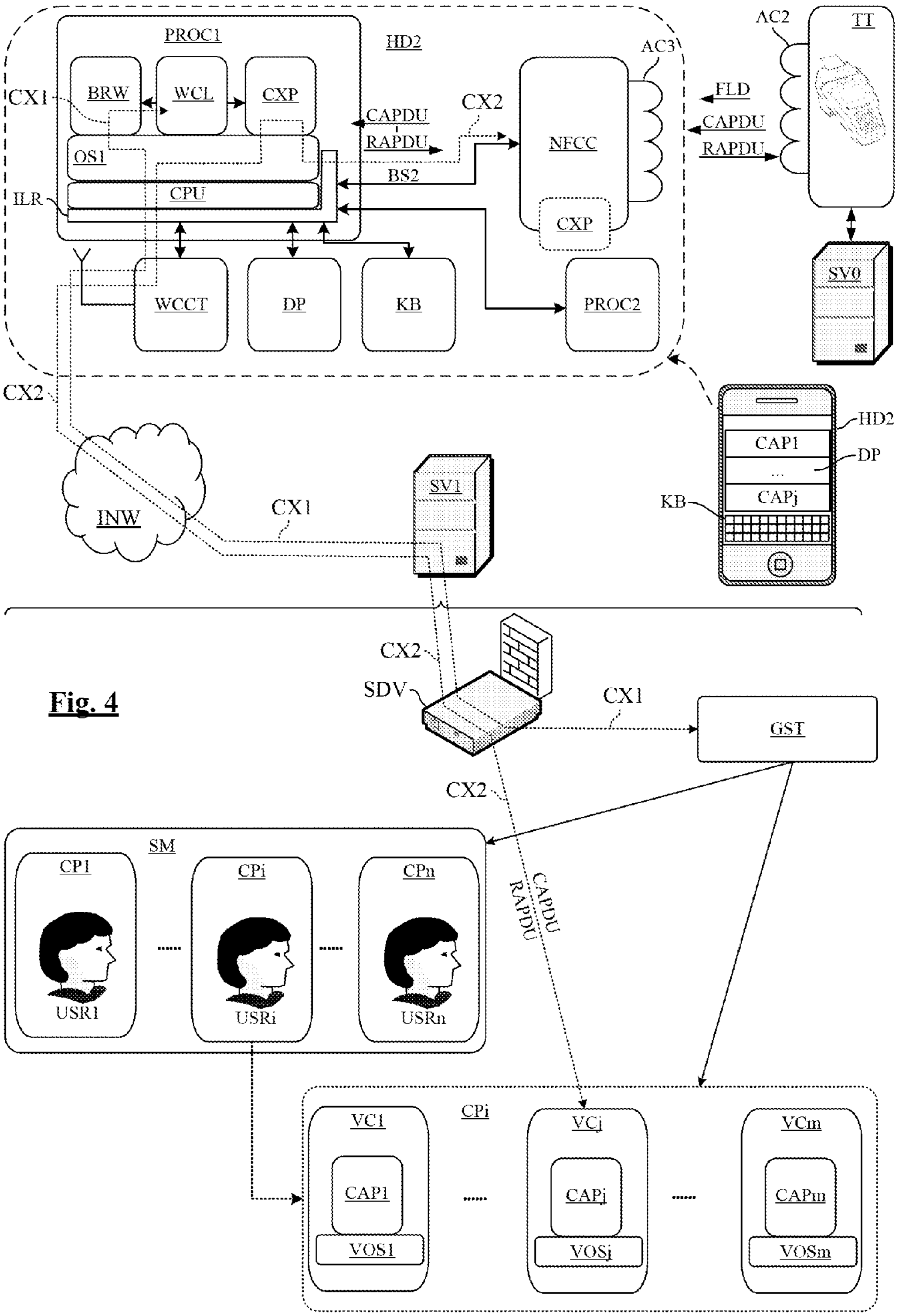

PROC1
HD2
BRW
WCL
CXP
CX1
OS1
CPU
ILR
CAPDU
RAPDU
CX2
BS2
NFCC
CXP
AC3
AC2
TT
FLD
CAPDU
RAPDU
SV0
WCCT
DP
KB
PROC2
CX2
INW
CX1
SV1
HD2
CAP1
...
DP
CAPj
KB
CX2
SDV
CX1
GST
CX2
SM
CP1
CPi
CPn
USR1
USRi
USRn
CAPDU
RAPDU
CPi
VC1
VCj
VCm
CAP1
CAPj
CAPm
VOS1
VOSj
VOSm

Fig. 4

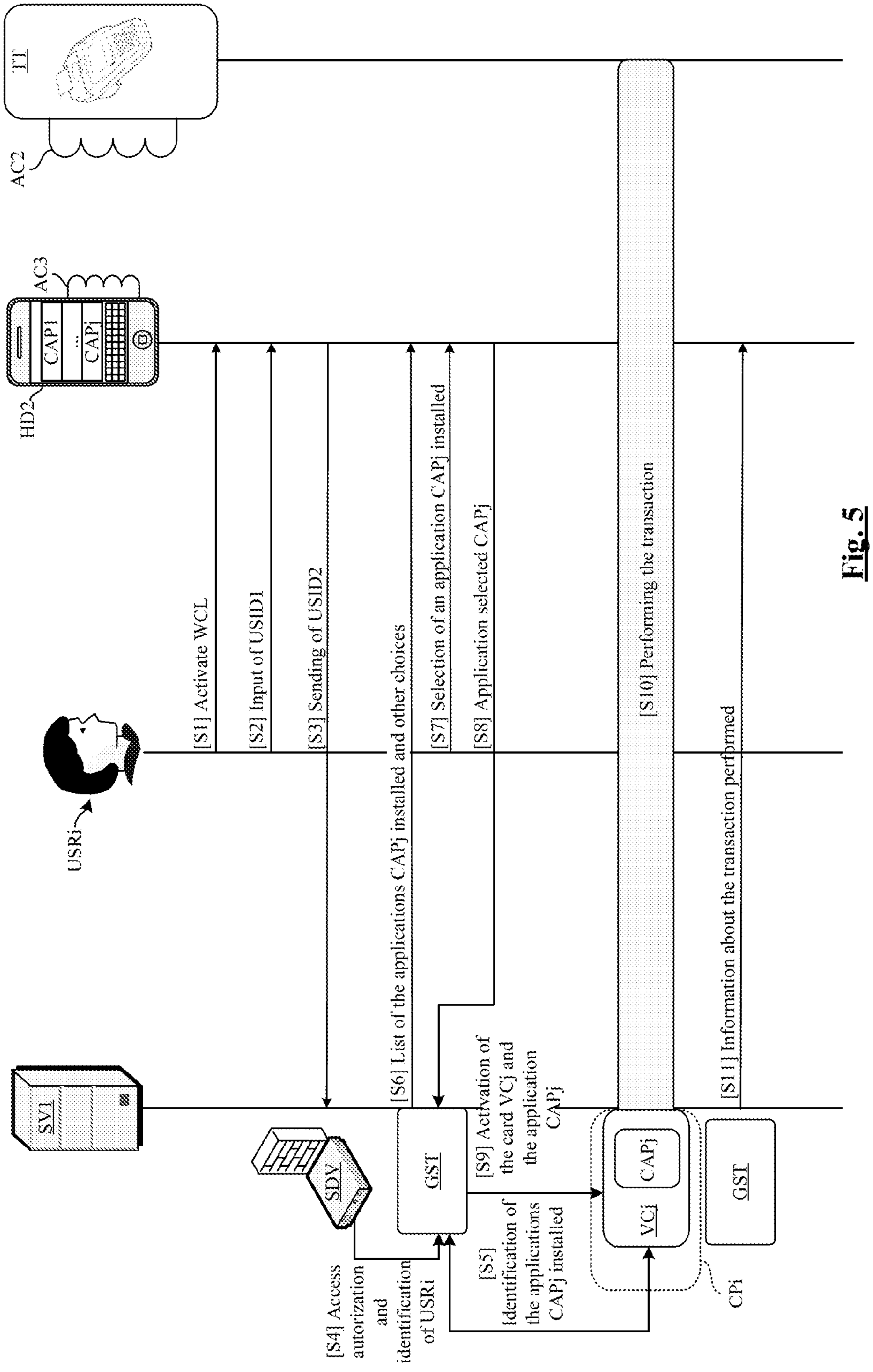

TT
AC2
HD2
AC3
CAP1
...
CAPj
USRi
SV1
SDV
GST
VCj
CAPj
GST
CPi
[S1] Activate WCL
[S2] Input of USID1
[S3] Sending of USID2
[S4] Access autorization and identification of USRi
[S5] Identification of the applications CAPj installed
[S6] List of the applications CAPj installed and other choices
[S7] Selection of an application CAPj installed
[S8] Application selected CAPj
[S9] Activation of the card VCj and the application CAPj
[S10] Performing the transaction
[S11] Information about the transaction performed

Fig. 5

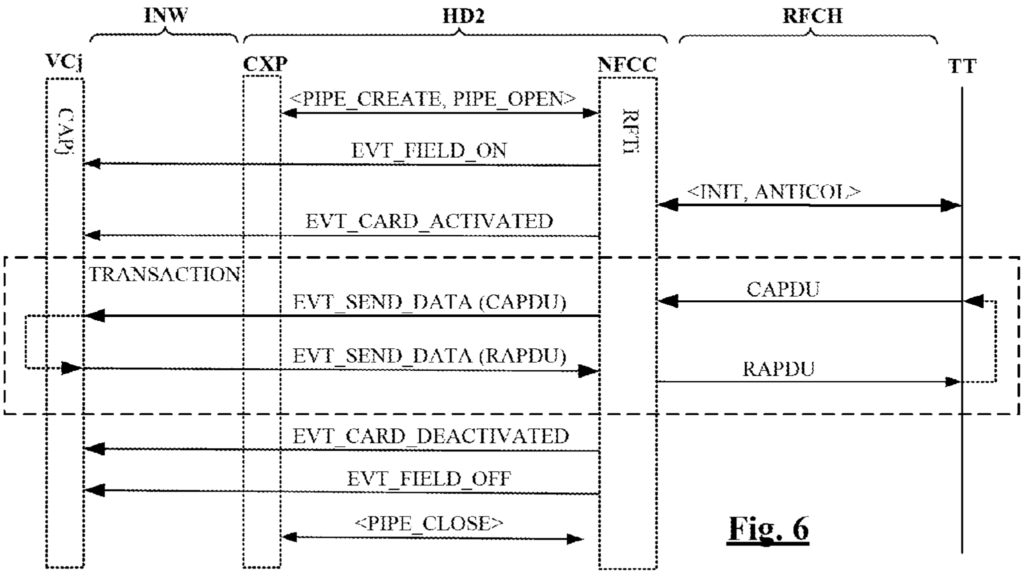

INW
HD2
RFCH
VCj
CXP
NFCC
TT
CAPj
RFTi
<PIPE_CREATE, PIPE_OPEN>
EVT_FIELD_ON
<INIT, ANTICOL>
EVT_CARD_ACTIVATED
TRANSACTION
EVT_SEND_DATA (CAPDU)
CAPDU
EVT_SEND_DATA (RAPDU)
RAPDU
EVT_CARD_DEACTIVATED
EVT_FIELD_OFF
<PIPE_CLOSE>

Fig. 6

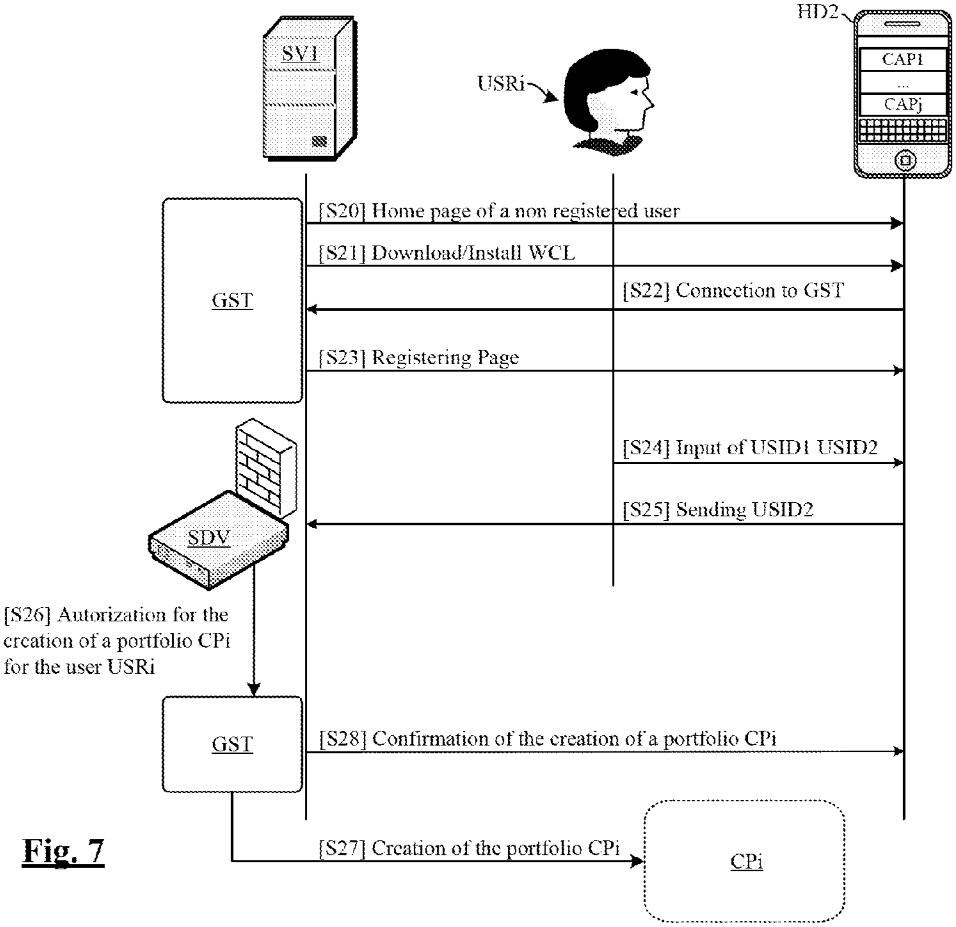

HD2
SV1
USRi
CAP1
...
CAPj
GST
[S20] Home page of a non registered user
[S21] Download/Install WCL
[S22] Connection to GST
[S23] Registering Page
[S24] Input of USID1 USID2
[S25] Sending USID2
SDV
[S26] Autorization for the creation of a portfolio CPi for the user USRi
GST
[S28] Confirmation of the creation of a portfolio CPi
[S27] Creation of the portfolio CPi
CPi

Fig. 7

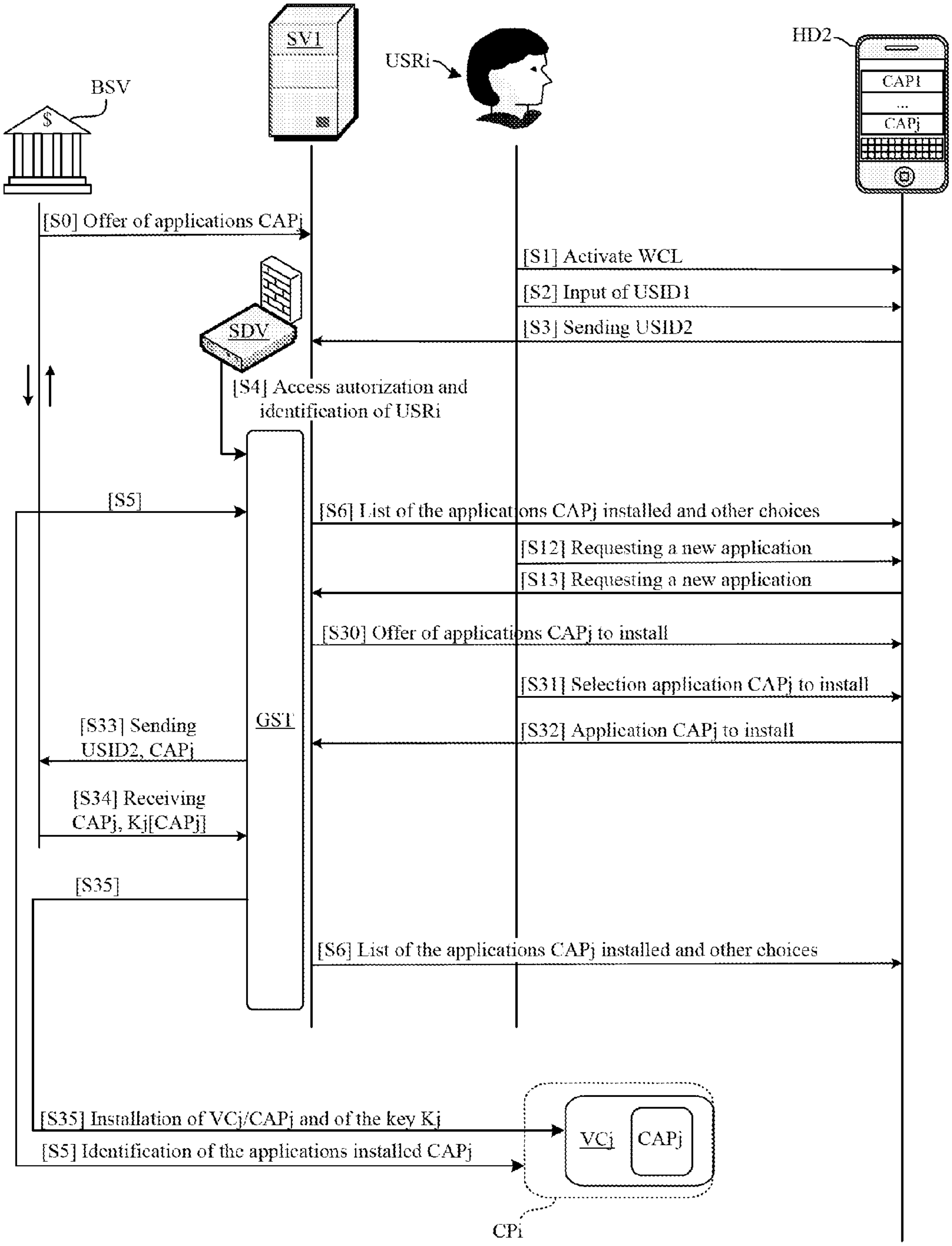

SV1
USRi
HD2
CAP1
...
CAPj
BSV
$
[S0] Offer of applications CAPj
[S1] Activate WCL
[S2] Input of USID1
[S3] Sending USID2
SDV
[S4] Access autorization and identification of USRi
[S5]
[S6] List of the applications CAPj installed and other choices
[S12] Requesting a new application
[S13] Requesting a new application
[S30] Offer of applications CAPj to install
[S31] Selection application CAPj to install
GST
[S33] Sending USID2, CAPj
[S32] Application CAPj to install
[S34] Receiving CAPj, Kj[CAPj]
[S35]
[S6] List of the applications CAPj installed and other choices
[S35] Installation of VCj/CAPj and of the key Kj
[S5] Identification of the applications installed CAPj
VCj
CAPj
CPi

Fig. 8

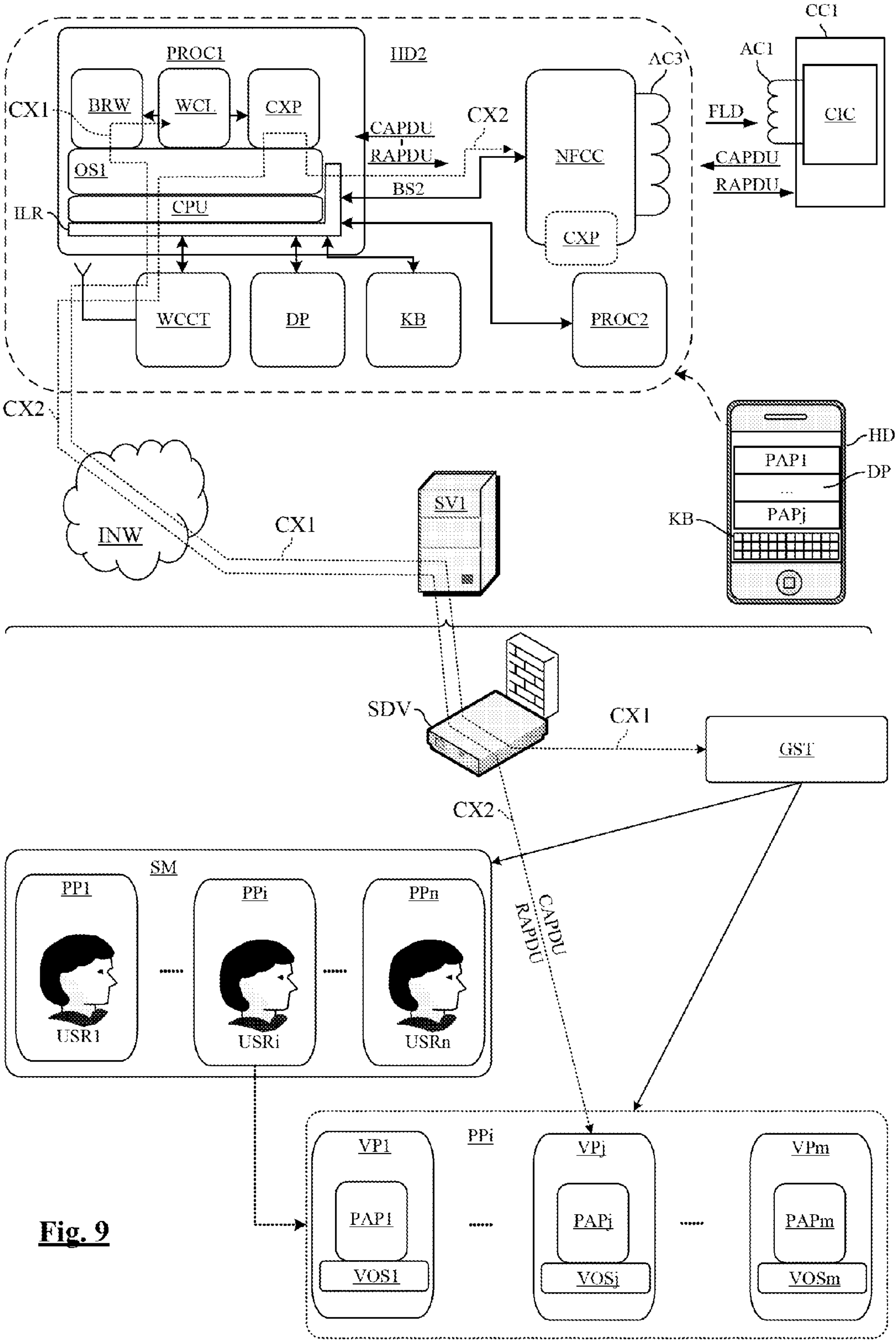

PROC1
HD2
CC1
AC1
AC3
BRW
WCL
CXP
CX1
CAPDU
RAPDU
CX2
NFCC
FLD
CIC
CAPDU
RAPDU
OS1
BS2
CPU
ILR
CXP
WCCT
DP
KB
PROC2
CX2
HD2
PAP1
...
PAPj
DP
KB
INW
CX1
SV1
SDV
CX1
GST
CX2
SM
PP1
PPi
PPn
USR1
USRi
USRn
CAPDU
RAPDU
PPi
VP1
VPj
VPm
PAP1
PAPj
PAPm
VOS1
VOSj
VOSm

Fig. 9

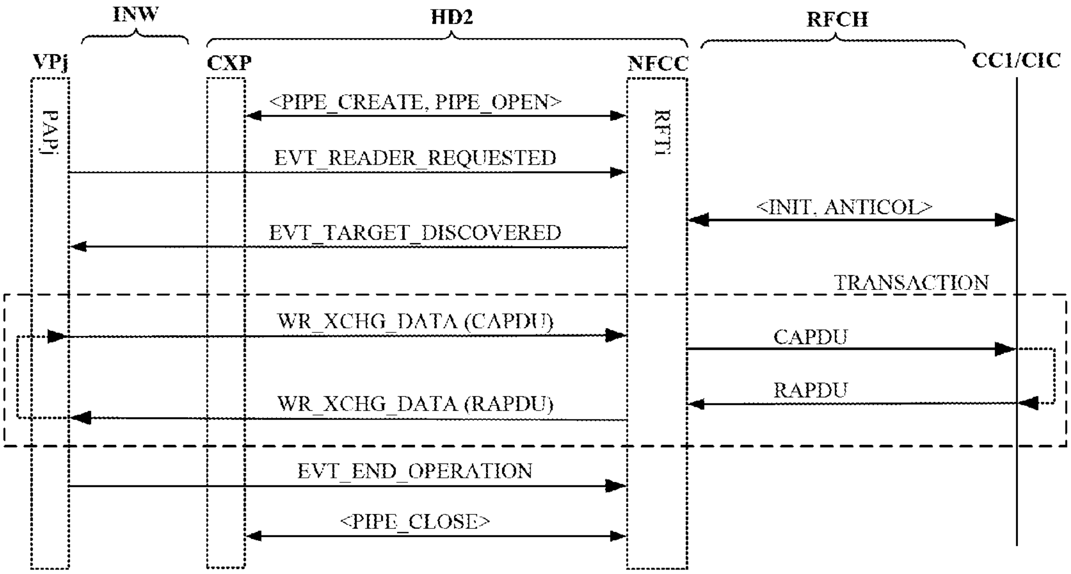

INW
HD2
RFCH
VPj
CXP
NFCC
CC1/CIC
PAPj
RFTi
<PIPE_CREATE, PIPE_OPEN>
EVT_READER_REQUESTED
<INIT, ANTICOL>
EVT_TARGET_DISCOVERED
TRANSACTION
WR_XCHG_DATA (CAPDU)
CAPDU
RAPDU
WR_XCHG_DATA (RAPDU)
EVT_END_OPERATION
<PIPE_CLOSE>

Fig. 10

NFC TRANSACTION METHOD AND SYSTEM

BACKGROUND OF THE INVENTION

[0001] Embodiments of the present invention relate to a near field transaction method and a near field transaction system.

[0002] In the last few years, the apparition of inductive coupling contactless communication techniques, also called NFC techniques (Near Field Communication), changed the field of chip cards, making it possible first to make contactless payment cards, and then, to integrate a secure processor and an NFC controller into electronic portable objects such as mobile phones, to perform near field transactions.

[0003] FIG. **1** schematically shows a conventional transaction system including a contactless chip card CC**1** and a transaction terminal TT. The terminal TT is for example a cash point, a sales outlet (e.g., ticket machine, food and drink dispenser), an automatic paying access control terminal (e.g., metro access terminal, bus payment terminal), or the like.

[0004] The contactless card CC**1** includes a Contactless Integrated Circuit CIC provided with a secure processor and an antenna coil AC**1** connected to the integrated circuit. The terminal TT includes an antenna coil AC**2** and is configured to perform a near field transaction with the card CC**1** by emitting a magnetic field FLD. The transaction includes exchanging Application Protocol Data Units APDU which will be hereinafter referred to as "application data" for the sake of simplicity. The application data APDU include commands CAPDU sent by the terminal and answers RAPDU sent by the card. The terminal TT may be linked in real time or delay time to a transaction server SV**0**, to validate a payment and/or debit an account of the user.

[0005] FIG. **2** schematically shows a transaction system including a mobile phone HD**1** and the transaction terminal TT. The phone HD**1** includes a main processor PROC**1**, a radiocommunication circuit RCCT, a secure processor PROC**2** of SIM card (Subscriber Identity Module), a NFC controller referenced "NFCC", an antenna coil AC**3** linked to the controller NFCC and a secure processor PROC**3** configured to perform NFC transactions.

[0006] The processor PROC**3** includes a central processing unit CPU, an operating system OS, a Card Application Program CAP and/or a Reader Application Program RAP. The processor PROC**3** is linked to the controller NFCC through a bus BS**1**, for example a Single Wire Protocol bus SWP. In practice, the processor PROC**3** may be a Universal Integrated Circuit Card UICC, for example of the mini-SIM or micro-SIM type.

[0007] An example of functional architecture of the controller NFCC and the processor PROC**3** is shown in FIG. **3**. The controller NFCC includes a host controller HC and a Contactless Front End Interface CLF which is linked to the antenna coil AC**3**. In practice, the host controller HC and the interface CLF may be integrated into the same semiconductor chip, such as the MicroRead® chip commercialized by the applicant.

[0008] The bus BS**1** linking the processor PROC**3** and the controller NFCC is used as physical support for a communication interface called Host Controller Interface (HCI) through which the controller NFCC and the processor PROC**3** exchange data in accordance with a Host Controller Protocol HCP. The interface HCI and the protocol HCP are described in the specifications ETSI TS 102 622 of the European Telecommunications Standards Institute, called "Smart Cards; Universal Integrated Circuit Card (UICC); Contactless Front-end (CLF) interface; Host Controller Interface (HCI)." The protocol HCP provides the routing of data according to routing channels called "pipes", through which application data APDU are exchanged during a transaction between the processor PROC**3** and the transaction terminal TT.

[0009] The interface CLF may generally operate according to several RF technologies referred to as "RFTi" in FIG. **3**, for example "Type A" or "Type B" such as defined by ISO/IEC 14443 parts 2, 3 and 4, "Type B'" such as defined by ISO/IEC 14443-2, with a standard framing such as defined by ISO/IEC 14443-3, and "Type F" such as defined by ISO 18092 (as passive mode at 212 and 424 kilobytes per second) or by the Japanese industrial standard JIS X 6319-4.

[0010] During the execution of the card application CAP, the processor PROC**3** emulates a contactless card and uses the controller NFCC in passive mode to perform a transaction with a transaction terminal TT which emits the magnetic field FLD. A pipe P**1** is first opened between the card application CAP and the interface CLF of the controller NFCC, which is configured for the occasion in an RFTi technology. The terminal TT sends to the controller NFCC commands CAPDU that the controller transmits to the processor PROC**3** through the pipe Pl. The processor PROC**3** emits answers RAPDU which are transmitted to the controller NFCC through the pipe P**1**, and then transmitted to the terminal TT by the controller NFCC, through a pipe RF.

[0011] During the execution of the reader application RAP, the processor PROC**3** performs a transaction with a contactless integrated circuit CIC arranged in a contactless card CC**1** or another support. The controller NFCC is in an active operating mode where it emits a magnetic field FLD. A pipe P**1** is first opened between the reader application RAP and the interface CLF of the controller NFCC, which is configured for the occasion in an RFTi technology. The reader application RAP then emits commands CAPDU which are transmitted to the controller NFCC through the pipe P**2**, and then transmitted to the integrated circuit CIC through a pipe RF. The contactless integrated circuit CIC sends to the controller NFCC answers RAPDU that the controller transmits to the processor PROC**3** through the pipe P**2**.

[0012] It is known that the development of the NFC technology is closely related to the development of card applications in portable devices such as mobile phones, so as to use such portable devices as contactless chip cards. Although infrastructures provided with NFC transaction terminals already exist, in particular in the field of payment, the integration of secure processors into mobile phones to execute such applications is not carried out at a sufficient rate to allow the NFC technology to be developed as expected.

[0013] A constraint which slows down the development is the complexity and cost of a secure processor such as the processor PROC**3** shown in FIGS. **2** and **3**. It must preferably be able to execute various card applications and must therefore contain as many bank keys (encryption keys) as card applications supplied by different banks. It must in addition have a sufficient computing power to carry out complex encryption calculations during the authentication phase of a transaction. In addition, the personalization of the processor, i.e., loading a card application CAP into the memory thereof, is a complex operation which must be highly secured and requires external managers such as a Trusted Service Manager TSM. Finally, in the event of phone theft or during a maintenance operation of the phone, the processor PROC3 is susceptible of being attacked by a fraud so as to discover the bank keys.

[0014] It is therefore desirable to provide a method allowing a NFC transaction to be performed by way of a portable device of the mobile phone type having an architecture which is simpler and less expensive to implement than known architectures.

BRIEF SUMMARY OF THE INVENTION

[0015] Embodiments of the invention relate to a method for performing a transaction between a portable device and a transaction device, including: providing at least one transaction server having at least one application program configured to receive, process and emit application data; establishing at least one data link between the portable device and the transaction server; establishing a near field communication channel between the portable device and the transaction device; and via the portable device, transferring to the application program of the server application data sent by the transaction device, and receiving application data sent by the application program of the server and transferring them to the transaction device.

[0016] According to one embodiment, the method includes installing in the transaction server at least one application program configured to emulate a chip card.

[0017] According to one embodiment, the method includes installing in the transaction server at least one application program configured to emulate a payment point in order to perform a transaction with a chip card.

[0018] According to one embodiment, the method includes, via the portable device, receiving from the server a choice of available transaction services and supplying to the server a selection of at least one transaction service, and activating in the server an application program corresponding to the transaction service selected and linking the application program to the portable device so that the application program performs the transaction.

[0019] According to one embodiment, the method includes, via the portable device, receiving from the server an offer of transaction services and supplying to the server a selection of at least one transaction service, and installing in the server an application program corresponding to the transaction service selected.

[0020] According to one embodiment, installing the application program includes installing an encryption key allocated to the application program.

[0021] According to one embodiment, the method includes, via the portable device, receiving from the server an offer for subscribing to transaction services and supplying to the server an acceptance of the subscription offer including identification data for identifying a user, allocating a memory area of the server to the identified user, and storing in the memory area a portfolio of applications allocated to the user.

[0022] Embodiments of the invention also relate to a transaction system including a portable device and a transaction device, each including near field communication circuitry, the portable device including wireless communication circuitry, wherein the system includes at least one transaction server accessible via the Internet network, including at least one application program configured to receive, process and emit application data during a transaction, and the portable device is configured to establish at least one data link with the transaction server through the wireless communication circuitry, establish a near field communication channel with the transaction device, transfer to the application program of the server application data sent by the transaction device, and receive application data sent by the application program of the server and transfer the application data to the transaction device.

[0023] According to one embodiment, the transaction server includes at least one card application program configured to emulate a payment card.

[0024] According to one embodiment, the transaction server includes at least one application program configured to emulate a payment point able to debit a payment card.

[0025] According to one embodiment, the portable device is configured to receive from the server a choice of available transaction services, and supply to the server a selection of at least one transaction service, and the server includes a service management program configured to, in response to the selection of at least one transaction service, activate in the server an application program corresponding to the transaction service selected.

[0026] According to one embodiment, the portable device is configured to receive from the server an offer of transaction services and supply to the server a selection of at least one transaction service, and the server includes a service management program configured to, in response to the selection of at least one transaction service, install in the server an application program corresponding to the transaction service selected.

[0027] According to one embodiment, the service management program is configured to, during the installation of an application program, also install an encryption key allocated to the application program.

[0028] According to one embodiment, the portable device is configured to receive from the server an offer for subscribing to transaction services and supply to the server an acceptance of the subscription offer including identification data for identifying a user, and the server includes at least one service management program configured to allocate a memory area of the server to the identified user, and store in the memory area a portfolio of applications allocated to the user.

[0029] According to one embodiment, the transaction server includes or is associated to a security and access control device or program configured to authorize the access to transaction services only after the portable device has supplied valid authentication data of a user.

[0030] Embodiments of the invention also relate to a portable device including near field communication circuitry and wireless communication circuitry, wherein the device is configured to establish at least one data link with a transaction server through the wireless communication circuitry, establish a near field communication channel with the transaction device, through the near field communication circuitry, transfer to the server application data sent by the transaction device, and receive application data sent by the server and transfer them to the transaction device.

[0031] According to one embodiment, the portable device is configured to receive from the server a choice of available transaction services, and supply to the server a selection of at least one transaction service to be activated in the server to perform a transaction.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0032] The foregoing summary, as well as the following detailed description of the invention, will be better understood when read in conjunction with the appended drawings. For the purpose of illustrating the invention, there are shown in the drawings embodiments which are presently preferred. It should be understood, however, that the invention is not limited to the precise arrangements and instrumentalities shown.

[0033] In the drawings:

[0034] FIG. **1** previously described shows a conventional NFC transaction system including a contactless chip card,

[0035] FIG. **2** previously described shows a conventional NFC transaction system including a portable device equipped with a secure transaction processor,

[0036] FIG. **3** previously described is a functional diagram of the transaction system of FIG. **2**,

[0037] FIG. **4** shows an embodiment of a NFC transaction system according to the invention,

[0038] FIG. **5** shows steps of a NFC transaction performed via the system of FIG. **4**,

[0039] FIG. **6** shows in greater details some steps of the transaction,

[0040] FIG. **7** shows an embodiment of a method for declaring a user to the transaction system of FIG. **4**,

[0041] FIG. **8** shows an embodiment of a method for activating an application before the implementation thereof in the transaction system shown in FIG. **4**,

[0042] FIG. **9** shows another embodiment of a NFC transaction system according to the invention, and

[0043] FIG. **10** shows steps of a NFC transaction performed via the system of FIG. **9**.

DETAILED DESCRIPTION OF THE INVENTION

[0044] FIG. **4** shows an embodiment of a transaction system according to the invention. The system includes a transaction terminal TT, a portable device HD**2** and a transaction server SV**1** connected to the Internet.

[0045] The terminal TT, provided with an antenna coil AC**2**, is configured to perform a NFC transaction with a contactless NFC card such as that shown in FIG. **1** or a device HD**1** such as that shown in FIG. **2**.

[0046] The device HD**2** includes a main processor PROC**1**, a display DP, a keyboard KB (which may be virtual and shown by the display), a NFC controller "NFCC" provided with an antenna coil AC**3** for establishing a near field communication with the terminal TT, and a wireless communication circuit WCCT to allow the device HD**2** to connect to the Internet INW.

[0047] The device HD**2** may be a phone, a PDA (Personal Digital Assistant), an MP3 file reader, or any other portable device having the capability of connecting to the Internet. If it forms a phone, the device HD**2** also includes a secure processor PROC**2** of SIM card authorizing the subscriber to use the telephone network GSM. The circuit WCCT may be a radiotelephone circuit for connecting to the Internet via the network GSM, for example a Long Term Evolution connection LTE or a GSM 4G connection, a WiFi card, or any other wireless circuitry for connecting to the Internet.

[0048] The processor PROC**1** may be the main processor of the device HD**2**, for example a baseband processor if the device HD**2** is a mobile phone, or an auxiliary processor. The processor PROC**1** includes a central processing unit CPU, a communication interface ILR, and an operating system OS**1**.

[0049] The communication interface circuit ILR, schematically shown in the form of blocs, includes all the connection ports of the processor and software layers for managing the corresponding communication protocols.

[0050] The processor PROC**1** is linked to the controller NFCC, the processor PROC**2**, the circuit WCCT, the keyboard KB and the display DP through the interface circuit ILR. More particularly, the processor PROC**1** is linked to the controller NFCC through a bus BS**2** and a corresponding port of the interface circuit ILR. The bus BS**2** is for example a data bus I2C (Inter Integrated Circuit) or SPI (Serial Peripheral Interface).

[0051] The server SV**1** is configured to offer transaction services to users USRi (USR**1**, . . . USRn). It includes a security device SDV, a transaction service management program GST, and a memory area SM dedicated to the storage of transaction data and programs. The memory area SM is divided into sectors, each including a portfolio of cards CPi (CP**1**, . . . CPn). Each sector forming a portfolio of cards CPi is allocated to a user USRi and includes sub-sectors receiving virtual cards VCj (VC**1**, . . . VCm). Each user USRi subscribing to the transaction services offered by the server SV**1** has one or more virtual cards VCj within the portfolio of cards CPi which is allocated to him/her. Each virtual card VCj is configured to perform at least one transaction corresponding to a service, and thus emulate a payment card of a determined type, for example a payment card for the metro, the bus, the supermarket, or more generally a bank card for withdrawing or paying money. A virtual card VCj thus forms the equivalent of a material card, in combination with the portable device HD**2**. A portfolio of cards CPi thus forms the equivalent of a material portfolio in which the user would place one or more material cards.

[0052] Each virtual card VCj (VC**1**, . . . VCm) includes a virtual operating system VOSj (VOS**1**, . . . VOSm) and at least one card application CAPj (CAP**1**, . . . CAPm). From the perspective of the transaction protocol, each virtual card VCj is the functional equivalent of a conventional secure processor PROC**3** of the type previously described in relation with FIG. **2**, which was previously in the form of semiconductor chip.

[0053] In one embodiment, the virtual operating system VOSj is a program which emulates an operating system OS of conventional secure processor PROC**3**, while the card application CAPj is a conventional transaction program executable as well as by a conventional secure processor PROC**3** as by a virtual operating system VOSj.

[0054] In an equivalent embodiment, the virtual operating system VOSj does not emulate an operating system OS of conventional secure processor. The card application CAPj is not executable by a conventional secure processor and is only executable by the virtual operating system VOSj. The virtual operating system VOSj and the card application CAPj are specific programs configured to operate in combination and form, together, the equivalent of a conventional secure processor PROC**3** provided with a card application as far as performing a transaction is concerned.

[0055] In another equivalent embodiment, the virtual operating system VOSj is included in the card application CAPj, both programs forming a single one.

[0056] In one embodiment making a priority of the optimization of the server memory space, the virtual operating systems VOSj and the card applications CAPj of the various virtual cards VCj are emulated by one or more centralized programs executed by the server SV**1** in multitask mode. For example, a first central program emulates several operating systems at the same time and a second central program emulates the same card application for several virtual cards at the same time.

[0057] In a preferred embodiment making a priority of the security against fraud, the memory area SM contains as many virtual operating systems VOSj and card applications CAPj as virtual cards VCj. In other words, the sectors of the memory area SM containing the portfolios, and also the sub-sectors containing the virtual cards are totally partitioned in relation to one another and include no shared program operating in multitask mode.

[0058] In one embodiment, each card application CAPj uses an encryption key Kj(CAPj) which allows it to answer to authentication requests requiring a cryptographic calculation. In the embodiment emphasizing security and the partitioning of the sectors and sub-sectors of the memory area SM, the key Kj is stored in the sub-sector of the memory area SM receiving the memory card VCj which executes this application, i.e., receiving the virtual operating system VOSj and the card application CAPj together forming the virtual card.

[0059] The security device SDV protects the server and in particular the access to the memory area SM and the transaction service management program GST. The device SDV may be purely software and executed by the server SV**1**, or include a hardware part different from the hardware part of the server and a software part executed by the server or the different hardware part. It preferably includes a function of firewall and detection of fraud attempt to access a card application.

[0060] The transaction service management program GST, hereinafter referred to as "service manager," performs the creation, activation, update and suppression of virtual cards, with the help of the security device SDV which grants or not the authorizations to that purpose.

[0061] The server SV**1** uses the device HD**2** as a remote NFC interface allowing a virtual card VCi to perform a transaction with the terminal TT. To that end, the processor PROC**1** includes, in a program memory, an Internet browser BRW, a program WCL referred to as "web client" and a connection program CXP. The web client WCL is configured to establish a data link CX**1** with the server SV**1** through the browser BRW, the communication circuit WCCT (connection by telephone LTE for example, or WiFi connection) and the Internet INW. Once connected to the server, the web client WCL dialogs with the security device SDV or with the service manager GST, and shows to the user web pages, information or information requests emitted by them.

[0062] The data link CX**1** allows to the web client WCL to dialog with the security device SDV and the service manager GST, and is shown in dotted line in FIG. **4**. The data link CX**1** is preferably a secure connection using, for example, the conventional Secure Sockets Layers technology SSL based on a public key encryption method establishing a ciphered communication channel after an authentication step.

[0063] The connection program CXP is configured to perform establishing a second data link CX**2** between the controller NFCC and a virtual card VCj, through the bus BS**2**, the communication circuit WCCT and the Internet INW. In one embodiment, the data link CX**2** is established after receiving a connection request emitted by the web client WCL or the browser BRW. In another embodiment, the data link CX**2** is permanently established between the controller NFCC and the security device SDV. The device SDV renders the data link CX**2** accessible to a virtual card VCj at the time when the virtual card must perform a transaction.

[0064] Like the data link CX**1**, the data link CX**2** is preferably secure. The data link CX**2** is for example formed via http communication pipes (HyperText Transfer Protocol) or via a low level User Datagram Protocol link UDP so as to limit data exchange load. The data link CX**2** may also be encrypted with the SSL technology or via a proprietary coding.

[0065] In another variation, the controller NFCC is provided with circuitry for connecting to the Internet and a proprietary encryption system is provided in the program memory thereof. This method allows a point-to-point ciphered tunnel to be made between the server SV**1** and the controller NFCC and offers a very high security level which cannot be attacked by spy software which would have been inserted into the program memory of the processor PROC**1**. In such an embodiment, the connection program CXP may be arranged in the program memory of the controller NFCC, like schematically shown by a dotted line in FIG. **4**. In that case, the bus BS**2** is used to allow the program WCL to send to the controller NFCC a connection request to the server SV**1** at the beginning of a transaction step S**10** described below. An additional data bus may be provided to directly link the controller NFCC to the wireless communication circuit WCCT, without passing by the processor PROC**1**.

[0066] In another variation, a coprocessor dedicated to the communication establishment and encryption is provided. This coprocessor is linked to the controller NFCC and to the wireless communication circuit WCCT and allows a card application CAPj to take control of the controller NFCC without depending on the software of the processor PROC**1** and on a possible spy program that it may include.

[0067] In another variation, the portable device HD**2** includes a single processor both controlling the elements of the device HD**2** and controlling NFC transactions in relation with the transaction server SV**1**.

[0068] In brief, according to the embodiment chosen, the connection program CXP may be included into the web client WCL, be included into the operating system OS**1** of the processor PROC**1**, be included into a program memory or into the operating system of the controller NFCC, be executed by a dedicated coprocessor, or be executed by a single processor replacing the processor PROC**1** and the controller NFCC.

[0069] FIG. **5** shows an embodiment of a transaction method according to the invention, implemented via the transaction system of FIG. **4**.

[0070] It is assumed here that a user USRi is near the terminal TT and wishes to use the portable device HD**2** to perform a transaction. The user first activates the web client program WCL (Step S**1**), for example by pushing a key of the keyboard or selecting a menu shown on the display. The program WCL then asks the user to supply identification data USID**1**.

[0071] After inputting the data USID**1** (Step S**2**), the web client WCL connects to the security device SDV via the data link CX**1** and supplies identification data USID**2** thereto (Step S**3**). The data USID**2** include all or part of the identification data USID**1** and may include additional identification data such as data peculiar to the device HD**2** that the web client takes in a memory of the device HD**2**.

[0072] The identification data USID**1** may be varied and their aim is to guarantee a high level of security. They may include a login (user name or email) that the user must supply as well as a password. A security code sent by a bank to a user, for example via a message of the SMS type, may also be included in the data USID**1**. Biometric data (voice, face, fingerprints, or the like) and/or dynamic data specific to the user, for example user code input data (input stress on the keyboard, input time, or the like) may also be used as identification data USID**1**. These biometric or dynamic data makes it possible to check, in addition to checking the user code, that this code has been input by the right person.

[0073] The data USID**2** may include all or part of the data USID**1** and the additional data the user has supplied only once for the creation of his/her portfolio of cards CPi. It may be identity data such as the birth date, the identity card number, the passport number, the user home address, or the like. The data USID**2** may also include data peculiar to the device HD**2**, such as the user phone number, an identification number of the device, for example, if it is a phone, the IMEI number (International Mobile Equipment Identity) and the SIM card number.

[0074] The security device SDV then uses the data USID**2** to check the legitimacy of the connection request. If the check result is positive, the device SDV gives the service manager GST the user identity USRi and a service access authorization (Step S**4**). It also opens the data link CX**1** to the service manager GST, if it has not been done previously.

[0075] Then, the service manager GST accesses the user portfolio CPi and determines if virtual cards VCj and corresponding card applications CAPj have been installed therein (Step S**5**).

[0076] If this is the case, the manager GST presents to the user, via the web client, a list of services corresponding to the card applications CAPj installed (Step S**6**) and asks him/her to select the service s/he wishes to use to perform a transaction. The services are for example “access to the metro X,” “payment checkout at the supermarket Y,” “bank card Z,” or the like. This home page also offers other choices to the user, in particular the installation of a new virtual card and a corresponding card application, the implementation of this option being described hereinafter.

[0077] The user selects the service wanted (Step S**7**) and his/her choice (“card application CAPj selected”) is sent to the manager GST by the web client (Step S**8**).

[0078] In a variation of Steps S**7**, S**8**, the user only confirms his/her wish to perform a transaction without specifying the service desired. In this case, the adapted card application CAPj is automatically selected at the time of transaction.

[0079] The web client WCL then asks to the connection program CXP to establish the data link CX**2** between the server SV**1** and the controller NFCC, while the service manager GST selects and activates the virtual card VCj of the user and the card application CAPj that the user has designated (Step S**9**). The user brings the device HD**2** closer to the transaction terminal TT so that inductive coupling establishes between the antenna coils AC**2** and AC**3**. In another variation, the data link CX**2** is previously established between the security device SDV and the controller NFCC, and is simply rendered accessible to the card application CAPj by the device SDV after Step S**9**.

[0080] The virtual card VCj is then linked to the controller NFCC. A connection is established with the transaction terminal TT and the card application CAPj of the virtual card VCj executes the transaction requested (Step S**10**). This transaction may include actions of the user, such as accepting an amount or choosing a product. Although it is not shown in FIG. **5**, the transaction terminal TT may also be linked to a bank server SV**0** (Cf. FIG. **4**) which requires authentication steps and checks that all the answers to authentication requests have really been sent by a card application using an authorized bank key.

[0081] When the transaction is over, the data link CX**2** is closed, the virtual card VCj is deactivated and the manager GST sends to the web client WCL information about the transaction performed, for example the object and amount of the transaction (Step S**11**). The web client may memorize and present the information to the user.

[0082] Those skilled in the art will note that the transaction method and the transaction system which have just been described are susceptible of other variations. In particular, the web client WCL is a “head-up” program which uses web pages or data supplied by the server SV**1** to form a user interface. Such a program may not be necessary. In this case, the user directly dialogs with the security device SDV and the service manager GST through web pages that both elements show him/her via the browser BRW.

[0083] FIG. **6** shows an example of transaction performed at Step S**10**. The transaction includes:

[0084] i) A pipe P**1** is created between the virtual card VCj and a technology RFTi executed by the controller NFCC, via commands “PIPE_CREATE,” “PIPE_OPEN.” This step may be performed by the connection program CXP, as shown. Alternately, this step may be performed by the virtual card VCj itself, if it includes a program for managing the interface HCI, or by the security device SDV. It is to be noted that the pipe P**1**, here complying with the protocol HCP, is established through the data link CX**2** which passes through the Internet and the bus BS**2**;

[0085] ii) The controller NFCC detects the magnetic field emitted by the terminal TT and sends the command EVT_FIELD_ON to the virtual card VCj;

[0086] iii) The controller NFCC performs steps for initializing a communication with the terminal TT including creating a NFC communication pipe (referred to as “RFCH” in FIG. **6**, or RF pipe) as well as possible steps of anticollision if other NFC devices or contactless cards are located in the interrogation field of the terminal TT (step “INIT, ANTICOL”);

[0087] iv) When the connection with the terminal TT is established, the controller NFCC sends a command EVT_CARD_ACTIVATED to the virtual card VCj to indicate to it that a transaction can begin.

[0088] The actual transaction then includes the following steps:

[0089] sending commands CAPDU by the terminal TT to the processor NFCC, via the communication pipe RF;

[0090] transmitting these commands to the card application CAPj of the virtual card VCj by the controller NFCC, through the pipe P**1**, in an encapsulated form into commands EVT_SEND_DATA;

[0091] sending to the controller NFCC, by the card application CAPj of the virtual card VCj, answers RAPDU, via the pipe P**1**, in an encapsulated form into commands EVT_SEND_DATA; and

[0092] transmitting the answers RAPDU to the terminal TT by the controller NFCC, via the pipe RF.

[0093] The commands CAPDU and the answers RAPDU (usually referred to as “C-APDU” and “R-APDU”) are defined by the standard ISO 7816-4. In a variation of the transaction, encapsulating the commands CAPDU and the answers RAPDU is performed via the http protocol instead of using encapsulation commands EVT_SEND_DATA.

[0094] The first command CAPDU sent by the terminal TT may be a command for selecting the card application CAPj, for example the command "SELECT_AID" such as defined by the standard ISO 7816-4. If the card application has previously been selected by the user at Step S**7** and if this application does not correspond to that requested by the transaction terminal TT, the virtual card VCj sends an error message and the transaction is interrupted.

[0095] In the variation of Step S**7** described above, where the user only confirms his/her wish to perform a transaction without selecting a determined virtual card, the virtual card containing the adapted card application is automatically selected by a card selection program included in the portfolio of cards of the user. At the beginning of Step S**10**, this high level program performs the initial activation of the card application gate CAG and the creation of the pipe P**1** so as to receive the command for selecting the card application. It then activates the card application designated by the command, if it is installed in the portfolio of cards. If not, the transaction is interrupted.

[0096] When the transaction is over (or interrupted), the terminal TT stops emitting the magnetic field and the controller NFCC sends to the virtual card VCj a command EVT_CARD_DEACTIVATED for deactivating the card application and a command EVT_FIELD_OFF indicating that the magnetic field is no longer present. The pipe P**1** is then closed between the virtual card VCj and the controller NFCC, via a command "PIPE_CLOSE." This step of closing the pipe P**1** may be performed by the virtual card VCj itself or the connection program CXP, as shown. Alternately, this step may be performed by the security device SDV. The service manager GST then executes Step Sll described above (FIG. **7**).

[0097] Those skilled in the art will note that this example of transaction through an interface HCI is not limiting. The connection between the virtual card VCj and the controller NFCC may be established via various other protocols and other commands may be provided.

[0098] The example of transaction which has just been described presupposes on the one hand that the user USRi has a portfolio of cards CPi and, on the other hand that the portfolio contains at least the virtual card VCj necessary for this transaction.

[0099] FIG. **7** shows an embodiment of a method for creating a portfolio of cards CPi. It is assumed that the user USRi first connects to the service manager GST as a non registered user, via an Internet connection. The manager GST then supplies to the device HD**2** a home page for non registered users, in which the user is offered to subscribe to the transaction services (Step S**20**). The acceptance by the user of the offer here triggers the download and installation of the web client WCL in the device HD**2** (Step S**21**). The web client WCL connects to the manager GST (Step S**22**) via the data link CX**1** and the manager GST sends to the user a registering page (Step S**23**) in which information is requested, to form the identification data USID**1**. In addition to these data, the user may be invited to communicate his/her bank details and any additional data allowing the data USID**2** to be defined. The web client may also take in the device HD**2** data specific to it, intended to form data USID**2**.

[0100] When the web client WCL has all the data USID**1** and USID**2** (Step S**24**) and possible other information necessary for the user to subscribe, it supplies the data USID**2** to the security device SDV (Step S**25**). The security device SDV then checks the identification data USID**2**, determines if the user USRi can be authorized to have a portfolio of cards, and sends an authorization for creating the portfolio to the service manager GST (Step S**26**).

[0101] The manager GST then creates the portfolio CPi (Step S**27**). In practice, this creation may simply consist in registering the user in a database containing the identification data USID**2** and a look-up table indicating the sector of the memory area SM allocated to the user.

[0102] The manager GST then sends to the device HD**2** a confirmation of creation of the portfolio CPi (Step S**30**).

[0103] FIG. **8** shows an embodiment of a method for acquiring a virtual card VCj. This method can be initiated after Step S**28** previously described or, as shown in FIG. **8**, after a new connection to the server SV**1**. This new connection includes the steps previously described i.e.:

[0104] activating the web client (Step S**1**),

[0105] inputting the data USID**1** (Step S**2**),

[0106] sending the data USID**2** to the security device SDV by the web client (Step S**3**), to check the legitimacy of the connection request,

[0107] checking the legitimacy of the connection request by the security device and communicating to the manager GST an access authorization (Step S**4**),

[0108] accessing the portfolio CPi by the manager GST and determining the card applications CAPj which have been installed therein (Step S**5**),

[0109] sending the user a list of the card applications CAPj installed, as well as a suggestion of installation of a new card application (Step S**6**).

[0110] It is assumed here that the user selects the option "installation of a new application" (Step S**12**) instead of selecting an application (Step S**7**, FIG. **5**), because s/he does not have any application installed or because s/he wishes to install a new one.

[0111] The web client sends the new application request to the service manager GST (Step S **13**). The following steps imply one or more bank servers, or certification servers, or preferably a single certification server BSV gathering the services of one or more banks. Before processing the request of installation of a new application, the service manager GST may have previously received from the certification server BSV an offer of applications CAPj (Step SO).

[0112] The service manager GST thus sends to the device HD**2** a page of offer of card applications CAPj presented in the form of an offer of transaction services (Step S**30**).

[0113] The user then selects a transaction service, which corresponds to the selection of a card application CAPj (Step S**31**). His/her choice is sent to the manager GST by the web client (Step S**32**).

[0114] The manager GST then provides the server BSV with the user identification data USID**2** as well as an identifier of the card application CAPj requested (Step S**33**), and requires an authorization for creating the corresponding virtual card. This step may include multiple accesses to the bank server. It may possibly be delayed if the certification server indicates that the user must previously be contacted by commercial attachés to perform some procedures. Conversely, the user may have already performed the procedures and supplied in the data USID**1** a code received from the bank, which authorizes him/her to obtain the card.

[0115] After checking, the server BSV sends to the manager GST the program of the card application and an activation bank key Kj(CAPj) allowing the card application to be used (Step S**34**). This key forms an encryption key allowing the application to authenticate to a transaction terminal, when it is requested thereto. The manager GST then creates the virtual card VCj in the portfolio CPi, and installs if need be the virtual operating system VOSj of the card, and then installs the application CAPj in the virtual card VCj, and installs the key Kj (Step S**35**).

[0116] In a variation, various card applications CAPj are memorized in a space for storing applications of the manager GST and the certification server supplies only the activation key Kj.

[0117] The manager GST then returns to Step S**6** to present to the user a list of the card applications CAPj installed, as well as a suggestion of installation of a new card application. The user may decide to install a new application again, to use the one which has just been installed or an application previously installed, or to disconnect from the server SV**1**.

[0118] In a variation, the manager GST does not have any right to modify virtual cards VCj and steps S**33**, S**34** and S**35** are left to the security device SDV.

[0119] The example of a transaction system which has just been described is susceptible of various other embodiments. In particular, embodiments of the transaction system may relate to the virtualization of a payment point implementing a payment point application instead of a card application. A payment point application PAPj differs from a card application CAPj in that the aim thereof is to collect an amount of money through a transaction with a chip card allowing the payer to be identified.

[0120] FIG. **9** shows a transaction system which has, in relation to that of FIG. **4**, the following differences:

[0121] the device HD**2**, instead of being arranged facing a transaction terminal TT, is arranged facing a contactless card CC**1** including an antenna coil AC**1** and a contactless integrated circuit CIC, and performs a transaction with it;

[0122] the server SV**1**, instead of managing card applications CAPj arranged in virtual cards VCj, which are arranged in portfolios of cards CPi, manages payment point applications PAPj (PAP**1**, . . . PAPm) arranged in virtual payment points VPj (VP**1**, . . . VPm), which are arranged in portfolios of payment points PPi (PP**1**, . . . PPn) allocated to users USRi. Each virtual payment point may include, in addition to a payment point application PAPj, a program VOSj (VOS**1**, . . . VOSm) for emulating an operating system of a payment terminal, which may also be included into the payment point application PAPj.

[0123] By analogy with the conventional transaction system shown in FIG. **1**, the device HD**2** acts here as transaction terminal TT. The controller NFCC emits the magnetic field FLD required to establish a contactless communication pipe with the card CC**1**. The payment point application program PAPj takes the control of the controller NFCC to perform the transaction. It emits commands CAPDU and receives answers RAPDU. The payment point application program PAPj may be configured to connect, during or after the transaction, to a bank authorization server such as the server SV**0** shown in FIG. **1**.

[0124] The method shown in FIG. **5** may be adapted for performing a transaction in payment point mode, by activating at Step S**10** a payment point application PAPj instead of a card application CAPj, and by searching at Step S**5** for the virtual payment points VPj installed in the portfolio PPi of a user USRi. At Step S**6**, the method may include the presentation of a list of available payment point applications PAPj instead of the presentation of a list of card applications CAPj, or a presentation of both types of transaction services. Eventually, the method shown in FIG. **7** may be adapted to the creation of a portfolio of payment points PPi instead of a portfolio of cards CPi. Likewise, the method shown in FIG. **8** may be modified so that Steps S**31** to S**35** relate to the installation of a payment point application and a virtual payment point.

[0125] FIG. **10** shows an example of transaction performed between a virtual payment point VPj and the contactless card CC**1**, which is implied for example at Step S**10** of the method of FIG. **5** adapted for performing a transaction in payment point mode. The transaction includes the following steps:

[0126] i) A pipe P**2** is created between the virtual payment point VPj and a technology RFTi executed by the controller NFCC, via commands "PIPE_CREATE," "PIPE_OPEN." This step may be performed by the connection program CXP, as shown. Alternately, this step may be performed by the virtual payment point VPj itself, if it includes a program for managing the interface HCI, or by the security device SDV, before it renders the data link CX**2** accessible to the virtual payment point VPj;

[0127] ii) Sending to the controller NFCC interrogation commands EVT_READER_REQUESTED which aim is to detect the presence of the contactless integrated circuit CIC (interrogation method called "polling"). This step may be performed by the virtual payment point VPj, as shown. Alternately, this step may be performed by the connection program CXP, or by the security device SDV, before it renders the data link CX**2** accessible to the virtual payment point VPj;

[0128] iii) When the contactless integrated circuit CIC of the card CC**1** is detected, the controller NFCC performs the steps "INIT, ANTICOL" for initializing a communication with the contactless integrated circuit CIC including the creation of a communication pipe RF (referred to as RFCH in FIG. **10**), and optionally anticollision steps (if other contactless integrated circuits are present in the field),

[0129] The controller NFCC sends the command EVT_TARGET_DISCOVERED to the virtual payment point VPj to indicate thereto that a transaction can begin.

[0130] The actual transaction then includes the following steps:

[0131] Sending to the controller NFCC, by the virtual payment point application PAPj, commands CAPDU, via the pipe P**2**, the commands CAPDU being encapsulated into commands WR_XCHG_DATA,

[0132] Transmitting by the controller NFCC commands CAPDU to the contactless integrated circuit CIC, through the pipe RF,

[0133] Sending to the controller NFCC, by the contactless integrated circuit CIC, answers RAPDU,

[0134] Transmitting the answers RAPDU to the virtual payment point application PAPj, by the controller NFCC, via the pipe P**2**, the answers RAPDU being encapsulated into commands WR_XCHG_DATA.

[0135] The transaction is closed when the command EVT_END_OPERATION is sent to the controller NFCC. This step may be performed by the virtual payment point VPj, as shown. Alternately, this step may be performed by the connection program CXP, or by the security device SDV, before it renders the data link CX**2** accessible to the virtual payment point VPj;

[0136] The pipe P**2** is then closed via a command "PIPE_CLOSE." This step may be performed by the connection program CXP, as shown. Alternately, this step may be performed by the virtual payment point VPj itself, if it includes a program for managing the interface HCI, or by the security device SDV.

[0137] The transaction system shown in FIG. **9** is susceptible of different variations. For example, the contactless card CC**1** may be replaced by another portable device HD**2**' which operates in the card emulation mode, such as previously described with reference to FIGS. **5** and **6**. If the same server SV**1** manages both card applications and payment point applications, both portable devices HD**2**, HD**2**' facing each other may execute a transaction, one as card, or payer, and the other as payment point, or receiver, while being simultaneously connected to the same server SV**1**. A transaction system according to the invention may therefore allow private transactions to be performed, for example a transfer of an amount of money from a person to another via their mobile phones.

[0138] Eventually, it is to be noted that the device HD**2** used before to perform a transaction with a transaction device such as the terminal TT (FIG. **4**) or the contactless card CC**1** (FIG. **9**), may be different from a mobile phone, a PDA or any other portable object generally used for other purposes than near field transactions. Thus, in some embodiments, the device HD**2** may be entirely dedicated to perform near field transactions and include a low cost simplified controller provided with near field communication circuitry and circuitry for connecting to the server and mainly configured to act as proximity relay between the server and the transaction device. To allow the user to choose between the transaction services offered by the server, such a low cost device may be provided with simplified keyboard and screen including minimum functionalities allowing the user to make his/her choices. In some embodiments, this low cost "relay device" may include no way to interface with the user, the choice of the adapted virtual card being automatically made by the server at the time of the transaction. In this case, it may be offered to the user to connect to the server via another device, for example a personal computer, to configure the portfolio of virtual cards or virtual payment points it has, by adding thereto or deleting cards or payment points.

[0139] It will be appreciated by those skilled in the art that changes could be made to the embodiments described above without departing from the broad inventive concept thereof. It is understood, therefore, that this invention is not limited to the particular embodiments disclosed, but it is intended to cover modifications within the spirit and scope of the present invention as defined by the appended claims.

I claim:

1. A method for performing a transaction between a portable device and a transaction device, the method comprising:

providing at least one transaction server comprising at least one application program configured to receive, process and emit application data,

establishing at least one data link between the portable device and the transaction server,

establishing a near field communication channel between the portable device and the transaction device, and

via the portable device:

transferring to the application program of the server application data sent by the transaction device, and

receiving application data sent by the application program of the server and transferring them to the transaction device.

2. The method according to claim **1**, further comprising installing in the transaction server at least one application program configured to emulate a chip card.

3. The method according to claim **1**, further comprising installing in the transaction server at least one application program configured to emulate a payment point in order to perform a transaction with a chip card.

4. The method according to claim **1**, further comprising:

via the portable device, receiving from the server a choice of available transaction services and supplying to the server a selection of at least one transaction service, and

activating in the server an application program corresponding to the transaction service selected and linking the application program to the portable device so that the application program performs the transaction.

5. The method according to claim **1**, further comprising:

via the portable device, receiving from the server an offer of transaction services and supplying to the server a selection of at least one transaction service, and

installing in the server an application program corresponding to the transaction service selected.

6. The method according to claim **5**, wherein installing the application program comprises installing an encryption key allocated to the application program.

7. The method according to claim **1**, further comprising:

via the portable device, receiving from the server an offer for subscribing to transaction services and supplying to the server an acceptance of the subscription offer comprising identification data for identifying a user,

allocating a memory area of the server to the identified user, and

storing in the memory area a portfolio of applications allocated to the user (USRi).

8. A transaction system comprising a portable device and a transaction device, each comprising near field communication circuitry, the portable device comprising wireless communication circuitry,

wherein the system further comprises at least one transaction server accessible via an Internet network, comprising at least one application program configured to receive, process and emit application data during a transaction,

the portable device being configured to:

establish at least one data link with the transaction server (SV**1**) through the wireless communication circuitry,

establish a near field communication channel with the transaction device,

transfer to the application program of the server application data sent by the transaction device, and

receive application data sent by the application program of the server and transfer the application data to the transaction device.

9. The transaction system according to claim **8**, wherein the transaction server comprises at least one card application program configured to emulate a payment card.

10. The transaction system according to claim **8**, wherein the transaction server comprises at least one application program configured to emulate a payment point able to debit a payment card.

11. The transaction system according to claim **8**, wherein:

the portable device is configured to receive from the server a choice of available transaction services, and supply to the server a selection of at least one transaction service, and the server comprises a service management program configured to, in response to the selection of at least one transaction service, activate in the server an application program (corresponding to the transaction service selected.

12. The transaction system according to claim **8**, wherein:

the portable device is configured to receive from the server an offer of transaction services and supply to the server a selection of at least one transaction service, and

the server comprises a service management program configured to, in response to the selection of at least one transaction service, install in the server an application program corresponding to the transaction service selected.

13. The transaction system according to claim **12**, wherein the service management program is configured to, during the installation of an application program, also install an encryption key allocated to the application program.

14. The transaction system according to claim **8**, wherein:

the portable device is configured to receive from the server an offer for subscribing to transaction services and supply to the server an acceptance of the subscription offer comprising identification data for identifying a user, and

the server comprises at least one service management program configured to:

allocate a memory area of the server to the identified user, and

store in the memory area a portfolio of applications allocated to the user.

15. The transaction system according to claim **8**, wherein the transaction server comprises or is associated to a security and access control device or program configured to authorize the access to transaction services only after the portable device has supplied valid authentication data of a user.

16. A portable device comprising near field communication circuitry and wireless communication circuitry,

is the portable device being configured to:

establish at least one data link with a transaction server through the wireless communication circuitry,

establish a near field communication channel with the transaction device, through the near field communication circuitry,

transfer to the server application data sent by the transaction device, and

receive application data sent by the server and transfer them to the transaction device.

17. The portable device according to claim **16**, configured to receive from the server a choice of available transaction services, and supply to the server a selection of at least one transaction service to be activated in the server to perform a transaction.

* * * * *