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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 June 2009 (11.06.2009)

PCT

(10) International Publication Number
WO 2009/071734 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *G06Q 20/00* (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/FI2007/000288

(22) International Filing Date:
7 December 2007 (07.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FI-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VEPSÄLÄINEN, Ari** [FI/FI]; Tikasniityntie 11, FI-02200 Espoo (FI). **SANDRINI, Marco** [IT/FI]; Neitojenranta 1 A 17, FI-00810 Helsinki (FI).

(74) Agent: **BERGGREN OY AB**; P.O. Box 16 (Antinkatu 3 C), FI-00101 Helsinki (FI).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,

[Continued on next page]

(54) Title: TRANSACTION AUTHENTICATION

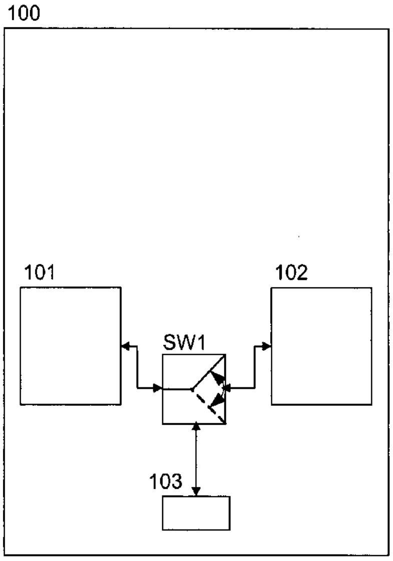

Fig.1

(57) Abstract: Various embodiments of the invention provide blocks or modules for a transaction to request authentication information regarding the user of the apparatus by way of switching from the transaction protocol, for example ISO-14443 communication, to peer-to-peer communications protocol, for example NFC-IP, and requesting user authentication information from the apparatus. The transaction can be authenticated accordingly. The authentication information may include, according to at least one embodiment, an image of the user or like, but also other kind of information that can be used as a proof of authenticity of the person using the apparatus can be used as well.

PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

Transaction Authentication

TECHNICAL FIELD OF THE INVENTION

The invention concerns an apparatus comprising an interface arranged to conduct a transaction via a short-range communications interface. Furthermore the invention concerns a wireless apparatus comprising an interface arranged to conduct a transaction via the short-range communications interface. Yet furthermore the invention concerns a method for operating the apparatuses. Yet furthermore the invention concerns a computer program arranged to perform operations of the method when stored and run on a computer.

BACKGROUND

Modern society has quickly adopted, and become reliant upon, handheld apparatuses for wireless communication. For example, cellular telephones continue to proliferate in the global marketplace due to technological improvements in both the communication quality and device functionality. These wireless communication apparatuses have become common for both personal and business use, allowing users to transmit and receive voice, text and graphical data from a multitude of geographic locations. The communication networks utilized by these apparatuses span different frequencies and cover different transmission distances, each having strengths desirable for various applications. The wireless communication apparatuses can communicate with short-range and wide area wireless communications networks.

Short-range wireless networks provide communication solutions that avoid some of the problems seen in large cellular·networks. Bluetooth^{TM} is an example of a short-range wireless technology quickly gaining acceptance in the marketplace. A 1 Mbps Bluetooth^{TM} radio may transmit and receives data at a rate of 720 Kbps within a range of 10 meters, and may transmit up to 100 meters with additional power boosting. Enhanced data rate (EDR) technology also available may enable maximum asymmetric data rates of 1448 Kbps for a 2 Mbps connection and 2178 Kbps for a 3 Mbps connection. A user does not actively instigate a Bluetooth^{TM} network. Instead, a plurality of devices within operating range of each other may automatically form a network group called a "piconet". Any apparatus may promote itself to the master of the piconet, allowing it to control data exchanges with up to seven "active" slaves and 255 "parked" slaves. Active slaves exchange data based on the clock timing of the master. Parked slaves monitor a beacon signal in order to stay synchronized with the master. These apparatuses continually switch between various active communication and power saving modes in order to transmit data to other piconet members. In addition to Bluetooth^{TM} other popular short-range wireless networks include WLAN (of which "Wi-Fi" local access points communicating in accordance with the IEEE 802.11 standard, is an example), WUSB, UWB and ZigBee (802.15.4, 802.15.4a). All of these wireless mediums have features and advantages that make them appropriate for various applications.

In addition to the above, near field communications technologies, which can be considered for providing very short-range or near to touch communication technologies, have become more interesting lately for providing new use and functionality to wireless communication devices. An example of near field communications technologies comprise Radio Frequency Identification (RFID) technology, which already exists in various consumers applications from transportation and payment systems to various identification systems including implantable RFID tags. Near Field Communication (NFC), is yet another short-range wireless communication technology, which enables the exchange of data between devices over a short distance. The technology is based on RFID, which makes it compatible with the existing contactless infrastructure already in use for public transportation and payment. Near Field Communication (NFC) Forum is a non-profit industry association that promotes the use of NFC short-range wireless interaction in various consumer electronics, wireless devices and PCs. The NFC Forum supports implementation and standardization of NFC technology to make it easier to get information, easier to pay for goods and services, easier to use public transport, and easier to share data between devices.

Payment and ticket applications are considered as one of the most important emerging usage areas that will leverage in the near field communications technologies field, such as, for example radio frequency identification (RFID) technology. For instance, a wireless device, such as, for example, a mobile phone implementing a radio frequency identification (RFID) transponder may be utilized to provide/present a digitally coded or electronic ticket, which has been obtained before, to a ticket checkpoint system of an entrance of a public transportation system. The digitally coded ticket is read out by corresponding radio frequency identification (RFID) reader, with which the checkpoint system is equipped, and is analyzed thereby. In case of validity of the digitally coded ticket the access to the public transportation system is granted to the owner of the portable terminal. The digitally coded tickets are not necessarily only a piece of code. They may also include authentication information, such as for instance in case of 30 travel tickets, wherein the actual purchase of a ticket may need to be included in the ticketing application, so that an inspector notices that the person has actually purchased those tickets.

Advantageously, such a ticket checkpoint system may be available for public transportation systems in various cities, which may result in the requirement for coding different digitally coded tickets. Moreover, the illustrated ticket checkpoint system may be extended to similar digitally coded records such as credit card information, loyalty card information, cinema tickets and the like, where the portable terminal performs information exchange with the very same equipment, e.g. point-of-sale equipment. The same applications may be realized by using optical or visual codes presented by an optical or visual encoding means and an optical or visual scanning means allowing for reading-out the optical or visual codes from the optical or visual encoding means.

In combination with the above-mentioned technology the usage of smartcards is steadily growing. Modern smartcards provide application developer with a secure and tamperproof environment for developing high value, secure and complex applications. Said smartcards include a central processing unit as well as secure memory areas making unwanted access by third parties very difficult. Further, cryptographic means are provided within the smartcard, which opens the deployment of smartcards for secure applications like banking or even personal identification applications.

Usually, smart cards create a secure environment for storing items of monetary value while the contactless feature is fast and convenient for users who only need to bring the card in close proximity to a card reader. These types of contactless cards do not require a Personal Identification Number (PIN) and are therefore suited for high-volume, low-value transactions. Users of the card can load value onto the card by using an Automated Teller Machine (ATM) or a kiosk to transfer money from a checking account, savings account, a credit card account or by inserting cash into the ATM. The user puts their ATM card or cash into the machine and positions a contactless card near the contactless reader/writer to complete the transfer of money. These ATMs are typically located at the entrance to the transit station where the customers purchase transit tokens. The popularity of contactless cards for transit has grown so that other vendors in area surrounding the transit system also accept the contactless card for payment for purchases such as parking, fast food, convenience stores, gas stations and vending machines. Many merchants are installing contactless smart card reader/writers in their stores to provide the ability to accept smart cards as a form of payment. It shall be appreciated that the above-mentioned embodiments regarding smartcards are only given to explain possible deployments of smartcards without any limiting intention. It is also imaginable that smartcards may be used in connection with credit card and debit transactions with dynamic value, for instance.

A wireless apparatus, such as, for example a mobile phone may contain a NFC module or other type of near field communications module. Furthermore the apparatus may contain a secure element such as a secure smart card. The secure element is used in association with the near field communications module to carry out acts that require trust and confident. Examples of these kinds of acts may be a payment, electronic payment, true identification, credit card, secure transaction, electronic ticket purchasing and validation etc. Another example can be a payment made by a mobile phone. A real authentication is however a problem with transaction related acts when the actual transaction operations are conducted electronically, such as, for example in connection with transaction operations involving the secure smart card. The transaction itself can be carried out quite easily and conveniently by the system nowadays. However, when an authentication involving the person carrying the wireless apparatus needs to be done, a known solution is to carry it out by non-electric means. For example by personally demonstrating a personal identification card such as a passport. Another known solution is to make a personal signature by hand. Yet another known solution is to enter a personal identification code matching with the secure element by hand with a keypad. Yet another solution is to conduct the authentication by way of biometric identification of the user. A common problem for these and any similar or equivalent known solutions is that the authentication involving the person carrying the wireless apparatus requires taking an effort by said person. For example, a user has to make the effort, e.g. prove his identity by showing an id etc. Thus, while the electric transaction itself is rather convenient, the authentication fails with this respect. Furthermore it's generally a problem to really discover that the performing party of the transaction is an authenticated one.

SUMMARY

It is the object of the invention to provide the apparatus with more convenient authentication.

In accordance with an aspect of the invention there is provided an apparatus, comprising:

a controller;

a near field communications module operatively coupled to the controller;

a first secure storage location operatively coupled to the controller and configured to store at least partly information for carrying out a transaction operation by way of a transaction communications protocol via the near field communications module; and

a second secure storage location operatively coupled to the controller and configured to store at least authentication information regarding authentic user of the apparatus;

wherein the controller is configured to switch communications from said transaction communications protocol to another communications protocol in response to detecting that said transaction is substantially carried out and communicate the at least authentication information regarding the authentic user of the apparatus via the another communications protocol.

In accordance with another aspect of the invention there is provided a wireless apparatus, comprising:

a controller;

a near field communications module operatively coupled to the controller;

a first secure storage location operatively coupled to the controller and configured to store at least partly information for carrying out a transaction operation by way of a transaction communications protocol via the near field communications module; and

a second secure storage location operatively coupled to the controller and configured to store at least authentication information regarding authentic user of the apparatus;

wherein the controller is configured to switch communication from said transaction communications protocol to another communications protocol in response to detecting that said transaction is substantially carried out and communicate the at least authentication information regarding the authentic user of the wireless apparatus via the another communications protocol.

In accordance with yet another aspect of the invention there is provided a method, comprising:

conducting substantially a transaction by exchanging transaction information via a first communications protocol,

switching to a second communications protocol upon detecting that the transaction is substantially conducted, and

finalizing the transaction by exchanging authentication information via the second communications protocol.

In accordance with yet another aspect of the invention there is provided a computer program code, wherein the computer program code is arranged to

conducting substantially a transaction by exchanging transaction information via a first communications protocol,

switching to a second communications protocol upon detecting that the transaction is substantially conducted, and

finalizing the transaction by exchanging authentication information via the second communications protocol.

In various embodiments of the invention there is no need to tamper the communication protocol that relates to the transaction. This is advantageous because such a protocol tend to be very protected and confident due to the nature of appliance. Furthermore various embodiments may take advantage of existing authentication of the apparatus as well as existing wireless transactions. Various embodiments are trust and reliable by combining the clumsy but secure transaction procedure with improved authenticity.

BRIEF DESCRIPTION OF THE DRAWINGS

Various further embodiments of the invention will now be described, by way of examples only, with reference to the accompanying drawings, in which:

Figure 1 depicts a block diagram of an apparatus in which general principles of the various embodiment of the invention can be applied,

Figure 2 depicts a block diagram of an apparatus having a switch configured to switch the protocol between the secure transaction element and the authentication module of the apparatus according to various further embodiments of the invention,

Figure 3 depicts a flow chart of the operations of the apparatus according to various further embodiments of the invention, and

Figure 4 depicts schematically a block diagram including functional and structural components of the apparatus according to some further embodiments of the invention.

DESCRIPTION OF FURTHER EMBODIMENTS

As previously referred figure 1 depicts a block diagram of an apparatus 100 in which general principles of various further embodiments of the invention can be applied. The apparatus 100 comprises a first secure storage location 101 such as a transaction element 101. The transaction element 101 may be, according to at least one embodiment, a secure smart card element configured for transaction operations for example. The secure transaction element 101 is arranged to communicate by a first communications protocol. Furthermore the apparatus comprises a second secure storage location 102 such as an authentication module 102. The authentication module 102 can be a smart card of the apparatus 100 for authentication. The authentication module 102 is arranged to communicate by a second communications protocol. The apparatus 100 comprises also a near field communications module 103, which can be alternatively referred to as as a short-range communications module. The apparatus, according to at least one embodiment, comprises also a controller SW1, which is coupled with the secure transaction element 101. The controller SW 1 is also coupled with the authentication module 102 and with the near field communications module 103. The controller SW1, according to at least one embodiment, is configured to switch communications from the first communications protocol to the second communications protocol once it is detected that a transaction operation is substantially carried out so as to provide means to authenticate a user of the apparatus responsible for carrying out the transaction using said another communications protocol. The authentication relating to the transaction is carried out on a basis of the authentication of the user of the apparatus. The apparatus 100 may contain hardware, software and/or middleware for carrying out the operations of various embodiments. Thus the apparatus 100 has computer code and/or the hardware for performing the operations of further embodiments.

In various further embodiments, the apparatus 100 may be a wireless radio frequency apparatus having a near field and/or a short range wireless communication capability. The apparatus 100 can be, according to a further embodiment, a mobile phone containing near field communications capability.

Various embodiments of the invention provide blocks or modules for a cashier/ticketing inspector to request authentication information regarding the user of the apparatus 100 by way of switching from the transaction protocol (for example ISO-14443 communication) to peer-to-peer communications (for example NFC-IP) and requesting user authentication information from the apparatus 100. The authentication information may include, according to at least one embodiment, an image of the user or like, but also other kind of information that can be used as a proof of authenticity of the person using the apparatus 100 can be used as well.

The authentication information is typically secured and may be, according to at least one embodiment, stored e.g. in the authentication module 102 in a secure memory location, such as, for example within a secure smart card (for example SIM card in case of a mobile phone). It should be also noted that in accordance of at least one further embodiment of the invention, the secure transaction element 101 effecting the transaction may be located within a certain memory area of a secure smart card 102, such as, for example SIM card in a mobile phone apparatus.

In some further embodiments of the invention, the authentication information (e.g. the image of the owner of the apparatus or like) can be secured by way of for example signing the authentication information with secure key of some reliable account provider. For example, according to at least one embodiment, a credit issuing company, such as, for example MasterCard may provide, in addition to actual payment application within the secure smart card element 102, also a secure signing of the authentication information with its secure key so that the authentication information can also be secured to prevent potential misuse. When the authentication information is provided to the cashier/ticketing inspector, it is conformed with the public key corresponding to the secure key so that the authentication information cannot be hacked. Further, in order to edit or update the authentication information that is accessible only via an entity, such as, for example the MasterCard, the user of the apparatus needs to first sign in and authenticate oneself to e.g. the entity via e.g. the entity's web pages, and only after the user is signed in, and authenticated, the user is provided an opportunity to amend or change the authentication information of the apparatus. This kind of feature is especially suitable in situations where the apparatus is sold to another person and the ticketing information needs to be updated so that the new user can utilize his/her own tickets etc. after purchase of the apparatus while ensuring that the person selling the apparatus doesn't loose his/her tickets in connection with the transaction.

Figure 2 depicts a block diagram of an apparatus 100' having a controller SW1' configured to switch the protocol between the secure transaction element 101' and the authentication module 102' of the apparatus 100' according to various further embodiments of the invention. Thus referring now to the Figure 2 there is being shown an example of an apparatus 100' according to various embodiments of the invention. The apparatus 100' comprises the secure transaction element 101'. Furthermore the apparatus 100' comprises near field communications module 103', a CPU, and an authentication module 102', such as, for example the SIM of the apparatus 100'. The secure transaction smart card element/module 101' is connected via the controller SW1' either to a near field communication NFC 103' interface providing connectivity with external devices by means of using for example RFID or optical connection. Alternatively, the secure transaction smart card element/module 101' is connected via the controller SW1' with a terminal CPU for providing control to the secure smart card element 101'. The NFC 103' interface allows both reading and writing operations to be conducted both to and from external tags/devices and also peer-to-peer type communication between two NFC terminals. The secure transaction smart card element 101' is directly linked to the NFC 103' interface by means of the controller SW1', in order to ensure that there will be no unnecessary delays within terminal logic that might hinder/prevent transactions due to the nature of RFID communications, which will typically require fast response times. An RFID transaction, for instance, will be typically conducted within, e.g., hundreds of milliseconds. The secure element 101' is thus connected with the controller SW1'. Furthermore the controller SW1' is connected with the near field communications module 103'. Also the CPU is connected to the SW1' and also to the NFC module 103'. The controller SW1' may switch communications to the authentication module 102'. The authentication module 102' applies another communications protocol than the secure element 101'. Once the transaction by the secure element 101' is substantially carried out, the CPU instructs the controller SW1' to switch to another communications protocol and further to the authentication module 102'. Apparatus 100' comprises also a memory which is connected with CPU. Furthermore the apparatus 100' may comprise a short-range transceiver which is coupled with CPU. Apparatus 100' comprises a network receiver which is couples with CPU. Furthermore the apparatus 100' comprises application storage which is coupled with a CPU. Furthermore the application storage may be coupled directly with the secure transaction element 101'. The apparatus comprises also a display which is coupled with the previous components. Furthermore the apparatus comprises an antenna which is coupled with the network transceiver and possibly with the short-range transceiver.

Referring to the further embodiments of Figure 3, a transaction is started in the step 200. The transaction is performed with the apparatus 100. The transaction takes place by reading and writing opertations that are concluded by the secure transaction element 101. According to at least one embodiment, the secure transaction element 101 may communicate via the near field communications module 103. Alternatively, the secure transaction element 101 may communicate via other communications modules of the apparatus 100, such as, for example, the network transceiver 105 and short range transceiver 104. The transaction takes place by using a communication protocol such as, for example, the ISO-14443 communications protocol. The transaction is completed using the communications protocol in the step 200. In the step 201 a controller SW1 switches communications to another communications protocol such as, for example the ISO-18092, or ISO-21481, once the transaction is substantially completed and carried out. The controller SW1 may switch communications to ISO-18092, or ISO-21481, which are examples of other communications protocols for NFC-IP based peer-to-peer communications. An authentication procedure for the transaction may now start in the step 202. The authentication information may be requested from the apparatus 100. According to embodiments of the present invention, the authentication information is requested from the authentication module 102 of the apparatus 100. For example the authentication is requested from a smart card 102' of the apparatus 100, such as, for example the SIM card or the like. The requesting party of the transaction is provided with the authentication information in the step 203. The authentication information is advantageously used to complete the transaction. The authentication information may be transferred for example by transmitting image information of the authenticated user of the device that can be presented as a picture of the authenticated user of the apparatus 100. Furthermore by providing the parties with digital signature etc. As said previously there are various examples.

In a further embodiment of the invention during the authorisation for completing the transaction, the controller SW1 is configured to switch communications from the secure transaction mode into the authentication mode. The authentication mode authenticates the user of the apparatus 100 by the necessary authentication information. The authentication information can be presented where necessary.

In a further embodiment of the invention, the controller SW1 is further configured to detect whether the transaction has substantially been carried out so as to switch to said another communications protocol. The controller SW1 may be further configured to detect specific data of the transaction so as to determine whether the transaction continues or is about to be substantially carried out. The controller SW1 may further be coupled with a timer (not shown) configured to prompt the controller to check a status of the transaction and/or determine whether messages related to the transaction has been exchanged within a certain predefined time period in yet another further embodiment. In accordance with a further embodiment, if the controller SW1 detects no transaction related messages have been exchanged within a predefined time period, the controller may determine that the transaction is substantially carried out.

Various embodiments of the invention use near field communication such as NFC for exchanging information. For example the near filed communications module 103 may use various near field communications, such as, e.g. the NFC or the like. The near field communications module 103, alternatively referred to as near field communications interface, provides necessary means to communicate with external tags/devices using e.g. RFID technology so that the terminal can conduct RFID-based payment and ticketing transactions, but not limited thereto. The near field communications module allows both reading and writing operations to be conducted both to and from external tags/devices and also peer-to-peer type communication between two terminals. As said the secure transaction module 101 and the secure authentication module 102 can be directly linked to the near filed communications interface 103, by means of the controller SW1, in order to ensure that there will be no unnecessary delays within terminal logic that might hinder/prevent transactions due to the nature or RFID communication, which will typically require fast response times. A RFID transaction, for instance, will be typically conducted within hundreds of milliseconds. NFC itself is a short-range wireless technology which enables the communication between devices over a short distance. The technology can be used in mobile phones and other RFID based apparatuses. NFC is compatible with the existing contactless infrastructure, for example in use for public transportation and payment. NFC works by magnetic field induction. It can operate within the globally available and unlicensed RF band of 13.56 MHz. Working distance can be 0-20 centimetres, and the speed: 106 Kbit/s, 212 Kbit/s or 424 Kbit/s. Generally there are two modes: Passive Communication Mode: The Initiator device provides a carrier field and the target device answers by modulating existing field. In this mode, the Target device may draw its operating power from the Initiator-provided electromagnetic field, thus making the Target device a transponder. Active Communication Mode: Both Initiator and Target device communicate by generating their own field. In this mode, both devices typically need to have a power supply. NFC can be used to configure and initiate other wireless network connections such as Bluetooth, Wi-Fi or Ultra-wideband. Use cases for NFC may for example be: Card emulation: the NFC device behaves like an existing contactless card. Reader mode: the NFC device is active and read a passive RFID tag, for example for interactive advertising. P2P mode: two NFC devices are communicating together and exchanging information. Plenty of applications will be possible such as: Mobile ticketing in public transport - an extension of the existing contactless infrastructure. Mobile Payment - the mobile phone acts as a debit/ credit payment card. Smart poster - the mobile phone is used to read RFID tags on outdoor billboards in order to get info on the move.

Pairing - in the pairing of devices with NFC support may be as easy as bringing them close together and accepting the pairing. The process of activating on both sides, searching, waiting, pairing and authorization can be replaced by a simple "touch" of the mobile phones. Other applications in the could include: Electronic tickets – airline tickets, concert/event tickets, and others, Electronic money, Travel cards, Identity documents, Mobile commerce, Electronic keys – car keys, house/office keys, hotel room keys, etc

NFC is an open platform technology standardized in ECMA-340 and ISO/IEC 18092. These standards specify the modulation schemes, coding, transfer speeds and frame format of the RF interface of NFC devices, as well as initialization schemes and conditions required for data collision-control during initialization-for both passive and active NFC modes. Furthermore, they also define the transport protocol, including protocol activation and data-exchange methods. NFC incorporates a variety of pre-existing standards including ISO_14443 both A (normal) and B (banking/short range), ISO_15693, and FeliCa.

A further embodiment of the invention takes advantage of smart card such as a subscriber identity module (SIM). Generally the SIM card may be an SD card or actually any other auxiliary secure element. In the further embodiment the SIM card contains the secure transaction element 101 as well. Thus the secure transaction element can be advantageously installed into the smart card. The switch mat switch between these blocks, for example as described in various embodiment of the invention.

In case that a user wants to conduct a NFC based transaction with a local point-of-sale terminal, comprising a NFC communication module, the user (or the terminal) activates elements, and may further select at least one of the transaction/applications to be active at the time. The selection may be based on e.g. default selection, based on user selection or alternatively the terminal 100 may be capable of selecting the suitable application based on the current context/environment of the terminal 100. The selection of the context/environment of the terminal 100 may be performed by the user e.g. by initiating reading a dedicated tag through the NFC module 103', wherein the tag could indicated the presence of certain type of POS terminal (e.g. local merchant having a contract with certain credit card company and also private loyalty card for the store), so that corresponding applications can be activated. The selection of the context/environment may alternatively be based on the current location of the mobile terminal, which may be based on GPS positioning information or alternatively information received through wide-area- or local-area networks.

Afterwards, when the amount of payment and other related information is negotiated (this “negotiation” means that user of the terminal 100 and the transaction provider have mutually agreed the amount of payment), the user can, for example, simply “touch” (i.e. brings his mobile terminal device in close proximity) the POS terminal NFC interface with the terminal 100, which results the terminals NFC interface 103' to communicate with the POS terminals NFC interface, so that the necessary information for conducting the agreed transaction will be exchanged. It should be further noted that the NFC interfaces 103 of the terminal 100 and the POS terminal may include any communication interface suitable for near field communication including RF and optical interfaces two name a couple of non-limiting examples. The necessary information includes at least following communication operations. All of the following operations shall be performed within the set time limit for the transaction that might be different for different embodiments. According to one non-limiting exemplary embodiment, the time limit may be set for 300-400ms for RFID-based transactions. In order to complete the transaction the authentication is provided as described by the various embodiments of the invention.

Fig. 4 illustrates schematically an implementation of an apparatus 100" such as a portable consumer electronic device being equipped with a RFID device according to some further embodiments of the invention. The block diagram of Fig. 4 illustrates a principle structural design of a cellular terminal, which should exemplary represent any kind of portable CE device 100" employable with the present invention. It shall be understood that the present invention is not limited to any specific kind of portable CE device such as that illustrated. The illustrated portable CE device 100" comprises typically a central processing unit (CPU) 410, a data storage 420, an application storage 430, input/output means including audio input/output (I/O) means 450, a keypad with input controller (Ctrl) 460 and a display with display controller (Ctrl) 470.

Additionally, the portable CE device 100" according to various further embodiments of the invention includes a cellular interface (I/F) 480 coupled to a cellular antenna and operable with a corresponding subscriber identification module (SIM) 440. In a further embodiment of the invention when integrating the smartcard module into the handheld mobile phone, security is improved as in order to use the mobile phone a PIN input is needed enabling GSM SIM in the mobile phone when the mobile phone is switched on. Thus the mobile phone when switched off or e.g. when activation of phone from screen saver mode a PIN is well protected from violation. According to further embodiments of the present invention, the smartcard module may be integrated in to SIM card of the portable CE device 100" instead of being a separate module. According to further embodiments, the smartcard module may be integrated into a MMC card or memory stick module in connection with the data storage 420 of the portable CE device. Moreover, the portable CE device 100" according to a further embodiment of the invention comprises also a local data interface (I/F) 400 and a general data interface (I/F) 490. However, it should be noted that in embodiments where the smart card module is integrated into certain modules, there needs to be a direct link to the local data interface (I/F) 400 in order to ensure the time requirement for the transaction.

The local (short-range) data interface (I/F) 400 or local (short-range) transceiver may be additionally implemented in portable CE device 100" to provide for local data communication with a corresponding counterpart network, base station or transceiver. In general, the local data interface (I/F) 400 can be realized by a low-power radio frequency (LPRF) transceiver such as a Bluetooth transceiver, a WLAN (wireless local area network) transceiver, an ultra-wide band (UWB) transceiver or any other transceiver operable with an IEEE 802.xx standard. Moreover, the local data interface (I/F) 400 can be also implemented as an infrared-based interface such as an IrDA (infrared direct access) interface or an interface being based on radio frequency identification (RFID) technology, namely RFID reader, RFID transponder and near field communication (NFC) standard, respectively.

The cellular interface (I/F) 480 is arranged as a cellular transceiver to receive signals from the cellular antenna, decodes the signals, demodulates them and also reduces them to the base band frequency. The cellular interface 480 provides for an over-the-air interface, which serves in conjunction with the subscriber identification module (SIM) 440 for cellular communications with a corresponding radio access network (RAN) of a public land mobile network (PLMN). The output of the cellular interface (I/F) 480 thus consists of a stream of data that may require further processing by the central processing unit (CPU) 410. The cellular interface (I/F) 480 arranged as a cellular transceiver also receives data from the central processing unit (CPU) 410, which are to be transmitted via the over-the-air interface to the radio access network (RAN). Therefore, the cellular interface (I/F) 480 encodes, modulates and converts the signal to the radio frequency, which is to be used. The cellular antenna then transmits the resulting radio frequency signal to the corresponding radio access network (RAN) of the public land mobile network (PLMN).

In addition to the local data interface (I/F) 400 and the general data interface (I/F) 490, the portable CE 100" device may include in certain embodiments of the present invention, a broadcast receiver interface (not shown), which allows the portable CE to access broadcast transmission services that include Digital Video broadcasting (DVB-T, DVB-H), Digital Audio Broadcasting (DAB), Digital Radio Mondiale (DRM), Integrated Services Digital Broadcasting-Terrestrial (ISDB-T), Advanced Television Systems Committee (ATSC) and Digital Multimedia Broadcasting (DMB-T) techniques to name a few.

The display and display controller (Ctrl) 470 are controlled by the central processing unit (CPU) 410 and provides information for the user typically by the means of a user interface. The keypad and keypad controller (Ctrl) 460 are provided to allow the user to input information. The information input via the keypad is supplied to the central processing unit (CPU) 410, which may be controlled in accordance with the input information. The audio input/output (I/O) means 450 includes at least a speaker for reproducing an audio signal and a microphone for recording an audio signal. The central processing unit (CPU) 410 may control the conversion of audio data to audio output signals and the conversion of audio input signals into audio data, where the audio data have a suitable format for cellular transmission.

The data interface (I/F) 490 serves for interfacing data and instruction communications between the local data interface module 400 and the portable CE device 100". The data interface (I/F) 490 may be established by various appropriate hardware and/or software interfaces.

The portable CE device 100" further comprises a protected memory, which is adapted for storing a plurality of data records, for instance within said smartcard module 101 and 103. As defined above, each data record shall be understood as a digital representation of information relating to for instance digital ticket data and digital payment data according to an embodiment of the present invention. The protected memory is specifically adapted to meet requirements, which have to be considered to ensure security and privacy aspects relevant in view of the sensitive digital information stored therein. Those skilled in the art will appreciate that the handling of the sensitive digital information such as digital ticket data and digital payment data as defined above is subjected to security and privacy aspects from user view as well as from service provider view, where the service provider relates to both issuing authorities and accepting authorities of the digital information in question.

In general, the portable CE device 100" described above may anyone of the example devices comprising illustratively a portable phone, a personal digital assistant, a pocket personal computer, a portable personal computer, a communicator terminal or any other portable consumer electronics (CE) with processing capability and appropriate communication means; i.e. comprising at least a transaction module 101, an authentication module 102, a and a near field communications module 103. In general the portable CE device 100" embodies a processor-based device, which allows implementation of the inventive concept. The following embodiment will illustrate enhanced identification device operation, which is for instance implementable in each of the aforementioned consumer electronic (CE) devices. However, illustration of the identification device will be given with respect to illustrated portable CE device 100", which has attached or has embedded such an identification device. But it shall be noted that the invention is not specifically limited to those identification devices and to portable CE device coupled thereto, respectively, which are herein illustrated merely for the way of illustration on the basis of embodiments according to the present invention.

In various embodiments of the invention the computer program can be a computer program product. The product is an example of a tangible object. For example, it can be a medium such as a disc, a hard disk, an optical medium, CD-ROM, floppy disk, or the like storage etc. In another example the product may in a form of a signal such as an electromagnetic signal. The signal can be transmitted within the network for example. The product comprises computer program code or code means arranged to perform the operations of various embodiments of the invention.

Ramifications and Scope

Although the description above contains many specifics, these are merely provided to illustrate the invention and should not be construed as limitations of the invention's scope. It should be also noted that the many specifics can be combined in various ways in a single or multiple embodiments. Thus it will be apparent to those skilled in the art that various modifications and variations can be made in the apparatuses and processes of the present invention without departing from the spirit or scope of the invention.

Claims

1. An apparatus, comprising:

a controller;

a near field communications module operatively coupled to the controller;

a first secure storage location operatively coupled to the controller and configured to store at least partly information for carrying out a transaction operation by way of a transaction communications protocol via the near field communications module; and

a second secure storage location operatively coupled to the controller and configured to store at least authentication information regarding authentic user of the apparatus;

wherein the controller is configured to switch communications from said transaction communications protocol to another communications protocol in response to detecting that said transaction is substantially carried out and communicate the at least authentication information regarding the authentic user of the apparatus via the another communications protocol.

2. An apparatus according to claim 1, wherein the controller is further arranged to authenticate the authentic user of the apparatus in said transaction using said another communications protocol, wherein the authentication relating to the transaction is carried out on a basis of the authentication information.

3. An apparatus according to any of the preceding claims, further comprising a smard card configured to store the first secure storage location.

4. An apparatus according to any of the preceding claims, further comprising a smart card configured to store the second secure storage location.

5. An apparatus according to any of the preceding claims, wherein the first and the second secure locations are arranged to be located at the same smart card or at least two different smart cards.

6. An apparatus according to any of the preceding claims, wherein the first secure storage location comprises a transaction module.

7. An apparatus according to any of the preceding claims, wherein the second secure storage location comprises an authentication module.

8. An apparatus according to any of the preceding claims, wherein the controller comprises a logical or a physical switch.

9. An apparatus according to any of the preceding claims, wherein said authentication comprises image information regarding the authentic user of the apparatus or a digital signature.

10. An apparatus according to any of the preceding claims, wherein the authentication information is configured to be secured so that an authentication key is needed to be presented for accessing authentication information.

11. An apparatus according to any of the preceding claims, wherein the controller is further configured to detect whether the transaction has substantially been carried out so as to switch to said another communications protocol.

12. An apparatus according to any of the preceding claims, wherein the controller is further configured to detect specific data of the transaction so as to detect that the transaction has been substantially carried out.

13. An apparatus according to any of the preceding claims, further comprising a timer coupled with the controller configured to prompt the controller to check a status of the transaction.

14. A wireless apparatus, comprising:

a controller;

a near field communications module operatively coupled to the controller;

a first secure storage location operatively coupled to the controller and configured to store at least partly information for carrying out a transaction operation by way of a transaction communications protocol via the near field communications module; and

a second secure storage location operatively coupled to the controller and configured to store at least authentication information regarding authentic user of the apparatus;

wherein the controller is configured to switch communication from said transaction communications protocol to another communications protocol in response to detecting that said transaction is substantially carried out and communicate the at least authentication information regarding the authentic user of the wireless apparatus via the another communications protocol.

15. A wireless apparatus according to claim 14, wherein the controller is further arranged to authenticate the authentic user of the apparatus in said transaction using said another communications protocol, wherein the authentication relating to the transaction is carried out on a basis of the authentication information.

16. A wireless apparatus according to claim 14, wherein the controller is further configured to detect whether the transaction has substantially been carried out so as to switch to said another communications protocol.

17. A wireless apparatus according to claim 14, wherein the controller is further configured to detect specific data of the transaction so as to detect that the transaction has been substantially carried out.

18. A wireless apparatus according to claim 14, further comprising a timer coupled with the controller configured to prompt the controller to check a status of the transaction.

19. A method, comprising:

conducting substantially a transaction by exchanging transaction information via a first communications protocol,

switching to a second communications protocol upon detecting that the transaction is substantially conducted, and

finalizing the transaction by exchanging authentication information via the second communications protocol.

20. A method according to claim 19, further comprising

authenticating a valid user of the apparatus in said transaction using said another communications protocol, wherein the authentication relating to the transaction is carried out on a basis of the authentication information.

21. A method according to claim 19, further comprising

detecting specific data of the transaction so as to detect that the transaction has been substantially carried out.

22. A method according to claim 19, further comprising

prompting, by a timer, to check a status of the transaction.

23. A computer program code, wherein the computer program code is arranged to

conducting substantially a transaction by exchanging transaction information via a first communications protocol,

switching to a second communications protocol upon detecting that the transaction is substantially conducted, and

finalizing the transaction by exchanging authentication information via the second communications protocol.

24. An apparatus, comprising:

means for conducting substantially a transaction by exchanging transaction information via a first communications protocol,

means for switching to a second communications protocol upon detecting that the transaction is substantially conducted, and

means for finalizing the transaction by exchanging authentication information via the second communications protocol.

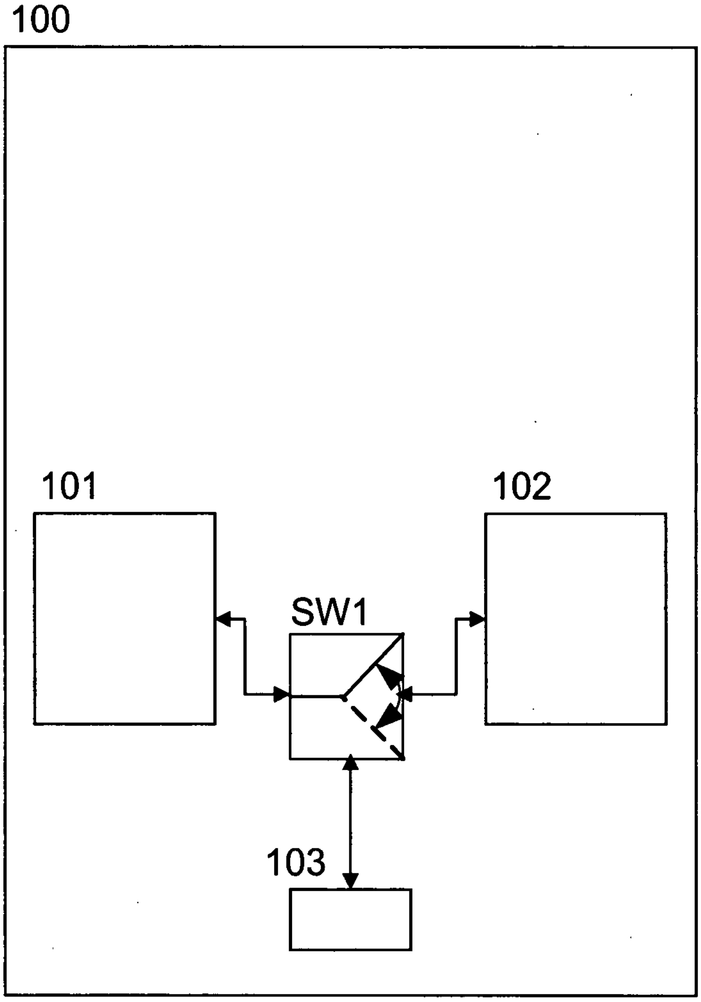

Fig.1

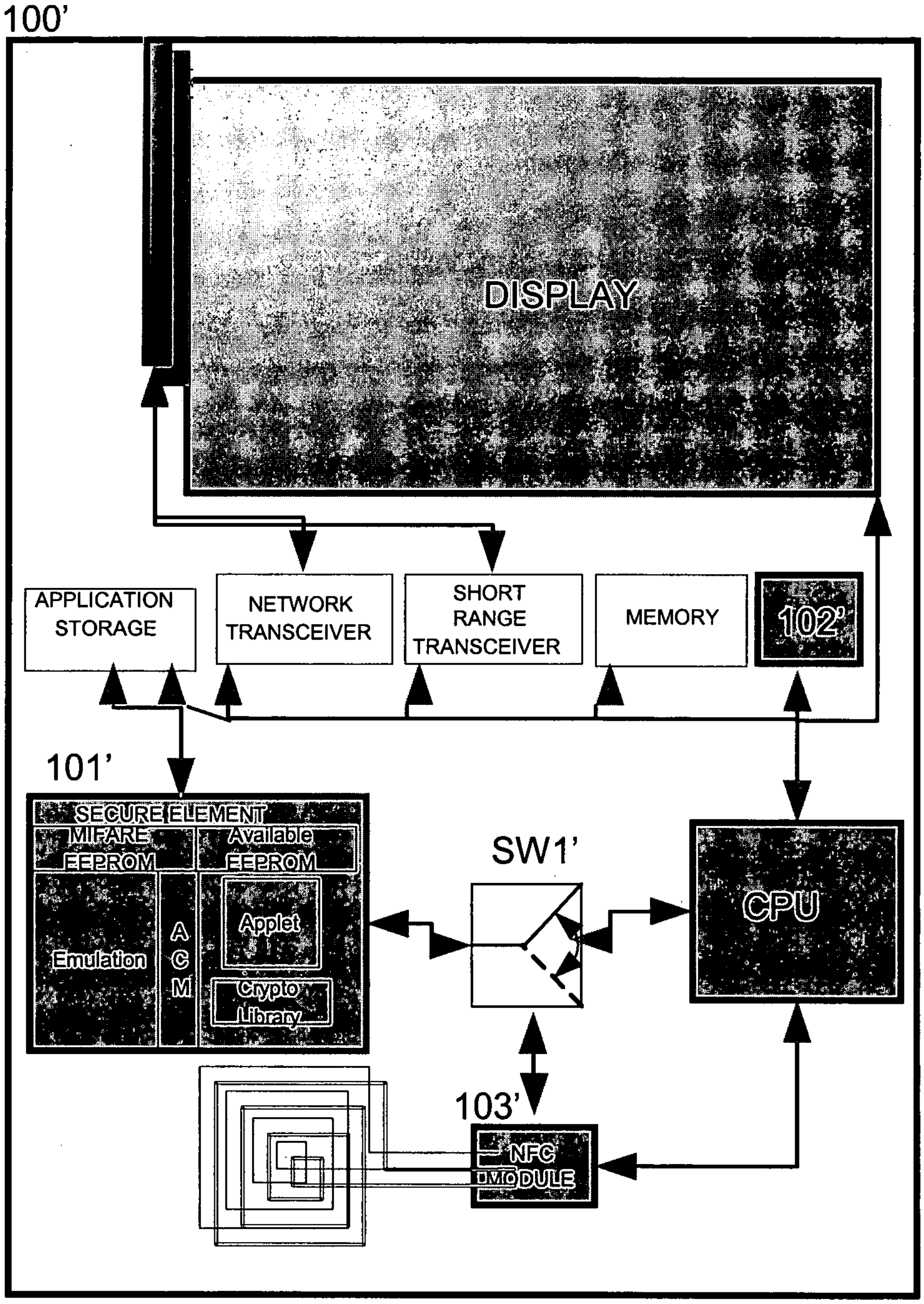
100'
DISPLAY
APPLICATION STORAGE
NETWORK TRANSCEIVER
SHORT RANGE TRANSCEIVER
MEMORY
102'
101'
SECURE ELEMENT
MIFARE EEPROM
Available EEPROM
Emulation
A C M
Applet
Crypto Library
SW1'
CPU
103'
NFC MODULE

Fig.2

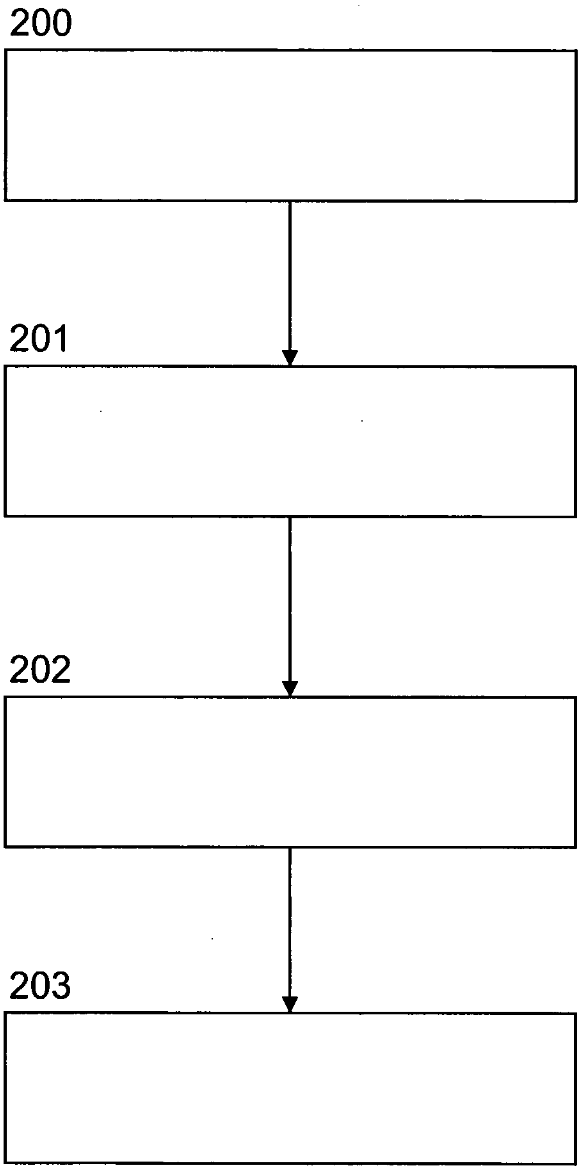

Fig.3

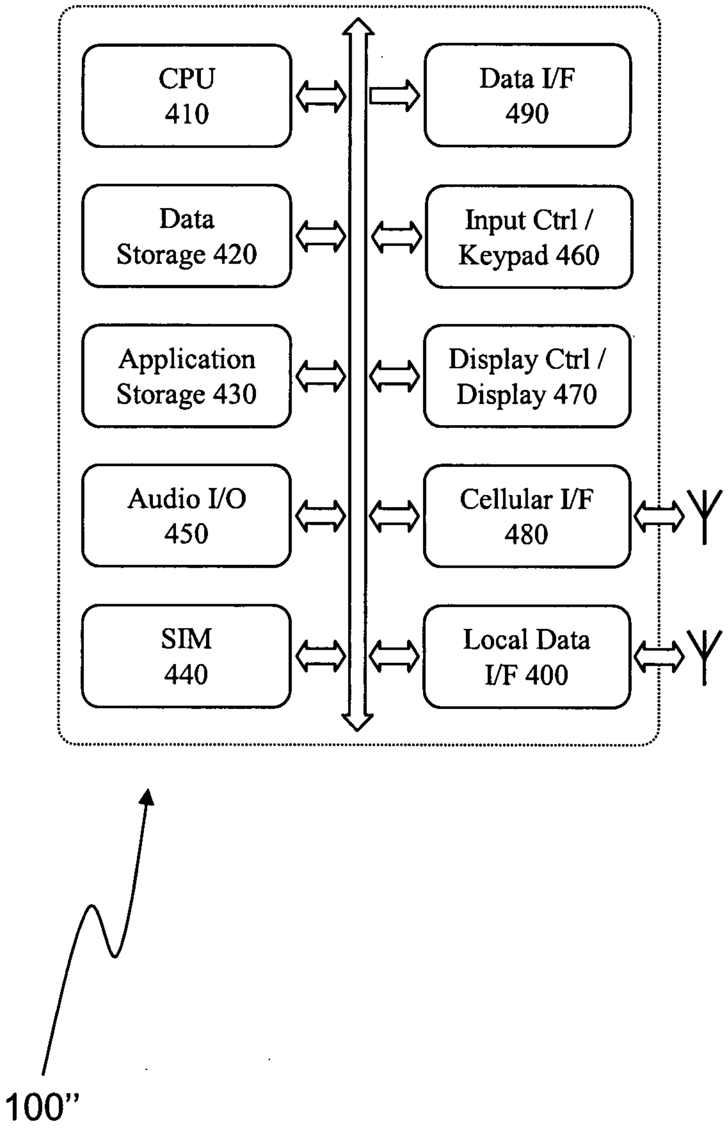
CPU
410
Data
Storage 420
Application
Storage 430
Audio I/O
450
SIM
440
Data I/F
490
Input Ctrl /
Keypad 460
Display Ctrl /
Display 470
Cellular I/F
480
Local Data
I/F 400
100"

Fig.4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2007/000288

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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)

IPC8: H04L 29/06, H04L 9/32, G06Q 20/00

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

FI, SE, NO, DK: H04L 29/06, G06Q 20/00

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, Full-Text cluster, Inspec, WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	WO 2007/044882 A2 (YUEN PHILIP et al.) 19 April 2007 (19.04.2007)	
X	abstract, paragraph [0029]	19-21, 23-24
A	abstract	1-18, 22
	US 2007/0278290 A1 (MESSERGES THOMAS S et al.) 06 December 2007 (06.12.2007)	
X	paragraph [0021]	19-21, 23-24
A	abstract	1-18, 22
	WO 99/35620 A1 (SUN MICROSYSTEMS INC) 15 July 1999 (15.07.1999)	
X	page 10, top paragraph; figure 5	19-21, 23-24
A	abstract	1-18, 22
A	US 2007/0156436 A1 (FISHER MICHELLE et al.) 05 July 2007 (05.07.2007), paragraphs [0013] and [0014]	1-24
A	US 2002/0174068 A1 (MARSOT RODOLPHE) 21 November 2002 (21.11.2002), claim 1	1-24

☒ Further documents are listed in the continuation of Box C. ☒ 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
18 August 2008 (18.08.2008)

Date of mailing of the international search report
20 August 2008 (20.08.2008)

Name and mailing address of the ISA/FI
National Board of Patents and Registration of Finland
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 9 6939 5328

Authorized officer
Olli Pekonen

Telephone No. +358 9 6939 500

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2424801 A (UNIWILL COMP CORP) 04 October 2006 (04.10.2006), abstract	1-24
A	ECMA International: ECMA 352 Standard. December 2003 [retrieved on Aug 14th, 2008]. Retrieved from the Internet: <URL: http://www.ecma-international.org/publications /files/ECMA-ST/Ecma-352.pdf>, figure 1	1-24

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G06Q 20/00 (2006.01)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2007/000288

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
WO 2007/044882 A2	19/04/2007	US 2007107044 A1	10/05/2007
		US 2007094150 A1	26/04/2007
US 2007/0278290 A1	06/12/2007	WO 2007146470 A2	21/12/2007
WO 99/35620 A1	15/07/1999	JP 2001516485T T	25/09/2001
		EP 0965107 A1	22/12/1999
		AU 2213599 A	26/07/1999
		US 2002161655 A1	31/10/2002
US 2007/0156436 A1	05/07/2007	US 2008052233 A1	28/02/2008
		US 2008052192 A1	28/02/2008
		US 2008051122 A1	28/02/2008
		US 2008051059 A1	28/02/2008
US 2002/0174068 A1	21/11/2002	EP 1256911 A1	13/11/2002
		FR 2824407 A1	08/11/2002
GB 2424801 A	04/10/2006	TW 256007B B	01/06/2006
		US 2006235711 A1	19/10/2006
		FR 2884010 A1	06/10/2006
		DE 102005046337 A1	05/10/2006