(54) Titre : PROCEDE D'AUTORISATION D'ACCES A UN SERVICE ET APPAREIL POUR METTRE EN OEUVRE CE PROCEDE
(55) Title: METHOD FOR AUTHORISED GRANTING OF A SERVICE AND DEVICE FOR CARRYING OUT SAID METHOD

(57) Abrégé/Abstract:
Current electronic cards (10), such as, for example, proximity cards, smartcards for short, can transmit data to a reader unit over a range of up to about 10 cm. Boosters are used to improve convenience which in essence represent a wireless extension. This is
然而，与终止有关的自主性、功能（结果）和不同的应用。一种方法是通过智能卡（10）传输服务特定代码（40），然后传输给便携式设备（30），并将其通过不同的通信连接（70）传输给受权的通信连接（70），以实现模块化系统，允许用户多访问服务。
Abstract

Current electronic cards (10), such as, for example, proximity cards, smartcards for short, can transmit data to a reader unit over a range of up to about 10 cm. Boosters are used to improve convenience which in essence represent a wireless extension. This is however not adequate with regards to autonomy, function (as a result of termination) and for the differing applications. A method is disclosed in which the transmission (40) of service-specific codes, stored on a number of different smartcards (10), to a portable device (30) is carried out. The portable device (30) then transmits one or more of said codes via several different communication connections (70) so that access to a service can be activated. By providing services to the corresponding authorised communication connection (70) a modular system is achieved, permitting multiple access for a user to services.
Method for authorized granting of a service and device for carrying out said method

The present invention relates to a method for authorized granting of a service in accordance with the preamble of claim 1 and to a portable device for carrying out said method in accordance with the preamble of claim 11.

In this document the term "electronic card" or "electronic medium" or "medium" for short is generally taken to include electronic identity cards with an identifying characteristic, and these are also sometimes referred to by terms such as smartcard, chip card, electronic ticket, proximity cards, vicinity cards and employee badges. Proximity cards and vicinity cards are standardized by ISO, these standards being defined in ISO 14443 [1] and ISO 15693 [2], in addition the proximity cards and vicinity cards also include proprietary brands such as LEGIC prime for example.

The terms and definitions given in the list of abbreviations and acronyms are an integral part of this document in the sense of a glossary. This means that not all acronyms and terms are specifically explained elsewhere in the document. The widely-used English expressions have been employed both here and in the original German document within the text and in the glossary for the individual units. Likewise the function implemented with a component is in some cases provided with the same reference symbol as the component itself. To avoid any uncertainty, as in the original German version, the normally-used English expressions, such as "challenge/response" are also employed in this translation for the individual units and methods.

Proximity Cards PICC can transmit data to a proximity card detector PCD at a range of between 1 and 10 cm. Thus, in order
to be granted access to a zone, a person is obliged to move the card into the vicinity of the Proximity Card Detector PCD. This is especially disadvantageous when entering a garage since the window of the vehicle must be lowered to do so. There is especially the danger of the card falling on the floor when being manipulated in this way.

Personal identification details and/or authorizations are stored on a smartcard. The term identification details and/or authorizations also includes keys in the cryptographic sense. These identification details or authorizations, if necessary together with further interaction by a user, allow access to a location or allow a service or information to be obtained.

The term "service" in this document includes both the classical term from telecommunications, such as a supplementary service for example. The term "service" in this document is also understood to include any access to a location or to a service or for obtaining information or for obtaining money.

Smartcards possess an air interface, e.g. in accordance with ISO/IEC 14443 [1], and/or a contact interface, e.g. in accordance with ISO 7816 [3]. Both interfaces are designed for communication in the near field. In the case of a wireless connection this near field covers around 10 cm. Communication with such cards is not possible over a greater distance.

Chip card devices for accepting a chip card, with which a wireless connection to a terminal for a payment or access to an object is enabled are known for example from EP 0 159 539 A1 [9], US 6,142,369 [10], US 6,250,557 B1 [11] or DE 198 41 862 A1 [12]. In US 6,250,557 B1 [11] there is provision, if a plurality of chip cards is inserted, for each chip card to be provided with its own IP address. In many cases a mobile
telephone is provided as a chip card device, featuring slots for further chip cards, i.e. in addition to the SIM card slot.

For communication over greater distances, but not via a public switched telecommunication network such as GSM, so-called "combi boosters" are known, made by Nedap [4, 5] for example. A "booster" is an electronic portable device (= electronic wallet), into which a proximity card can be inserted. An identifier, mostly a personal identifier - referred to below as a "personified" identifier - is transferred from the proximity card via the air interface into the wallet. This wallet sends the received identifier on another frequency, e.g. on the ISM band of 2.45 GHz, to a static receiver unit. The received identifier is evaluated in a background system and, if the identifiers match, a release signal for granting access is generated. The wallet in this case can also contain a further identifier, so that access is only possible with the relevant wallet and the card. With the proprietary variant mentioned at the start it should be noted in this case that the connection cannot be terminated in the wallet unless a corresponding proprietary chip is built into the wallet. The reason for this the Layer 1/ Layer 2 transmission used and not disclosed by scrambling.

Such a system is also desirable for access control in which a person carries such a wallet with an electronic card inserted into it. The above solution for parking lot entry is not satisfactory for further applications for the following reasons:

a) Autonomy is restricted or operation must be though an installation in a motor vehicle with wired energy supply.

b) Depending on the type of access implemented by radio technology, a correspondingly equipped electronic wallet must also be carried.
To grant an individual service, such as withdrawing cash from an ATM, a method is disclosed in 101 04 409 B4 [6] in which the ATM reads a code from the mobile telephone, preferably a bar code. This code contains a unique address for example, such as a MAC address for a first authentication for example. The further steps for dispensing the cash are undertaken via radio communication, e.g. via Bluetooth.

Such portable electronic devices have also already been proposed, such as in European Patent Application EP 05013418.8 [7] for example, in which the aforementioned disadvantage relating to the greatly restricted autonomy is remedied by "waking" of the electronic wallet by a near field. Following the "waking" with a first lower frequency of the portable electronic device there is intermittent bidirectional communication with an access point at a higher frequency. After a certain time without communication there can be provision for the portable device to return to the sleep state again. This enables a significantly great autonomy to be achieved.

The solution still does not satisfactorily remedy the disadvantage listed above under b), since this solution is restricted to a specific physical access and to a specific smartcard with a specific service.

The underlying object of the present invention is to create a method for a medium containing an identifier for granting a service, such as admission to a zone for example or for authorized use of service, with this method on the one hand overcoming the disadvantages stated above and also enabling the following:
- Use for different types of electronic cards/media;
- Usable for different cards of the same type, in which
data/authorizations granted by an issuer are accessible in different ways, i.e. stored and/or accessible in separate segments;
- Compatible with different interworking units;
- Decoupling of the type of communication link from the authorization stored on the smartcard;
- Simple handling by the user;
- The safety mechanisms stored in the medium do not have to be disclosed.

The object of the invention is also to specify a portable device suitable for executing the above method.

This object is achieved for the method by the features specified in claim 1 and for the portable device by the features specified in claim 11.

The method defined in claim 1 provides a user with secure access to services in a modular manner. "Near field" of the first communication link means that the medium is in the direct vicinity within the range of up to a few millimeters from the portable device. By means of a plurality of media each containing at least one service-specific identifier service-specific authorization data can thus be requested for obtaining a service or for access to a zone. For a body issuing a medium such as a smartcard this has the advantage that the stored identifier assigned to a service can be administered independently of other identifiers. The function and the security are guaranteed despite the "portable device" vehicle because of the secure end-to-end connection, meaning that the portable device is not involved in the end-to-end data encryption. The bidirectional communication between the portable device and the access point makes it possible, with a conventional card reader located in the access point, for the
card issued in the portable device to be emulated in the access point. On the one hand this allows existing access points to continue to be used and on the other hand the interface between access point and an assigned server or network management system does not have to be disclosed. This makes it possible to decouple access to a service from the actual means embodied for transmission to an access point such as a card reader for example.

In a development of the method an input means can be arranged on the portable device for authentication of the user based on a user interaction. A biometric sensor, e.g. a fingerprint sensor or keys can be arranged as the input means. The unit can be configured by means of entries made via the keys. Expediently a display is also to be provided, e.g. an LCD display. Both "challenges" and also "responses" for the authentication, which are needed for authentication of a user, can be shown on the display. The display also serves to display operating states relating to the portable device and also in relation to the granting of a service. The control elements are used not only for the above-mentioned authentication and/or configuring, but allow access to a possibly chargeable service based on an active deliberate action.

Further advantageous embodiments of the invention are specified in further claims.

The invention is explained in more detail below with reference to the drawing. The figures show:

Figure 1  spatial arrangement of the various functional units in a passage area;
Figure 2.1  front view of a wallet;
Figure 2.2  cross section of a wallet and an assigned access
Figure 2.3  rear view/section of wallet;
Figure 3  Wallet with partially inserted card;
Figure 4.1 exploded view of the basic components and mechanical design of the wallet in a cross section seen from the side;
Figure 4.2 mechanical design in cross section from the longitudinal direction;
Figure 5  block diagram of a portable device;
Figure 6  diagram of the modular concept for the different services;
Figure 7  diagram of secure communication links and the assignment of the services.

An overview of the principal function of the inventive method and of the components involved is given below with reference to Figure 1. Details of the individual components and their function are then provided by subsequent Figures 2 to 7.

Figure 1 shows the spatial arrangement of the different functional units or components in a passage area 50, which is formed by two entry pillars 51. An identifier located on the card 10 for access to a service is transmitted by a medium 10, preferably a smartcard 10, to the portable device 30 via a first secure communication link 40. The portable device 30 establishes a second communication link 70 to an access point 60. The aforementioned identifier and/or a further identifier are transmitted via this second likewise secure communication link 70 to the access point 60. The identifier transmitted in this way is evaluated via a connection 80 in a unit 61 located in the background, e.g. an authentication server 61, in order to establish on the basis of a comparison whether access can be granted in this way or whether a specific service may be obtained. The transmission of the identifier explained above
never includes the transmission in clear text of only the identifier stored on the smartcard 10 under any circumstances. Instead a mapping (math.) of the identifier based on data encryption or based on a logical combination is transmitted. For encryption and authentication the appropriate keys and digital identity credentials are optionally stored on the portable device 30 and/or on the medium 10. The light barrier shown in Fig. 1 between the two entry pillars can for example serve to secure the data link of the zone 50 itself, to prevent a person being caught by an automatic door. Not explicitly shown are the actual variants of a service, such as delivery of digital goods such as a piece of music for example or access to specific information, etc. The figure also shows with optical interface 52 that, for a challenge/response, there is optical transmission to a portable device 30 on the basis of which a response is computed by a crypto controller in the device 30 and/or in the smartcard 10. In this case the portable device is to be held at this light barrier by the user. The actual embodiment of this optical interface is in this case of no significance for the present invention. In specific embodiments this optical interface can contain a section from a display on the entry pillars 51, so that with a pattern recognition implemented on the portable device a challenge can be read and a response computed in the way explained above. This type of information presentation on the display is referred to as "flickering". The computation of the response can be undertaken in this case on the basis of an additional authentication of the user. Further information can be found in the explanation of Figure 5. The challenge can however also be transmitted via the second radio communication link 70. A PKI-secured challenge-response protocol preferably executes between server 61 and medium 10. The smartcard 10 generates a response on the basis of the challenge. From the
response, the server 61 detects the following:
I) That authorization exists for access to a service.
II) That the authorization is authentic.
III) That smartcard rightfully carries this authorization.
IV) That the response is current.

It is pointed out once more at this juncture that such a real access zone 50 in accordance with Figure 1 only represents one example. The access point 60 can be coupled in an appropriate variant to a server 61 in order in this manner to allow the granting of a service as is shown in principle in Figure 7. The access point 60 can also be embodied as a personal computer 60. In this case the above-mentioned optical interface can be realized with a section of the display of the personal computer 60. As a result of a successful authentication the server 61 for example grants access to a chargeable Internet page or for obtaining a specific material or immaterial service.

The wallet 20 only shown in summary in Figure 1 is illustrated extensively in Figures 2.1, 2.2, 2.3, 3, 4.1 and 4.2. It is stated expressly at this point that this wallet 20 represents a useful vehicle for executing the inventive method, but that the wallet 20 is in no way a requirement.

The first communication link 40 between smartcard 10 and portable device can for example be made wirelessly in accordance with ISO 14443: To this end a person only needs to hold the smartcard 10 and the portable device together, as is shown in summary in the upper part of Figure 4.1.

In especially sensitive zones there is even today a statutory duty to carry identification. To this end a wallet 20 is provided with a transparent cover 28 so that the picture assigned to a person is visible on the smartcard to third
parties. The wallet 20, provided with portable device 30 and smartcard 10 can thus be worn visibly as an item of clothing. The mechanical design of the wallet 20 can be found in Figures 3, 4.1 and 4.2. The opening 22 as shown in Figure 3 is used to make removal of the card 10 from the wallet 20 easier.

For the case in which an electrical connection such as that defined in ISO 7816 [3] for example is required between smartcard 10 and portable device 30, the wallet 20 depicted in Figures 2.1, 2.2, 2.3 and 3 provides the contacting for card 10 with a contact pad 23. The corresponding electrical contacting with the portable device 30 is undertaken via the contacts 24, which are preferably embodied sprung in order to ensure secure connection with a certain pressure. The wallet 20 does not have any other so-called intelligent electronics, but merely makes a reliable electrical connection.

In the case of a wireless connection between smartcard 10 and portable device 30 the wallet merely functions as a mechanical connection so that the two parts are protected against accidental loss.

In practical operation a user will establish a connection between different smartcards 10 and the portable device 30 in order to use the system. When a wallet 20 is used an insertion opening with a ramp 25 is provided which facilitates insertion.

Figure 5 shows a block diagram of a portable device 30 in a preferred embodiment. In this case components such as energy supply and processor system, such as an 8051 single-chip processor for example, are not shown in detail. The above-mentioned first communication link 40 between smartcard 10 and device 30 is made on the one hand via an electrical interface unit 321 according to ISO 7816 for example. On the other hand
an air interface unit 322, as defined in ISO 14443 for example, is provided. In this embodiment two crypto controllers 15 each with a Secure Application Module SAM 151 are arranged on the card. Communication is undertaken for example for the one controller 15 via contact interface unit 321 and for the other controller 15 via a radio interface unit 322 in the immediate near field.

Also arranged on the portable device 30 is a crypto controller 35 with at least one Secure Application Module SAM 351. These crypto controllers 15 and 35 provide a secure connection 40 between smartcard 10 and portable device 30 and also between portable device and access point 60. Contained in the crypto controller 15 for such an application can be a biometric authentication e.g. fingerprint details and/or keys for further biometric authentication methods. Likewise so-called digital identity credentials can be stored in the crypto controllers 15 and 35. A secure end-to-end connection in a form of tunneling is implemented between the crypto controller 15 between smartcard 10 and access point 60. The underlying methods can be found in the prior art, the security is preferably implemented using an asymmetrical PKI method or using the symmetrical so-called 3DES method. The communication link 70 between access point 60 and portable device 30 can be realized with:
- Wide area interface 311, "Long Range Communication" with a two-stage transmission method, such as is disclosed in EP 1 210 693 B1 [8];
- Air interface 312 "Short Range Communication" according to ISO 14443;
- Optical Interface 313.

Instead of or in addition to the aforementioned radio interface in accordance with ISO 14443, an NFC interface can
also be provided which includes the interface as defined in ISO 14443. At this juncture it is pointed out, to avoid misunderstandings, that the interface unit 312, as defined in ISO 14443 for example, has an entirely different function from the interface unit 322. In this way an emulation for card readers already installed is possible, without the relevant smartcard 10 having to be suitable for them, since this is dependent on the portable device 30 and not on the smartcard 10 coupled to the device at the time.

For interaction between a user and the portable device 30 the following are to be provided as an alternative or cumulatively:
- Display 33;
- Key or keypad 342;
- Biometric sensor 341, e.g. fingerprint sensor.

The functional complexity contained in such a device requires configuration for most applications. This configuration is preferably undertaken via a wired interface unit 314, e.g. USB.

It is possible to use this wired interface in addition to or as an alternative to the second wireless communication link 70, e.g. for an access to service granted via a personal computer such as specific content of chargeable Internet pages.

The above modular system for access to the various services is shown in tabular form in Figure 6. The Applic column uses the codes A1, A2, .. to list potentially available services such as
- Access to a building,
- E-banking at a bank,
- Access to an automatic teller machine,
- Internet access to the pages of a specific provider,
- Electronic tickets of a local rapid transit company,
- A person's health data,
- ...

The physical communication links provided for each such service are now defined. The "permission carrier" of a relevant service is a specific smartcard MF1, MF2, ..., on which an identifier specifying the personified service is contained. In this case there can be provision, provided this is allowed by the service providers, for a number of identifiers each specifying a service to be stored on a smartcard 10, each in their own section.

The above-mentioned assignment is either solely stored on the smartcard 10 or also stored on the portable device 30. As already stated, this assignment or configuration of the device is preferably undertaken via a wired interface unit 314 such as USB for example. In this way, for initiation of the use of a service the communication link type used for it is selected.

The functions of a card reader associated with classic technology can be freely distributed by the present disclosed embodiment of the invention between the portable device 30 and the access point 60 and thus allow a very flexible adaptation to the very widest range of applications, this relating in particular to the location of the so-called termination.

Figure 7 shows the communication links and the associated services. In a preferred embodiment, the services are either assigned to a plurality of smartcards 10 each with a service-specific code, or a smartcard 10 contains a plurality of such service-specific codes. The transmission 40 between smartcard 10 and portable device is mostly secured using a symmetrical data encryption since there is a 1:1 relationship for this. By
contrast the communication link 70 from the portable device via the access point 60 to server 61 is secured with a PKI method since a 1:n relationship exists here. As a result of the two secured connections 40 and 70 there is thus a secure end-to-end protocol between the smart card 10 and the server 61. There is no contradiction here, if the reference symbol 70 is used for the connection between server 61 and device 30, since the access point 60 generally only has a transit function, i.e. neither access authorizations are checked within it nor are any precautions taken to secure the connection. As a result of the above check, i.e. authentication, a release signal is issued by the server 61 to the relevant service server 62. The service in this case is allocated to the user or granted via a connection 81. This service can be provided in a diversity of ways and is therefore shown in Figure 7 only in a very rudimentary manner. The connection 70 can however optionally be established to an access point 60 in the near field for a specific service. For this purpose the block diagram in accordance with Figure 5 contains an interface 312 as defined in ISO 14443.

The present invention is implemented with a very wide variety of card systems such as Legic or Mifare for example. It can also be used for different cards of the same system, namely if the difference only relates to the issuer or the owner of the card.
<table>
<thead>
<tr>
<th></th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Electronic card, chip card, proximity card, vicinity card; Medium</td>
</tr>
<tr>
<td>15</td>
<td>Crypto controller resident on the card</td>
</tr>
<tr>
<td>151</td>
<td>Secure Application Module SAM assigned to the crypto controller</td>
</tr>
<tr>
<td>20</td>
<td>Wallet for accepting a card and a module</td>
</tr>
<tr>
<td>21</td>
<td>Opening for an attachment element, e.g. clips</td>
</tr>
<tr>
<td>22</td>
<td>Opening for ejecting the card</td>
</tr>
<tr>
<td>23</td>
<td>Contact pad, e.g. for contacting a card in accordance with ISO 7816</td>
</tr>
<tr>
<td>24</td>
<td>Contacts for contacting of a module</td>
</tr>
<tr>
<td>25</td>
<td>Insertion opening, ramp for easier insertion of a card</td>
</tr>
<tr>
<td>28</td>
<td>Cover, transparent cover</td>
</tr>
<tr>
<td>30</td>
<td>Portable device, transceiver unit, module, communication module for physical access, token</td>
</tr>
<tr>
<td>311</td>
<td>Wide area radio interface, &quot;long range&quot;</td>
</tr>
<tr>
<td>312</td>
<td>Interface according to ISO 14443 or NFC interface</td>
</tr>
<tr>
<td>313</td>
<td>Optical interface</td>
</tr>
<tr>
<td>314</td>
<td>Wired interface, e.g. USB</td>
</tr>
<tr>
<td>321</td>
<td>Wired interface for smartcard, e.g. according to ISO 7816</td>
</tr>
<tr>
<td>322</td>
<td>Interface for smartcard, e.g. according to ISO 1443</td>
</tr>
<tr>
<td>323</td>
<td>Optional further interface to other medium</td>
</tr>
<tr>
<td>33</td>
<td>Display, e.g. realized as LCD display</td>
</tr>
<tr>
<td>341</td>
<td>Biometric sensor, e.g. fingerprint sensor</td>
</tr>
<tr>
<td>342</td>
<td>Key, keypad</td>
</tr>
<tr>
<td>35</td>
<td>Crypto controller</td>
</tr>
<tr>
<td>351</td>
<td>Secure Application Module SAM assigned to the crypto controller</td>
</tr>
<tr>
<td>40</td>
<td>First communication link</td>
</tr>
<tr>
<td>50</td>
<td>Passage zone, passage area</td>
</tr>
<tr>
<td>51</td>
<td>Pillar</td>
</tr>
</tbody>
</table>
52 Light barrier
60 Personal computer access point
61 Server background system, computer system,
Network management system for evaluation of the code
and for generation of a release signal for granting a
service
62 Service server, server system containing the services
to be provided
70 Second communication link, bidirectional communication
80 Connection between access point 60 and server 61
A1, A2, Actual variants of a service, for example
   - Electronic ticketing,
   - Building access,
   - E-commerce over the Internet,
   - E-banking service of a bank,
   etc.

Applic service, application
LRA Long Range Access
MF1, MF2, .. Mifare card 1, Mifare card 2, ..
MRA Mid Range Access
SAM Secure Application Module

List of acronyms used

3DES Triple DES
DES Data Encryption Standard, standardized private key
method as defined in ANSI- X3.92-1981
GSM Global system for Mobile Communication
NFC Near Field Communication in accordance with
http://www.nfc-forum.org
PCD Proximity Coupling Device; in accordance with ISO 14443
PICC Proximity Cards; in accordance with ISO 14443
Literature list

[1] ISO/IEC 14443-1
Identification cards - Contactless integrated circuit(s) cards - Proximity cards -
Part 1:
Physical characteristics
ISO/IEC 14443-2
Identification cards - Contactless integrated circuit(s) cards - Proximity cards -
Part 2:
Radio frequency power and signal interface

Identification cards - Contactless integrated circuit(s) cards - Vicinity cards -
Part 1:
Physical characteristics
ISO/IEC 15693-2
Identification cards - Contactless integrated circuit(s) cards - Vicinity cards -
Part 2:
Air interface and initialization
ISO/IEC 15693-2
Identification cards - Contactless integrated circuit(s) cards - Vicinity cards -
Part 3:
Anticollision and transmission protocol

Identification cards - Integrated circuit(s) cards with contacts -
Part 1:
Physical characteristics
ISO/IEC 7816-1
Identification cards - Integrated circuit(s) cards with contacts -

Part 2:
Dimensions and Location of the contacts

System for the contactless exchange of data, and responder for use in such a system
N.v Nederlandsche Apparatenfabriek NEAP.
Connection selection using an optical code WINCOR NIXDORF International GmbH, 3106 Paderborn.
Application date: 22.06.2005
Title: Method, electronic wallet and access point for granting access to a zone with a card.
[8] EP 1 210 693 B1
Method and System for registration of tickets
Siemens VDO Automotive AG, CH - 8212 Neuhausen am Rheinfall.
[9] EP 0 159 539 A1
Chip card system
Siemens Aktiengesellschaft Berlin and Munich.
[10] US 6,142,369
Electronic Transaction terminal for conducting electronic financial transactions using a Smart Card
Assignee: AU-system, Stockholm
Methods and arrangements for a Smart Card wallet and
uses thereof
Assignee: Telefonaktiebolaget LM Ericsson, Stockholm.

[12] DE 198 41 862 A1
Integration of chip card functions into a mobile
communication device
Wieland, Andreas, DE 57076 Siegen DE.
Claims

1. A method for authorized granting of access to a location or for obtaining information or cash - referred to below as authorized granting of a service (Appl) - with an electronic medium (10), on which an authorization is stored for a specific service with an identifier; with
- the service-specific identifier being transmitted over a first secured communication link (40) between the medium (10) and a portable device (30) in the near field;
- the service-specific identifier being transmitted over a second secured communication link (70) between the portable device (30) and an access point (60),
- if there is a match between the identifier received by the access point (60) and a stored identifier, a release signal for granting the service (Appl) is created; characterized in that,

the first communication link (40) between the portable device and the medium (10) can be established for a plurality of service-specific identifiers stored on the medium (10) and/or for plurality of different types of media (10), so that for each service (Appl) a secured end-to-end connection (30, 70) is set up between access point (60) and medium (10).

2. The method as claimed in claim 1, characterized in that
a check is made on the match between the identifier received by the access point (60) and an identifier stored in a server (61) coupled to the access point (60).

3. The method as claimed in claim 2, characterized in that
a further identifier is stored in the portable device (30) which is transmitted via the second communication link (70)
and the release signal is only generated if the further identifier matches a stored further identifier.

4. The method as claimed in claim 3, characterized in that a means of input (31) is provided on the portable device (30), so that the further identifier is only transmitted via the second communication link (70) if a code is entered via the input means (31) and it is established that this code matches a stored code.

5. The method as claimed in claim 4, characterized in that the stored code is stored either in the portable device (30) or in the access point (60) or in the server (61) and that at least one transmitted identifier is modified in relation to the stored identifier as a result of an authentication.

6. The method as claimed in one of the claims 3 to 5, characterized in that the further identifier is formed in accordance with the challenge-response method.

7. The method as claimed in one of the claims 3 to 6, characterized in that the entered code is formed using a biometric method.

8. The method as claimed in one of the claims 1 to 7, characterized in that the portable device (30) features a plurality of air interfaces (311, 312) and the second communication link (70) is selected from the above-mentioned plurality depending on the service (Appl) defined by means of the identifier.

9. The method as claimed in one of the claims 1 to 8, characterized in that
the first communication link (40) is established electrically and/or wirelessly.

10. The method as claimed in one of the claims 1 to 9, characterized in that, the secure connections (40, 70) are established according to the PKI method or the 3DES method.

11. An electronic portable device (30) for carrying out the method as claimed in one of the claims 1 to 10, with said device (30) containing:
   - at least one interface unit (321, 322) via which a first secure communication link (40) can be routed in the near field to a medium (10) containing an identifier;
   - at least one air interface unit (311, 312) via which a second secure communication link (70) can be routed to an access point (60);
   - a crypto controller (35) which is connected to the interface unit (321, 322) and to the air interface unit (311, 312);

with a service-specific identifier being transmitted from the medium (10) to the access unit (60) for an authorized granting of a service (Appl) and, if the identifier received by the access unit (60) matches a stored identifier, a release signal for granting the service (Appl) being generated; characterized in that

the first communication link (40) between the at least one interface unit (321, 322) and the medium (10) is able to be established for a plurality of service-specific identifiers stored on the medium (10) and/or for a plurality of different types of media (10), so that a secure end-to-end connection is able to be set up by means of the crypto controllers (30, 70) for each service (Appl) between medium (10) and access point (60).
12. The device (30) as claimed in claim 11, characterized in that an input means (341, 342) is coupled to the crypto controller (35) in order to carry out an authentication of a person assigned to the service-specific identifier or to set a specific operating state.

13. The device (30) as claimed in claim 12, characterized in that a keypad (342) or a biometric sensor (341) is coupled to the crypto controller (35) as the means of input.

14. The device (30) as claimed in claim 13, characterized in that the biometric sensor (341) is embodied as a fingerprint sensor.

15. The device (30) as claimed in one of the claims 11 to 14, characterized in that a display (33) is coupled to the crypto controller (35) on which operating states or challenges or response are able to be displayed.

16. The device (30) as claimed in one of the claims 11 to 15, characterized in that at least one wired interface (314) is provided, which allows configuration data to be transmitted to the device (30).
<table>
<thead>
<tr>
<th>Applic</th>
<th>Modul</th>
<th>Card</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LRA</td>
<td>MRA</td>
</tr>
<tr>
<td>A1</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>A2</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A10</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>A11</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig 6