Abstract: The present invention relates to a locking system, in which a wireless link is used for data transmission between a key and a lock. According to the invention the receiver or transceiver of the wireless link of the lock being in conjunction with the lock is awakened only if the lock needs to be informed of something, e.g. the door is being opened or closed, and which accordingly lock awakes the lock electronics. The wireless link of the lock is energized and activated by the energy transmitted by the key, whereby it may be a passive element. The required energy is drawn from the battery of the key. The energy for the lock electronics is drawn from the lock's own battery.
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
LOCKING SYSTEM AND METHOD FOR LOCKING SYSTEM

Technical field

The invention relates to a locking system, in which a wireless link is used for data transmission for instance between a key and a lock. In particular, the invention refers to a system utilizing radio waves.

Prior art

Traditionally, the locking of doors has been realised either totally by means of mechanical locks or, as nowadays to an increasing extent, also by electro-mechanical locks, especially in larger buildings. Electro-mechanical locks are generally connected by cables to an external power source and control systems. Electric locking systems are used especially in localities requiring passage control, such as in banks, business firms and other major localities. In private homes the use of electro-mechanical locking is still relatively unusual.

The electro-mechanical locking system will, however, gain more ground also in private homes, as it has considerable advantages compared to a mechanical system. Various kinds of surveillance and control systems for homes and buildings as well as networks are becoming more and more common (e.g. COBA standard, Connected Open Building). In these systems, lighting, heating, water and electricity consumption as well as other issues related to the building can be monitored and controlled through the network of the system. It is thus natural that also the locking systems in homes or buildings are connected to the surveillance and control system already in use. This requires means not only for data transmission but also for supplying the necessary energy between the surveillance and control system and the locking. In addition, it is required that the systems can be installed reliably and at a reasonable cost.
It is possible to reduce the initial costs of a locking system considerably, if cable lines could be totally eliminated. There are several methods for realising data transmission wirelessly. For supplying the energy required by the locking system one possibility is to start using a battery, accumulator or similar energy storage as an energy source for the lock. Then the lock no longer requires any cables.


It is also known to use data transmission especially based on electromagnetic induction as described, for example, in the publication WO 97/44557. In that case, the distance of the data transmission remains to be short.

For wireless data transmission there are at least two generally used methods: an infrared link (IR link) or a radio frequency transmitter/receiver link. The disadvantages of the IR link are, among other things, the visual communication required between the transmitter and the receiver (e.g. the key and the lock), and the susceptibility of the lenses to dirt and dust as well as the narrowness of the IR link beam, which requires for instance that the IR-key is directed toward the lock. In an entrance door to a private home, in particular, an IR link is not the best possible communication means, as the dust, snow etc. possibly collected on the doors might cause communication problems.

Due to the above a radio frequency transmitter/receiver system is a more natural choice for wireless data transmission. Then, for instance in a simplex wireless key system the transmitter is on the same side as the key, whereas the receiver is located on the same side as the lock. In duplex systems, which are often necessary, both sides are provided with a receiver and a transmitter, whereby data transmission is possible in both directions. One of
the advantages of the systems based on radio waves is that no visual communication is required and the directing of the transmitter and the receiver is not that crucial as in the case of an IR key. For this kind of short-range wireless data transmission there are several suitable solutions and standards, for instance Bluetooth, Zigbee and Zensys.

Using a battery in the lock requires low consumption of the lock’s energy both when the lock is in an active mode (i.e. it is being released or closed) and also during its period of inactivity (i.e. in a so-called sleep mode), when the lock is in an energy saving mode waiting for an opening command for instance from a key.

In the active mode the energy consumption of the system is quite high, as energy is required for producing the mechanical action of an actuator (electric motor or the like). The operating time of the actuator is easily of the order of 200 ms (100 ms for unlocking and 100 ms for locking).

During the active mode the power consumption of the processor and other electronics of the lock is generally quite low (usually a few mA) compared to the power consumption of the actuator. Even if the wireless link of the system were duplex, the energy consumption of the actual data transmission (the energy required by the transmitter of the wireless link) is relatively low compared to the energy consumption of the actuator, as the power consumption of the transmitter is typically in the approximate order of 15 mA. The supply voltage and the transmission time may be for instance about 5 V and 20 ms, respectively.

It is possible to make the power consumption of the electronics (processor, memories etc.) of the lock itself sufficiently low in the sleep mode by using the present solutions, but as the proportion of that time is large, the energy consumption in the sleep mode is still significant. A so-called polling function of the lock, i.e. the monitoring of the lock environment, is also related to the
sleep mode. Owing to the polling the lock is ready to react, if somebody wants release the locking by using a wireless key, for instance.

The energy consumption during the listening/polling by the receiver of the wireless link is a problem. The time for reacting to the opening command cannot be too long (in practise, not much longer than a second), as people are not willing to stand in front of the door waiting for the door to open. Since it is also impossible to foresee the moment someone wants to release the lock, one cannot use a clock, counter or another similar arrangement for awaking the lock and its electronics. This means in practise that the receiver needs to be active for instance once in a second and for as long as it takes to detect a potential opening command coming from a key. Thus, the transmitter in conjunction with the lock needs to poll the environment once in a second or even more frequently. If there is for instance no key with a message (e.g. a request for opening the door) in the environment of the lock during the polling, the lock needs to go back to the energy saving mode and wake up again after a second in order to listen to (poll) the environment. Even if the listening time of the transmitter was only 20 ms at intervals of one second, it makes altogether a significant daily energy amount thus discharging the energy source of the lock, e.g. the battery of the lock, even if the lock was not opened once.

The energy consumption is 10 joules per day, for instance, if the power consumption in the active mode is 200 mA, one unlocking/locking takes 200 ms, the lock is released/closed 50 times a day and the supply voltage is 5 V, whereas the energy consumption is about 85 joules a day, if the reaction time of the listening/polling by the wireless link is 1 s, the listening time 20 ms, the power consumption 10 mA during the listening and the supply voltage 5 V. The conclusion is that a significant part of the energy consumption of the lock provided with a wireless link consists of the energy consumed in the polling by the receiver.
A practical requirement is that a battery should in normal use last a relatively long time (preferably for years), whereby the battery needs to be sufficiently large or an energy source outside the lock needs to be used, i.e. wires outside the lock, which is something one often wants to get rid of, as already mentioned in the above.

An object of the invention is to minimise the disadvantages of the above-discussed prior art solutions. The object is achieved in a way described in the claims.

Brief description of the invention

The idea of the invention is to awake the receiver or transceiver of the wireless link of the lock, being in conjunction with the lock, only if the lock needs to be informed of something, e.g. opening/closing of the door, and which accordingly wakes the electronics of the lock. In this case the polling function of the wireless link is not necessary. The invention decreases the energy consumption in an energy saving mode to a considerable extent. However, the transition at a random moment of time from the energy saving mode (sleep mode) to an active mode is fast. It is a random moment of time from the viewpoint of the lock, as it cannot foresee the moment a key user wants to release the lock. The random moment of time is thus the moment, at which a key user uses a key to release the lock. This is accomplished, if the receiver or transceiver of the wireless link of the lock in conjunction with the lock, more briefly also called 'the wireless link of the lock' in the present text, is energized and activated by the energy transmitted by the key, whereby it may be a passive element. The required energy is drawn from the energy source of the key, typically from a battery. The activated link for its part awakes the actual lock, more precisely the electronics of the lock. The energy for the lock electronics is drawn from the lock's own energy source, typically from a battery.
The invention refers thus to a locking system, in which a wireless link is used for data transmission. The system comprises at least one lock, one key and one receiver or transceiver of the wireless link of the lock being in communication with the lock. The key comprises a transmitter or a transceiver, an energy source, from which the necessary energy is drawn at a random moment of time for transmitting key-specific data to the wireless link of the lock as well as the necessary energy for activating the wireless link of the lock. The energy required by the wireless link of the lock is transmitted to the receiver of the wireless link simultaneously with the data. The simultaneousness means that the data may be transmitted either precisely at the same time as the energy required by the link, or the respective transmission times differ slightly from one another (the energy transmission for instance starts slightly before the data transmission). What is essential is that no unnecessarily long delay is caused for the user. There is a second energy source available for the lock for drawing the necessary energy for activating the lock and for its operations in response to the message transmitted by the receiver of the activated link.

The invention also refers to a locking system of the same kind as the above-mentioned locking system comprising at least one passage control system and one transmitter/receiver of the wireless link included in the passage control system. In this system the key preferably comprises a remote identifier. The transmitter/receiver of the wireless link included in the passage control system comprises an energy source, from which the necessary energy is drawn at a random moment of time for transmitting an opening command to the wireless link of the lock and the necessary energy for activating the receiver of the wireless link of the lock. The opening command is based on the data received from the key. In this system the opening command and the energy are transmitted simultaneously to the receiver of the wireless link. There is a second energy source available for the lock for drawing the necessary energy for activating the lock and for its operations.
It is also possible to realise the invention as a combination of the above systems, whereby the energy required by the wireless link is drawn from the energy source of the key or from the transceiver of the passage control system.

The invention also refers to a method for a locking system, in which a wireless link is used for data transmission. In the method the key, which comprises an energy source and a switch, is activated to an operating mode in response to the turning-on of the switch taking place at a random moment of time. The key-specific data and the required energy are transmitted to the wireless link of the lock for energising and activating the wireless link of the lock. The wireless link of the lock is energised in response to the received energy and activated in response to the received data and the energising. Next, the lock comprising a second energy source is activated by transmitting a request from the link to the lock, whereby the necessary energy is drawn from the second energy source. The key-specific data received by the wireless link is read and the read data is checked. In response to the checking a potential operation is performed taking the necessary energy from the second energy source.

List of drawings

In the following the invention is described with reference to the attached drawings, in which

Figure 1 shows an example of an embodiment according to the invention;

Figure 2 shows an example of a second embodiment according to the invention;

Figure 3 shows an example of a third embodiment according to the invention;
Figure 4 shows an example of a flow diagram illustrating the method according to the invention.

Description of the invention

FIG. 1 shows an example of the system according to the invention. In the solution according to the invention the lock 16 does not poll the environment via its wireless link 7 as in the prior art solutions. The wireless link (i.e. more precisely the receiver or transceiver of the wireless link) is awakened by other means. The idea is to draw the energy required by the wireless link, as in solutions based on electromagnetic induction, from a key 1, i.e. from the energy source 5 of the key, which is usually a battery. After the wireless link 7 of the lock has been awakened, i.e. it has become active, the actual lock 16 is awakened. The lock takes the necessary energy from the energy source 9 of its own, e.g. from a battery. Thus, in the locking system according to the invention at least two different energy sources are utilised: the energy source of the key and the energy source of the lock. When the lock is in its energy saving mode the aim is to minimise the energy amount the lock takes from the battery.

The key 1 in the locking system according to the invention comprises a transmitter 3 (reader) of the wireless link, its antenna 2, an energy source 5, i.e. usually a battery, and an opening push-button 4. In addition, the key comprises a small-scale memory 17, which may be integrated inside the wireless link. The memory includes the marker of the key.

The wireless link 7 of the lock is a radio communication channel to the environment of the lock. In addition to the actuating member 7 itself, it comprises an antenna 6. The actuator is usually an electronics circuit. The energy (and data) 15 transmitted by the key via radio communication is received in the antenna 6, from which the actuator generates its own operational energy, i.e. its operational electricity. Thus, the wireless link does not need an
energy source of its own (e.g. a battery), but it may be a so-called passive unit as regards its operating principle. The actuator of the link is in communication with the actual lock 16 via the link interface 8 of the lock, so that data can be transmitted to the lock from a key (or another data source) as well as an interrupt message. The interrupt message is a command or request, by which the lock is told to interrupt the energy saving mode and go to an active mode. The wireless link of the lock may also be included in the lock instead of being an external element in communication with the lock. Therefore the wireless link of the lock in conjunction with the lock refers in this description to a receiver or transceiver of the wireless link located either outside or inside the lock unit.

The lock comprises an electronics circuit 10, a memory 18, a power management unit 120 and possibly a processor 19 (in larger applications). The memory stores key numbers, which indicate the keys authorized to release the lock. The electronics circuit receives its energy from the energy source 9 of the lock. The energy source is usually a battery, but it may also be another source, such as an electric conductor connection to the general electricity supply of the building. In addition, the lock is provided with a control circuit 11 for actuator for controlling the operations of the actuator 12. The actuator is in mechanical communication with the mechanical locking elements 13 (such as the dead bolt) of the lock, which are moved by the actuator for releasing or closing the lock. In the example of Fig. 1 the controller 11 of the actuator and the battery 9 are illustrated outside the electronics circuit, but they could as well be integrated into the circuit, i.e. be parts of the lock. Correspondingly, the memory, the power management unit and the processor included in the circuit 10 could be separate elements outside the electronics circuit.

The key (i.e. the reader of the wireless link) acting as a transmitter awakes the wireless link of the lock by the energy preferably included in the data transmitted by it. Thus the link gets its energy from the energy of the data
message. In other words, if nobody is in the process of releasing the lock (or there is nothing to report to the lock at a certain moment), the wireless link of the lock is not active, whereby it does not consume energy. Accordingly, the wireless link of the lock does not need any energy saving mode (sleep mode), as there is no need for it to wake up in order to react or listen. Polling according to prior art is thus not necessary.

A key transmits energy to the lock only if there is a need to release the lock by the key (i.e. the user of the key presses the opening push-button). The rest of the time the key electronics are totally de-energised or in a very low-current mode. Even if the power taken by the key from the battery in a transmission situation is fairly high (for instance about 0.5 W), the total energy consumption is low, as an individual key is used relatively seldom and the time required for a transmission of one opening command is short. The change and charging of the battery in a key is far easier to arrange than that of the battery located inside the actual lock, door or doorframe.

The lock (more precisely the lock electronics) instead is awakened by an interrupt command or request coming from the wireless link of the lock, which has already been activated by the energy included in the message from the key. In other words, also the lock is activated only if the lock needs to be used or informed of something. The lock may also for some reason be activated by itself (for instance in emergency situations, which the locking system is able to detect independently). The rest of the time the lock electronics are in a stand-by state (energy saving mode, sleep mode) consuming only very little power (a few microamperes).

FIG. 2 shows an example of a second embodiment according to the invention. In this example the invention is put into practice by using an RFID system (Radio Frequency Identification) as a part of the locking system. RFID is previously known technology for instance from electric identifying of items.
In the system according to the invention the RFID technology is, however, applied in a novel fashion.

In the prior art RFID applications (for instance bar code systems) either a stationary or a movable reader (RFID reader) is used for reading the data on the item. The reader may be in communication with external data networks or data systems. The item or the package thereof is provided with a remote identifier (RFID remote identifier). The data on the item is located in the remote identifier, from which the reader can catch it and forward the read data to data systems.

An RFID system has also been used for passage control in buildings. People carry along a remote identifier (acting as an electric key), which contains specific data on the remote identifier. Similarly, the passage control apparatus is provided with a reader (for instance at a door frame), which reads the data of the remote identifier, when it is taken into the vicinity of the reader. The passage control device checks the passage rights of the remote identifier on the basis of the read data.

In the example according to FIG. 2 the remote identifier is made an integrated part of the lock operation, especially of its data transmission and activation. The transmitter 23 of a key 21 is in practise an RFID reader, but it now transmits its marker to the RFID remote identifier located in the actuator of the link 27 of the lock, after the opening push-button 24 of the key has been pressed. The reading, i.e. data transmission, is carried out via radio communication 217 through the antenna 22 of the key and the antenna 26 of the wireless link of the lock. In the data transmission the RFID reader transmits energy and data on the key to the RFID remote identifier. The necessary energy is drawn from the energy source 25 of the key.

It is to be noticed that in practise the key may be composed around the RFID reader. Thus, it can be concluded that the key is an RFID reader. The shape
of the key 21 in FIG. 2 illustrates such an example, where the necessary elements are located inside a common enclosure. It should, however, be mentioned that the key may also have a mechanical key section, as is shown in FIG. 1.

5
The remote identifier in the link is passive, i.e. it has not an energy source of its own, but it takes the required energy from the energy transmitted by the reader. The necessary input power is nowadays quite low, approximately of the order of a few \( \mu \)W’s. The actuator 27 of the link is in communication with the actual lock 218 via the link interface 28 of the lock, so that data can be transmitted to the lock from a key (or another data source) as well as interrupt information.

10
The electronics circuit 210 receives the data and the interrupt message from the interface and performs the awakening, i.e. activation, of the lock. The energy is drawn from the lock’s energy source 29 through a power management unit 214. In this example the power management unit is separated from the electronics circuit 210 of the lock, but it may also be connected to the circuit in question. The power management unit takes care of the energy supply to the other parts of the lock, in other words the lock electronics including the processor thereof and the locking sensor 215 receive supply voltage VCC and the controller of the actuator and the actuator itself get supply voltage VDD. VCC and VDD may also be one and the same supply voltage. The power management unit is also controlled by the processor’s request/command R to move the lock into an energy saving mode.

15
The memory of the key electronics stores key numbers, which indicate the keys authorized to release the lock. Thus, the electronics circuit receives its energy from the energy source of the lock. The energy source is usually a battery, but it may also be another source, such as an electric conductor connection to the general electricity supply of the building. In addition, the lock is provided with a control circuit 211 for actuator for controlling the op-
erations of the actuator 212. The actuator is in mechanical communication with the mechanical locking elements 213 (such as the dead bolt) of the lock, which are moved by the actuator for releasing or closing the lock. A locking sensor 215 controls the mode of the locking and transmits the mode data to the electronics of the lock. Further, the figure shows also a parallel alternative for releasing the lock through a mechanical element 216 (a key cylinder).

If a duplex service between the RFID reader (i.e. in practise the key) and the RFID remote identifier (i.e. in practise the lock) is desired, a so-called backscatter modulation may be utilised.

In practise, also a so-called anti-collision method is required for the embodiments of both FIG. 1 and 2, since there may be several doors (RFID remote identifiers) and keys (RFID readers) within the range of the system.

The RFID reader may be either an independent device (i.e. the RFID reader is a key) or it may be arranged as a part of another device (for instance of a mobile phone).

The system shown in FIG. 2 operates on radio waves at a frequency of 869 MHz based on the RFID standard proposal ISO 18000-6 (but does not necessarily follow it precisely). A similar operation may also be performed e.g. at a frequency of 13,56 MHz and for instance by using magnetic induction, if so required. The range of the key, though, may then be less than one meter and the size of the antennas significantly larger.

If the aim is to arrange an RFID reader into a very small device, a higher frequency may be used, for instance 2,45 GHz, for which there is also an RFID standard proposal ISO 18000-4. Then the size of the antennas will also be smaller.
In the above-mentioned systems there is no need for a battery for the wireless link of the lock.

FIG. 3 shows an embodiment according to the invention comprising a passage control apparatus (Access Control System) or the like. The lock 218 and the wireless link 27 of the lock located at a door 14 are similar elements as those in FIG. 2 (software differences might occur). The key 31 is now provided with an RFID remote identifier 33 (not with an RFID reader) and it is in communication 36 with the passage control system 310 through an RFID reader 38 included therein. The separate RFID reader 38 included in the passage control system monitors its coverage area and is in communication with the keys within the area. The communication may be link communication (e.g. radio communication), which is continuously turned on or link communication, which is intermittently turned on (e.g. at intervals of a few seconds).

In practise, the communication exists between the antenna 32 of the key and the antenna 39 of the passage control reader.

If a key is authorized to open the door controlled by the reader of the passage control, the passage control system 310 transmits this information through the reader 38 to the RFID remote identifier of the wireless link of the lock, which forwards it to the lock, which is then released. That being the case, it is not necessarily the lock that makes the decision about releasing the lock, but that is the task of the passage control. Thus, the passage control has the necessary information about the rights of the keys. At the same time as the information about the release the lock is transferred 37 to the wireless link of the lock, also the energy required by the wireless link of the lock is transferred. If there are several locks and passage control readers within an overlapping coverage area, the lock can be provided with a lock-specific code, by which the opening requests intended for the lock can be distinguished from other opening requests. Then the opening request needs to contain the lock specific-code. The wireless links of the locks within the same coverage area receive the same opening request, but only the wireless
link of the right lock awakens the lock electronics. It is thus advantageous to check the code in the link and not in the lock electronics in order to avoid unnecessary activation of the lock, whereby the energy source of the lock will neither be used in vain.

Also in this system a duplex communication between the RFID reader (i.e. in practise the passage control apparatus) and the RFID remote identifier (i.e. in practise the lock) can be arranged by utilizing the above-mentioned backscatter modulation. Then the lock may wake up for instance by means of the dead locked interrupt of a locking sensor (or similarly by means of the mode data sensor of the lock, not shown in the figure), after which the lock electronics report this through the RFID remote identifier of the lock to the passage control apparatus by utilising for instance the above-mentioned backscatter modulation. By using this method the lock may report for instance a potential burglary attempt to the system.

Also a duplex communication between the RFID reader of the passage control apparatus and the RFID remote identifier of the key can be arranged applying the same principle.

In this embodiment the cost of the keys is considerably lower and their size much smaller, as in this case the key is not an RFID reader, but a far simpler and less expensive RFID remote identifier. Since the remote identifier does not necessarily require a battery (i.e. it is a passive remote identifier), its operating life is practically unlimited. Also a battery may, however, be included in the key, whereby it is possible to add to the functions of the key. Thereby for instance an active or a semi-active RFID remote identifier are possible arrangements, as mentioned in the above.

Also in this embodiment there can be naturally several remote identifiers of keys and locks within the same area, whereby an anti-collision method is required.
One passage control apparatus may control several doors by one RFID reader, if its range is sufficiently wide. In addition, several RFID readers may be connected to one passage control apparatus, whereby the range (coverage area) of the system may be considerably widened.

It is also possible to have an embodiment, in which the solutions according to FIGS. 2 and 3 are combined. In other words, if the key is an RFID reader, it may be in direct communication with the lock, and if the key is an RFID remote identifier, it is in communication with the passage control system, which transmits the necessary data to the lock. This embodiment requires an efficient anti-collision method (for instance a frequency or time division).

In the embodiments according to FIGS. 1 – 3 the wireless links in the locks and the transmitters in the keys are shown as one-circuit arrangements. In other words, the wireless link of the lock in conjunction with the lock comprises one circuit unit and correspondingly, the transmitter of the key comprises one circuit unit. It is, however, possible that the wireless link of the lock consists of several circuits, e.g. of two circuits, of which the first one is meant for awakening the lock and receiving the energy transmitted from the key or the passage control, and the second one is a circuit used for receiving and/or transmitting data. Similarly, the key may have two circuits (or even several circuits set up for a specific purpose), of which the first one transmits data and the second one energy. Thus, there are several variations for realising the circuit on the side of the wireless link of the lock and the key and these can be realised irrespectively of the realisation of the opposite side of the link as long as they have a common interface between them. Thus, in this text the receiver, transmitter and transceiver of the wireless link refer to all possible embodiments thereof.

FIG. 4 shows an example of a flow diagram illustrating the method according to the invention that is meant to use in a locking system wherein there exists
an energy source both in the key and in the lock. In view of normal usage the key de-energised in the initial situation, as is also the wireless link of the lock. The lock electronics are in a low-current mode, i.e. in a sleep mode (or in some applications de-energised). During the sleep mode the energy is drawn from the energy source of the lock. In the initial situation of this example the lock is latched also by mechanical locking elements (i.e. the dead bolt is out). The locked state does not require any operation of the actuator. In other words, the actuator does not consume any energy in the locked state.

When the aim is to release the lock, the key is activated 41 to an operating mode in response to the turning-on of the opening switch, i.e. to the pressing of the opening push-button. Then the electricity for the key is switched on. The energy is drawn from the energy source of the key. Next, an opening command/request is transmitted 42 from the key to the lock. The opening command contains the marker of the key. At the same time the opening command contains enough energy for activating the wireless link of the lock. It is preferable to transmit the marker and the necessary energy together, but it is also possible to transmit the marker and the energy separately, for instance at different frequencies (through different channels). The opening command/request should be understood so as to contain both the marker of the key and the necessary energy regardless of the technical realisation of the transmission. The transmission energy is taken from the energy source of the key.

In response to the energy of the opening command, the wireless link of the lock is energised 43, i.e. an energy source is connected to the link. By utilizing the received energy transmitted by the key the wireless link of the lock is activated, i.e. awakened, 44. Further, the activated link transmits an interrupt request or command to the lock electronics, whereby the sleep mode of the lock is interrupted and the lock wakes up. In other words, the lock electronics are activated 45. The activated lock reads 46 the opening command
transmitted by the key, i.e. in practise the marker of the key, which the lock receives from the wireless link of the lock. The activated lock takes the necessary energy from the lock’s own energy source. The read marker is checked 47 in order to verify the validity of the opening command. The marker of the key is compared with the numbers stored in the lock memory and on the basis of the data in the memory it is verified whether the key indicated by the marker has a right to release the lock.

On the basis of the checking a potential operation is performed 48. If the key has a right to release the lock, the lock electronics take care of the releasing of the lock by means of the actuator. The energy is drawn from the power source of the lock. If the key does not have a right to release the lock, the door remains locked. In addition, it is possible to inform the centre of the locking system, if there is any, about the opening attempt. The released lock goes back to the sleep mode preferably after a certain delay, i.e. the lock electronics become de-energised or almost de-energised. The wireless link of the lock will become de-energised after the energy transmitted to it by the key has run out. It is also preferable that the lock goes back to the locking mode after a certain time from the opening. This may be realised so that after a certain time from the opening of the lock the lock electronics may wake up automatically and close the lock by the help of the actuator. After this, the lock goes back to the sleep mode.

The steps of the method according to FIG. 4 may be performed also in another order, if the embodiment of the invention so requires. For instance the key marker, the opening command or another marker may be checked already by the wireless link, and only in case the operation is legal and necessary, the lock electronics will be activated. In other words, steps 46 and 47 of FIG. 4 are practised before step 45. Then the wireless link of the lock contains the necessary data, i.e. the rights of the key.
It may also be the case that the key does not communicate directly with the lock, but only through the passage control apparatus, which checks whether the key in question is entitled to open the door. If it is authorised to open the door, the passage control apparatus will transmit an opening command to the lock. So, in this arrangement it is not necessarily the lock that decides whether somebody is allowed to open the door, but that is the task of the passage control apparatus. Accordingly, the opening command from the key to the passage control apparatus is read and checked by the passage control apparatus. In other words, steps 46 and 47 of FIG. 4 are practised before step 42. In this case the key-specific data transmitted to the wireless link of the lock refers to an opening command.

The embodiments according to the invention may also comprise various kinds of applications. The wireless link of the lock may for instance check first the general code transmitted by the key, whereby it is verified that the key is included in the system (even if not allowed to release the lock). By the general code it is ensured that something else (or a disturbance) operating at the same frequency does not unnecessarily awake the lock electronics.

The lock electronics may also transmit data (e.g. a random number) to the key via the wireless link, which data is transformed for instance by a code and returned back by the key. This operation may be utilized for instance for encryption of data. The operation requires that the link communication is duplex, i.e. there is a transceiver at both ends of the link. Thereby there are either respective channels in both directions or the same channel is used for transmitting data alternately to the lock and the key. The operation may also be arranged by using backscatter modulation technology described in the above.

To allow the release of the lock may also be the task of the key, whereby its memory contains the data (markers or the like) on the locks that may be released by the key in question. In this case it is not necessary to store this
data in the lock, whereby the operation of the lock will be simplified. This could be a suitable method (cf. FIG. 4) in case the key is for instance a mobile phone, which has enough memory and processing capacity and the data in which is easier to update, i.e. to add the most recent information, than in the case of a lock attached to a door.

A key or a similar device (for instance a passage control apparatus), which is located at a communication distance from the lock may also transmit energy (and data) continuously, or for instance by pulsing, to the wireless link of the lock, but if the right code (e.g. the opening command of the lock) is not received, the wireless link of the lock does not activate the lock electronics. Thus, the energy of the lock battery is not used in vain. This kind of situation may be preferable for instance in the case of an object provided with passage control, in which the passage control apparatus communicates with both the lock and the key. Then, there does not necessarily have to be an opening push-button in the key, but it has to be taken into account that the operating life of the energy source is shorter, if the key transmits energy continuously.

In the initial situation the key may also be in a low-current mode (sleep mode), and not totally de-energised. In the same way the wireless link of the lock may be in a low-current sleep mode, but it does not poll the keys with its receiver. In this case the energy is drawn for instance from the battery of the lock.

Also the lock electronics may awaken the wireless link of the lock, if the lock electronics for instance want to communicate with similar kind of devices in the vicinity thereof (e.g. with the passage control apparatus provided with a wireless link), even if they would not have anything to communicate with the lock at that moment.

For a moment the wireless link of the lock may also take its energy for instance from the battery of the lock, and after the link has been activated,
start using the energy coming through the wireless link of the passage control apparatus, key or another similar device.

The wireless link of the lock may initially use also the energy coming from the transmitter (e.g. from the key) and then start using the lock's own battery as an energy source. In other words, in this version the wireless link of the lock is only activated by the energy transmitted by the key and after that the energy required for the actual data transmission is drawn from the battery of the lock.

The energy may, instead of a battery, be also drawn from an accumulator, condenser or another similar energy storage.

The embodiments disclosed in this text are applied to an electro-mechanical lock, but the wireless link according to the invention may also be used in other applications, in which a device or system needs to be awakened from the energy saving mode quickly and by a small amount of energy without knowing in advance when the awakening is going to take place, and without polling.

In the light of the above it is apparent that the invention may also be realised by such embodiments that are not described in this text. Thus, the invention is not limited to the above-described examples only, but it can be utilised also in a plurality of other practical applications within the scope of the inventive idea.
CLAIMS

1. A locking system, in which a wireless link is used for data transmission and which comprises at least one lock, one key and one receiver of the wireless link of the lock being in communication with the lock, the key comprising a transmitter of the wireless link, and an energy source from which the necessary energy is drawn at a random moment of time for transmitting key-specific data to the wireless link of the lock as well as the necessary energy for activating the wireless link of the lock, which energy is transmitted to the receiver of the wireless link simultaneously with the data, characterised in that there is a second energy source available for the lock for drawing the necessary energy for activating the lock and for its operations in response to the message transmitted by the receiver of the activated link.

2. A locking system according to claim 1, characterised in that the receiver of the wireless link of the lock being in communication with the lock also comprises a transmitter, and the transmitter of the wireless link of the lock located in the key comprises a receiver.

3. A locking system according to claim 1 or 2, characterised in that the key comprises an RFID reader and the receiver of the wireless link in communication with the lock comprises an RFID remote identifier.

4. A locking system according to claim 1, 2 or 3, characterised in that the receiver of the wireless link of the lock being in communication with the lock is a passive element.

5. A locking system according to any one of claims 1 - 4, characterised in that the receiver of the wireless link of the lock being in communication with the lock is a part of the lock.
6. A locking system according to any one of claims 1 - 5, characterised in that the second energy source is a part of the lock.

7. A locking system according to any one of claims 1 - 6, characterised in that the lock consists of an electronics section, an actuator and mechanical locking elements.

8. A locking system according to claim 7, characterised in that the electronics section comprises a processor.

9. A locking system according to any one of claims 3 - 8 and claim 2, characterised in that data is transmitted also to the key through the wireless link of the lock.

10. A locking system according to any one of claims 1 - 9, characterised in that the lock or the receiver of the wireless link of the lock being in communication with the lock contains the data on the keys, which are entitled to release the lock.

11. A locking system according to claim 10, characterised in that the lock or the receiver of the wireless link of the lock being in communication with the lock checks whether the lock is allowed to be released by a certain key, on the basis of which checking the lock is released, if the key is authorised to release the lock in question.

12. A locking system according to claim 9, characterised in that the key has data on the locks, which it is entitled to release, whereby the key may allow the release of the lock on the basis of the lock-specific data transmitted from the lock, whereby an opening request may be transmitted to the lock, which request is fulfilled by the lock.
13. A locking system according to any one of claims 1 - 12, **characterised** in that the key and/or the receiver of the wireless link of the lock being in communication with the lock are in a low-current mode.

14. A locking system according to any one of claims 1 - 13, **characterised** in that the receiver of the wireless link of the lock being in communication with the lock takes the necessary energy from the second energy source except for the awaking of said receiver, or the receiver of the wireless link of the lock takes the energy for awaking the lock from the second energy source and the rest of the required energy from the key.

15. A locking system according to any one of claims 1 - 14, **characterised** in that also the lock may awake the receiver of the wireless link of the lock being in communication with the lock.

16. A locking system according to any one of claims 1 - 15, **characterised** in that the system comprises an anti-collision system.

17. A locking system according to any one of claims 1 - 16, **characterised** in that the key is a part of a mobile phone.

18. A locking system, in which a wireless link is used for data transmission and which comprises at least one lock, one key and one receiver of the wireless link of the lock being in communication with the lock, one passage control system and one transmitter/receiver of the wireless link included in the passage control system, the key comprising a remote identifier, **characterised** in that the transmitter/receiver of the wireless link included in the passage control system comprises an energy source, from which the necessary energy is drawn at a random moment of time for transmitting an opening command to the wireless link of the lock, which opening command is based on the data received from the key, as well as the necessary energy for activating the receiver of the wireless link of the lock, which energy is
transmitted to the receiver of the wireless link simultaneously with the opening command, and that there is a second energy source available for the lock for taking the necessary energy for activating the lock and for its operations in response to the message transmitted by the receiver of the activated link.

19. A locking system according to claim 18, characterised in that the receiver of the wireless link in communication with the lock comprises an RFID remote identifier, the transmitter/receiver of the wireless link included in the passage control system comprises an RFID reader and the key comprises an RFID remote identifier.

20. A locking system according to claim 18 or 19, characterised in that the receiver of the wireless link in communication with the lock also comprises a transmitter.

21. A locking system according to any one of claims 19 - 20, characterised in that in addition to said keys the system comprises at least one key, which includes a transmitter of the wireless link and an energy source, from which the necessary energy is drawn at a random moment of time for the transmitting key-specific data to the wireless link of the lock, as well as the necessary energy for activating the wireless link of the lock, which energy is transmitted to the receiver of the wireless link simultaneously with the data.

22. A locking system according to any one of claims 18 - 21, characterised in that in the system the lock, the receiver of the wireless link of the lock being in communication with the lock or the passage control system checks whether the key is entitled to release the lock in question, on the basis of which checking the lock is possibly released.

23. A locking system according to any one of claims 18 - 22, characterised in that the system comprises an anti-collision system.
24. A locking system according to any one of claims 18 - 23, \textit{characterised} in that the key is a part of a mobile phone.

25. A method for a locking system, in which a wireless link is used for data transmission and which comprises at least one lock, one key and one receiver of the wireless link of the lock being in communication with the lock, the key comprising a transmitter of the wireless link, the method, in which method:

- activating the key, which comprises an energy source and a switch to an operating mode in response to the turning-on of the switch taking place at a random moment of time,
- transmitting key-specific data and the required energy for energising and activating the wireless link of the lock to the wireless link of the lock,
- energising the wireless link of the lock in response to the received energy,
- activating the wireless link of the lock in response to the received data and the energising,
- reading the received key-specific data,
- checking the received data,

\textit{characterised} in that the method further comprises the next phases:

- activating the lock, which comprises a second energy source, by transmitting a request from the wireless link of the lock to the lock, whereby the necessary energy is drawn from the second energy source,
- performing a potential operation in response to said checking taking the necessary energy from the second energy source.

26. A method according to claim 25, \textit{characterised} in that the key-specific data and the required energy for energising and activating the wireless link of the lock are transmitted simultaneously.
27. A method according to claim 25 or 26, characterised in that said wireless link is duplex, whereby said receiver comprises a transmitter and said transmitter comprises a receiver.

28. A method according to claim 25, 26 or 27, characterised in that the lock may awake the receiver of the wireless link in communication with the lock.

29. A method according to any one of claims 25 - 28, characterised in that the step of reading the received data and the step of checking the read data are practised before the step of activating the lock.

30. A method according to any one of claims 25 - 28, characterised in that the system also comprises a passage control apparatus including at least one transmitter/receiver, whereby parallel with the activating step there is an alternative step, in which the transmitter/receiver of the passage control apparatus is activated at a random moment of time.

31. A method according to claim 30, characterised in that the step of reading the received data and the step of checking the read data are practised before the transmission of the key-specific data and the required energy to the lock.
ACTIVATING THE KEY TO AN OPERATING MODE IN RESPONSE TO TURNING-ON OF THE SWITCH

TRANSMITTING THE OPENING COMMAND TO THE LOCK

ENERGISING THE WIRELESS LINK OF THE LOCK IN RESPONSE TO THE OPENING COMMAND

ACTIVATING THE WIRELESS LINK OF THE LOCK IN RESPONSE TO THE OPENING COMMAND AND AND THE ENERGISING

ACTIVATING THE LOCK ELECTRONICS

READING THE OPENING COMMAND

CHECKING THE VALIDITY OF THE COMMAND

PERFORMING A POTENTIAL OPERATION ON THE BASIS OF THE CHECKING
**INTERNATIONAL SEARCH REPORT**

**INTERNATIONAL APPLICATION NO.**  
PCT/FI 2004/000684

**A. CLASSIFICATION OF SUBJECT MATTER**

**IPC7: E05B 47/00**  
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)

**IPC7: E05B, G07C, B60R**  
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE, DK, FI, NO classes as above

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

**EPO-INTERNAL**

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>US 5920268 A (G.BUCCI ET AL), 6 July 1999 (06.07.1999), abstract</td>
<td>1-31</td>
</tr>
<tr>
<td>A</td>
<td>WO 9744557 A2 (PONENZIANI, PAOLO), 27 November 1997 (27.11.1997), abstract</td>
<td>1-31</td>
</tr>
<tr>
<td>A</td>
<td>EP 1338734 A1 (ZHAI, XIAO MING YANGZHOU), 27 August 2003 (27.08.2003), abstract</td>
<td>1-31</td>
</tr>
</tbody>
</table>

[X] Further documents are listed in the continuation of Box C.  
[X] See patent family annex.

<table>
<thead>
<tr>
<th>Special categories of cited documents:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;A&quot; document defining the general state of the art which is not considered to be of particular relevance</td>
</tr>
<tr>
<td>&quot;E&quot; earlier application or patent but published on or after the international filing date</td>
</tr>
<tr>
<td>&quot;L&quot; 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)</td>
</tr>
<tr>
<td>&quot;O&quot; document referring to an oral disclosure, use, exhibition or other means</td>
</tr>
<tr>
<td>&quot;P&quot; document published prior to the international filing date but later than the priority date claimed</td>
</tr>
<tr>
<td>&quot;T&quot; 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</td>
</tr>
<tr>
<td>&quot;X&quot; 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</td>
</tr>
<tr>
<td>&quot;Y&quot; 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</td>
</tr>
<tr>
<td>&quot;&amp;&quot; document member of the same patent family</td>
</tr>
</tbody>
</table>

**Date of the actual completion of the international search**  
10 February 2005

**Date of mailing of the international search report**  
11-02-2005

**Name and mailing address of the ISA/ Swedish Patent Office**  
Box 5055, S-102 42 STOCKHOLM  
Facsimile No. +46 8 666 02 86

**Authorized officer**  
Lars Jakobsson /itw  
Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (January 2004)
<table>
<thead>
<tr>
<th>Category*</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>DE 3735470 A1 (FRANZEN SICHERHEISTECHNIK GMBH &amp; CO), 3 May 1989 (03.05.1989), abstract</td>
<td>1-31</td>
</tr>
<tr>
<td>Country</td>
<td>Application Number</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EP</td>
<td>1338734 A1</td>
<td>27/08/2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td>3735470 A1</td>
<td>03/05/1989</td>
</tr>
</tbody>
</table>