

Selection of Authentication Systems for Hungarian Health Care, Based on Physiological Study

Part II.

The RFID Systems

BARÁTH Artur

The actuality of the topic indicated in the title comes from more and more events where the verification of identity might be required. Health-care is an important part of critical national infrastructures. A primary task of the protection of critical information infrastructures consists in the access control of data managed by IT system where the identity-authentication forms an important part. For this reason, the technologies considered suitable for use and their supporting means are listed. After examining and comparing the relevant parameters, the optimum solution for the authentication procedures in the Hungarian health care system is specified. First of all, the modern and efficient biometric identification processes are examined; however, the possession-based Radio Frequency Identification (RFID) as an additional system is also studied. Due to the well-known problems of passwords and chip cards. They were deliberately omitted during the system planning and efforts were made to exclude the human factors from the planned authentication system as much as possible.

Keywords: authentication, biometry, RFID, health care, human factors

Study of RFID Systems

In general, it can be said that the radio frequency identification systems serve for identification of goods, products or persons by using radio frequency data transmission. The communication takes place between the writing/reading device (reader) and the electronic data carrier unit (transponder) at a frequency corresponding to the external conditions and the required reading distance.

Basically, two types of systems in service are distinguished:

- *Passive system* – the transponder has no dedicated power supply; the energy required for the signal transmission is obtained from the electromagnetic field generated by the reader.
- *Active system* – the transponder has its own power supply and emits its identification signal either continuously or on call received from the reader.

Passive System

The data to be identified are stored in a circuit provided by an antenna and a memory (transponder). For data acquisition, a so-called reader is used. The RF3 signal modulated by the control data will be amplified in an amplifier unit and radiated through an antenna system. Within the range of a reader, the radiated signal induces power supply by means of the transponder antenna in the transponder circuit. The transponder addressed radiates a reply signal corresponding to the data read from its memory back to the reader. The reader forwards the signal reflected by the transponder by means of an amplifier and a demodulator to the processing computer. Thus, using the RFID, the necessary information becomes accessible in a simple way, quickly and reliably without physical contact. [1] Figure 1 shows the block diagram of passive system.

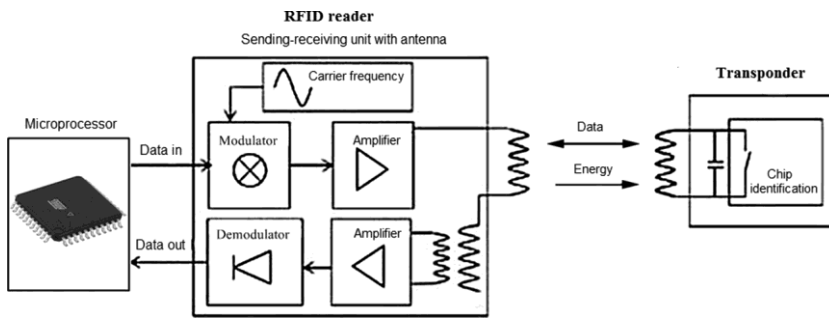


Figure 1. Block diagram of passive system. (Made by the author.)

Active System

Having its own power supply, the transponder radiates its identification signal continuously, or, in a so-called semi-active mode, in reply to the signal radiated by the reader, the transponder radiates a reply signal corresponding to its identifier stored in its memory by using its own power supply to the reader.

The use of RFID technology in access control systems was the prime mover of system development. According to the different security level of access control systems various card types (transponders) were developed that can be characterized by the type of memory, coding of identification data, and the range of reading.

In the operating principle of a system a number of groupings in addition to the two ones already made by power supply to transponder can be used. The most important features of RFID systems are: operating frequency and range of reader as well as the mode of coupling. The range of reading depends on many factors, but the most important ones are the power supply to the transponder and the mode of data transfer to the reader. Various couplings are used for this purpose. [1]

The systems can operate in a very wide frequency range from 13 kHz to 5.8 GHz. The available range extends from a few mm to 15 m in passive transponders and from 20 m to 100 m in active systems.

The large international frequency management organizations allocated four frequency classes for the purpose of RFID:

- low frequency (LF) RFID identification;
- high-frequency (HF) RFID identification;
- ultra-high frequency (UHF) RFID identification;
- microwave frequency identification RFID.

The coupling procedures of transponders specify the way in which the reader and the transponder can contact each other. The different coupling modes can be classified according to the coupling range i.e. close, vicinity and long-range. The range of close coupling lies within 0.01 m, the vicinity one between 0.01 and 1 m while the long range one exceeds one meter.

Connection procedures

The different coupling modes can be classified based on the physical properties of the coupling. Based on this, inductive, capacitive, magnetic, and backscatter couplings are distinguished. The capacitive and magnetic couplings are used in close-coupled systems, inductive coupling usually in vicinity-coupled systems, and the backscatter coupling in long range systems. In the present environment the subject of importance is that the operating conditions of medical devices shall be taken into account, while taking care that the radio frequency communication shall not cause problems during operation. [1]

Inductive coupling: “With the view of power supply to the transponder, the reader antenna generates a high-frequency electromagnetic field. The C_r capacity connected parallel to the reader antenna coil form a resonant circuit with a resonant frequency corresponding to the data transfer frequency of the reader. The transponder antenna-coil and the C_1 capacity connected parallel are tuned to the data transfer frequency of the reader, resulting in the voltage drop across the coil takes its maximum.” [1] (Figure 2)

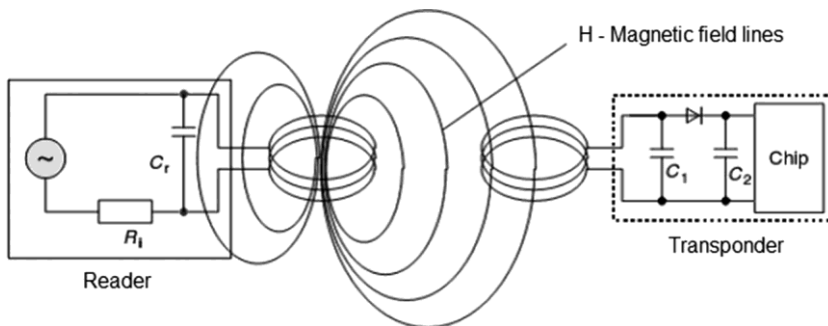


Figure 2. Model of connection. (Made by the author.)

Capacitive coupling: “Capacitive coupling requires no antennas, instead a pair of electrodes. Both the reader and the transponder have a conductor plate each that together form a capacitor. Of course, the realization of coupling requires the two plates to be parallel to each other. The transponder microchip located between two plates, one of which forms a capacitor with the plate of the reader and the other one with the ground. The voltage between the two plates of the transponder serves for power supply to the transponder microchip.” [1] (Figure 3)

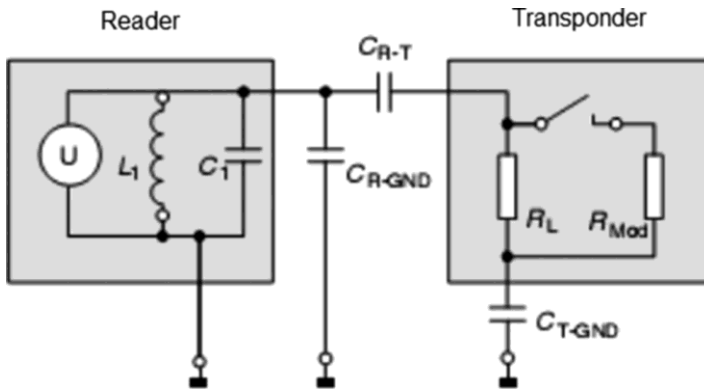


Figure 3. Capacitive coupling. (Made by the author.)

Magnetic coupling: “The magnetic coupling is very similar to the inductive one in that the antenna of transmitter and receiver form a transformer. The difference lies in that the antenna coil of the reader consists of a ferrite core provided with a circle- or U-shaped coil.” [1]

Backscatter coupling: “Only a small part of power P_1 radiated by the antenna of the reader reaches the antenna of the transponder (due to the section attenuation and undirected antennas) After rectification, the high-frequency voltage generated by the power P_1 coming to the transponder is capable of reviving the integrated circuits of the transponder. Part of the power P_1 is reflected by the antenna that comes back to the reader as an energy P_2 . The reflection characteristics of the antenna can be modified by altering the load connected to the antenna. Accordingly, during the transponder to reader communication a loading resistor R_L that can be switched on/off is connected in series with the antenna. Switching it on and off, the data stream can be transferred. Thus, the P_2 output power can be modulated (modulated backscatter). The reflected power P_2 is also attenuated in space according to the outdoor attenuation, and therefore only a small fraction separated from the original signal comes to the reader so as to be able to be processed by the reader.” [1]

Kinds of RFID Chips

In the description of RFID technology based identification, the element called a transponder is also very important. The chip carries the data of the person to be identified. During employment, a transponder is assigned to the person. This relationship will be stored in a database and processed using software. Due to cost-effectiveness, typically passive chips will be proposed to be used; yet, in view of the more accurate and more reliable operation, the selection of active chips is preferred.

Passive LF Chip

Passive timing chip, not programmable, contains a factory made unique identifier. The chip is mounted in a special plastic envelope that protects it against external physical impact and ensures practical wearing. It is reusable; therefore it could be used even in the further development in case of patients as well.

Active LF Chip

An active transducer used in the system is equipped with an internal energy source, which results in the production cost being multiplied; in exchange two wires as an antenna are sufficient. In addition, the operation is more efficient by one order of magnitude. Since the position and fixing of the connection points in this device allow more flexible solutions, the system provides more options. As the costs are much higher in case of this system, the application is likely still to come.

Passive UHF Chip

It is the write-once and read-many times chip that seems to be the best alternative. A capacitive coupling to the reader is used; therefore the antenna is designed as an armature with a relatively large surface. These chips were originally developed and produced as identifiers for one of the largest buyer markets of the RFID technology for the purpose of tracking goods in logistic systems. Due to the high volume of orders, it can be purchased from manufacturers at low cost; therefore it can also be used in a non-recurrent way. The efficiency of these chips has deteriorated in a wet environment and therefore their use for measurement causes problems if shaded by the human body or covered by wet or sweaty clothing. This problem can be solved by using a spacer that provides the necessary distance of two to-three mm away from the human body.

Battery Assisted Passive (BAP) Chip

The BAP chips contain a battery plate built in a passive chip that contributes to the power supply required to wake up the chip and increase the energy level of the reply signal. This allows measurements at distances of as much as 100 m. BAP chips preserve their charge for 2.5 years, then they continue to operate as common passive chips.

Reader (Reader and Data Collector)

To obtain data to be identified and stored on the chip a so-called reader is used to produce the signal that powers the antenna to generate the appropriate electromagnetic field. It is another task to detect the data radiated back by the chip and, by processing them, to obtain the necessary information. The data thus obtained are stored in its memory and transmitted to the computer connected to it, which, in turn, saves the data by means of software into a remote database. Thus, a safe system is implemented, should the backup of data in the remote database fail; data can be found in the storage of a reader and transferred again.

It may have its own power supply, so that the operation is not affected by any power supply failures, yet, the power supply to the other components of the system shall remain operative.

In case of appropriate types of chips, certain RFID readers are also capable of writing not only reading. In practice, this means that information can be added to or deleted from the data stored in the chip's memory.

The proper communication requires an RFID/UHF reader. Depending on its design, it is capable of controlling 4 or 8 antennas. The high data bandwidth and advanced anti-collision algorithm allows for 430 chips/sec reading speed, therefore it is primarily used in applications with a large number of chips. It is powered by internal battery or an external power supply.

In getting acquainted with the technology and equipment one can realize that a system of proper configuration can be developed. In my opinion, the RFID is suitable to be used even as a basic system, i.e. in applications where problems of authority arise in respect to use – e.g. elevator, door instrument. A further advantage is that, in case of proper design, the position of employees wearing individual chips can be known at any time, which is a significant aspect in emergency situations. The possibility of improvement is also given in fact; it is not only the employees that can be provided with RFID but also the patients for the time of treatment in hospital. The biometric system can be used as an additional identification system if required by the circumstances.

Conclusions

The studies have shown that the benefits of biometric systems are clear while their disadvantages are far from those unable to be managed. From among the systems studied, it is the fingerprint testing system that is considered the most appropriate one and its use is proposed as supplementary equipment in the applications as follows:

- computer login in every case;
- entry to any surgical environment;
- access particular high-value assets;
- entry to ICU.

Of course, the certification can happen only if, in addition to the positive result of additional test, the admission from the principal system is also obtained by the person to be identified. It is the RFID technology that is selected as the main authentication system. In my opinion, each and every employee should wear a chip integrated in a wrist strap so as to be at hand any time without taking any trouble with it. It can be used in any case without obstructing the life of the wearer and its loss is properly hindered. As a result of study the structure set on the basis of preliminary expectations has been changed and the application fields of procedures interchanged.

Raising the range of systems described above to a national level, the permeability between institutions will be made feasible due to the possibility of configuring the authority levels at an institutional level. Thereby any employee wearing a RFID wrist strap can have admission to any health care institution in the country; thus those employed by several employers – as it is very frequent in Hungarian health care at present – can be identified by the same wrist strap.

As a further development, the use of a wrist strap could be extended to bed-ridden patients as well, that would improve the possibility of control and safety.

This study fails to define the technology to be applied; in fact, by the time that the study came to the phase of implementation, any and all equipment up-to-date at present would – fortunately – virtually be outdated due to technical development. The detailed specification of equipment shall be made at the time the introduction of the Unified Health-Care Authentication System becomes opportune.

Reference

- [1] IMRE S. et al.: *Examination of RFID Systems In Terms Of Consumption and Technology*. (In Hungarian). www.rfid.answer.hu:8080/site/kutatasi-erdmenyeink/radios-megoldasok/2006/rfid-rendszerek-vizsgalata-felhasznalas-es-technologia-szemponjtjabol.pdf/view (downloaded: 12 02 2012)