IDENTITY MANAGEMENT IN RFID APPLICATION

by

EVA FIALOVÁ[*]

The RFID technology serves to identify objects and persons at distance using radio frequencies. On RFID chips data about individuals are stored and can afterwards be processed in a privacy infringing way. Since the RFID is suitable for identification, the technology is used to verify identity of the individual in order to allow access to buildings, to provide services or to check payments. The identity of the individual is usually disclosed whenever his/her RFID-enabled device gets in reach of a RFID reader or RFID tag. In order to reveal only the necessary information about individuals, the identity management should be applied, including identification, authentication and authorization. The identity management also concerns finding a balance between privacy and personal data protection on one side, and the need for verification on the other side. This paper deals with principals of the abovementioned balance and its legal regulation.

KEYWORDS

RFID, identity management, privacy, smart cards

1. INTRODUCTION

The technology of identification by means of radio frequency technology is used mostly to identify products in logistics and retail of goods. Since the technology allows unique identification, the radio frequency identification or RFID is employed also in various other ways. More and more common is its application in identification of persons via RFID enabled devices such as smart cards, smart tokens or mobile phones in order to provide a service, to allow access to a building or to check payments for a service or goods.

[*]evafialova@mail.muni.cz

In these situations it is necessary to reveal the identity of an individual to some degree. In order to keep the privacy of the individual as protected as possible, only the minimal amount of information should be disclosed, and this should only be the information relevant to the purpose. Privacy of the individual is to be protected by means of identity management.

2. RADIO FREQUENCY IDENTIFICATION

Even though the awareness about RFID rises, a brief overview of the technology should be given. RFID is a generic name for a system that allows a unique identification of products or persons at a distance using radio frequencies. The choice of the frequency has to be derived from the planned application. The lower frequencies penetrate easily through barriers, but their speed of propagation is slower than for higher frequencies.

RFID consists of three parts: a RFID tag, a reader and a middleware. The RFID tag is equipped with a chip and an antenna. The chip serves for data storage, and the antenna for signal transmission between the tag and the reader. There are three different types of RFID tags: passive tags that just receive the signal emitted by the reader, active tags containing a battery that are able to send data to the reader independently, and semi-passive tags which also contain the battery but only in order to increase the memory capacity of the chip. The RFID reader emits signals towards the passive and semi-passive tags or receives them from the active ones. There exist stationary or mobile RFID readers. The last component is the RFID middleware. The middleware is software that resides on a server between RFID readers and an ICT-infrastructure. Its function is to filter data entering the ICI-infrastructure and let through only the data that are useful for the purpose set by the operator of the system (further: "operator").

3. IDENTIFICATION BY MEANS OF RFID

As the radio frequency identification is the generic name for the technology, there are many possible RFID applications. The technology is used in smart labels, smart tokens, smart cards and implants. Smart labels are used for object identification in logistics and retail. The applications important for the identity management-related problems are primarily smart tokens and smart cards utilized for identification of persons. Since the RFID is suitable for unique identification, the personal identity of the individual can be ascertained or verified by the technology. After the identification, the individual is allowed for exampleto enter a building or to use a service. The identity of the individual is disclosed whenever his/her RFID tag-enabled device comes in reach of a RFID reader.

There are various examples of personal identification through RFID. Common is customers' or clients' identification. The marketers embed RFID tags in their loyalty or discount cards. A well-known example is the *Tesco Club Card* issued by the British retail chain.[1]

The RFID-enabled discount cards are also issued by public transport companies. The Prague public transport company uses so called *open card*[2], Dutch public transport system introduced a national wide *OV-chipkaart*.[3] Other cards equipped with radio frequency technology are members' cards and employees' cards which, besides the identification of members of an institution, organization or a club, enable their holders to enter a room or a building. Public domain does not stay aside either. National governments introduce RFID-embedded ID cards[4] or passports[5] (often labeled as *eGovernment services*).

4. THE IDENTITY MANAGEMENT

"Identity Management is understood as how a person, interacting with an information system, defines what is known and not known about him/her to others using the system and how this relates to the information known or not known to the persons maintaining the system."[6]

The identity management is not represented by one single well-defined process. It is an approach that should be followed in order to disclose only the information necessary for a given purpose. The identity management by

[1] Clews, M. L. 22 April 2009, 'Tesco unveils plan for next generation of loyality card', Marketing Week, available at: <http://www.marketingweek.co.uk/news/tesco-unveils-plan-for-next-generation-of-loyalty-card/2065136.article>.

[2] Ochrana osobních údajů v rámci projektu opencard (Protection of Personal Data in the Project of Opencard), Opencard.cz. Available at: <http://www.opencard.cz/jnp/cz/o_karte/bezpecnost/ochrana_osobnich_udaju.html>.

[3] What is the ov-chipkaart, OV-Chipkaart.nl. Available at: < http://www.ov-chipkaart.nl/aanvragen/watisdeovchipkaart/?taal=en>.

[4] Wessel, R. 6 October 2010, 'Germany Gets Set to Issue RFID ID Cards and Readers to Its Citizen', RFID Journal. Available at: <http://www.rfidjournal.com/article/view/7927>.

[5] The U.S. Electronic Passports, A Service of the Bureau of Consular Affairs, U.S. Department of State. Available at: < http://travel.state.gov/passport/passport_2498.html>.

[6] European Parliament 2007, RFID and Identity Management in Everyday Life. Striking the balance between convenience, choice and control. p. 3. Available at: <http://www.umic.pt/images/stories/publicacoes2/stoa182_en.pdf>.

RFID application is crucial because the huge amount of data related to the individual may be stored on a chip and processed either in accordance with the data protection law or not. The data may be afterwards used for profiling, data mining or data sharing.

Another privacy infringing activity connected with smart cards and smart tokens is tracking of individuals inside buildings (e.g. employees entering into workplace or a particular room) or within a specific area (e.g. a stadium).[7]

The identification process consists of three steps: identification in narrow sense, authentication and authorization.[8] The identification as a first step is represented by logging in the system. In case of the smart card and smart token this step means to get them close to the RFID reader. The particular distance depends on the frequency used. The authentication or, in other words, that the individual is who he/she claims to be, means that the system, after the identity disclosure, recognizes the individual in accordance with the data on the RFID chip and those stored in a database of an operator. In the last step, the authorization, the system makes possible that the individual may act in a particular way defined by the operator.

By the identification an individual discloses his/her partial or full identity. Partial identity means different representation of the individual in different context or in relation to different purposes of identification.[9] For example, for the purpose of public transport another information about the user is important than for provision of health services in a medical center. To the contrary, full identity is disclosed in case that the operator requires all information about the individual because it might be necessary for a task which the operator, i.e. government, fulfills.

The abovementioned identity is related to the issue of control of individual's identity. There exist three main models of identity management, organization-centric model, federated model and user-centric model. The

[7] By means of RFID enabled devices were tracked visitors of the Madejski Stadium in Britain. European Parliament 2007, RFID and Identity Management in Everyday Life. Striking the balance between convenience, choice and control. p. 17. Available at: <http://www.umic.pt/images/stories/publicacoes2/stoa182_en.pdf>.

[8] Van ´t Hof, Ch., Van Est, R., Daemen, F. 2011, Check In/Check Out. The Public Space as an Internet of Things, NAi Publishers, Rotterdam. p. 26.

[9] Olsen, T., Mahler, T. 2007, 'Identity Management and Data Protection Law Risk, responsibility and compliance in 'Circles of Trust'', Computer Law & Security Report, vol. 23, no. 5, pp. 1-34. p 7. Available at: <http://ssrn.com/abstract=1015006>.

organization-centric model is represented by synchronized identity used by different entities keeping an identity register. In contrast, in case of the user-centric model, the person that keeps the identifiers of the system is the individual and he/she is the only one who knows a relation between them.[10]

Between the organization and user centric models stands the so called federated model. This model functions on the basis of a circle of trust formed by several service providers. The identifier is ensured by a third party - the identity provider - that acts on behalf of the service providers.[11]

5. PRIVACY INFRINGING IDENTITY DISCLOSURE

In light of the foregoing, the process of identification comprises the disclosure of personal data or other information relating to the individual. Providing that an improper identity management is applied by the operator, privacy and data protection law can be infringed. Privacy infringing identification occurs by requiring an extensive amount of data for the defined purpose or data not necessary for that purpose whatsoever. The identification for provision of public transport services can serve as an example. For a public transport company is indispensable to know whether a physical holder of a card has paid for the service. Some public transport companies do not issue anonymous discount cards. Every applicant is obliged to fill in at least a name, a date of birth and an address into a document. When submitting the document the applicant may be required to identify himself/herself by means of an official identification card or a passport.[12] The applicant's data are stored on a RFID chip or in a database. After putting the card closer to the RFID reader, a ticket inspector becomes familiar with personal data of the card holder whereas the information necessary for the provision of the service is only whether the person keeping the card has paid for the service or not.

A special issue regarding privacy infringement is multi-purpose smart cards. These cards serve for various purposes simultaneously. The mul-

[10] Rundle, M. 2007, 'e-Infrastructures for Identity Management and Data Sharing: Perspectives across the Public Sector', no. 12, pp. 1-25. p. 11-12.Available at: <http://ssrn.com/abstract=1325235>.

[11] Smedinghoff, T.J. 2009, Federated Identity Management: Balancing Privacy Rights, Liability Risks, and the Duty to Authenticate, Working Paper, pp. 36. p. 12. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471599>.

[12] e.g. How to manage, Opencard.cz. Available at: <http://opencard.praha.eu/jnp/en/how_to/issue.html>.

ti-purpose cards are mostly used as a combination of a discount card and an electronic wallet for payments of parking fees or travel tickets, and a device enabling access to registers.[13] Another possible combination is an entrance card together with an electronic wallet for a canteen or restaurant, and an application allowing tracking the card holder inside a specific area. The inside tracking resembles the obligatory logging in of the card holder in the time of entering particular space in the area.

By means of the multi-purpose smart card may be provided an access to one single database in which data are processed for various purposes as well as an access to more databases simultaneously. That implies that the operator is able to acquire knowledge about the purpose irrelevant information relating to the individual after his/her logging in the system. The similar situation may occur in case that personal data of the individual processed for different purposes are stored in one application on the chip.

6. IDENTITY MANAGEMENT IN RFID APPLICATION

Together with the increasing use of smart card rises the demand on suitable identity management. The identification process has evolved from the quick presentation of a paper or plastic card to a practice of logging in by a chip card into a system, where every log is stored in a database that contains personal data of the user. The operator should primarily obey principles of data processing set down by the OECD Privacy Guidelines and the Data Protection Directive 95/46/ES:

1. Collection for specific, explicitly defined and legitimate purpose: the declared purpose should not comprise only the identification of the individual, but also the purpose for which the identification takes place.

2. Fairness and lawfulness of processing.

3. Compatible use: the identifier or other personal data should not be processed for a purpose incompatible with the identification purposes.

4. Preservation: the identifiers and personal data about the individual should be preserved for a period of time needed for the accomplishment the purpose.

5. Data quality: the personal data should be accurate and kept up to date.

6. Security: the processed personal data should be kept secure. This requirement relates to a database as well as an adequate encryption of the

[13] What can be used for, Opencard.cz. Available at: <http://opencard.praha.eu/jnp/en/uses/index.html>.

chip in a smart card in order not to be read by other than an appropriate RFID reader.

7. Providing individuals with information: the individuals should be informed i.e. about the personal data processed for the identification purposes, about what data are uploaded on the chip in the smart card and who is authorized by the operator to have access into the database.

Besides the legal regulation governing the protection of personal data, the operator should be aware of specifics of the identification process and adhere to particular maxims of the identity management. The well-known laws of identity were set down by Cameron. He recognizes seven basic rules:[14]

1. User control and consent: the individual should know what information about him/her is stored in the system and grant consent to its employment for identity management.

2. Minimal disclosure for a constrained use: the operator should use the minimal amount of information for the identification purposes.

3. Justifiable parties: the operator should determine only limited number of persons authorized to come into a contact with identifying information.

4. Directed identity: in case of a universal system of identification, this system should support a universal identifier for public sector and specific identifiers for private sector.

5. Pluralism of operators and technologies: also in case of a universal system of identification, the identification system should support more operators and technologies in diverse contexts.

6. Human integration: the system should communicate with human user; otherwise it can become unpredictable and ambiguous. Only the human user can ensure the smooth interaction with the system.

7. Consistent experience across contexts: the user should have a consistent experience in all contexts and applications.

7. SOLUTION OF IDENTITY MANAGEMENT

The identity management by identification by means of RFID technology has to be assessed thoroughly and carefully. The operator of the system should search a solution pursuant to the abovementioned principles of data protection and identity management.

[14] Cameron, K. 2005, Laws of Identity, pp 1-12. p. 6-11. Available at: <http://www.identityblog.com/?p=354>.

First of all the individuals should not be forced to use the smart cards for identification, on the contrary, the use of smart card should be voluntary. The identification can be carried out by e.g. a gatekeeper who recognizes a face of the individual without knowing or remembering his/her name.

The most convenient model with respect to privacy is the user-centric model in which the individual keeps the identifiers to the systems and is free to dispose with them in accordance with his/her needs. By the other models – organization-centric and federated model – the individual may not know with certainty what entity has acquired the identifier and his/her personal data. Nevertheless, by RFID applications the user-centric model assumes more RFID enabled smart cards or other devices, which may become inconvenient in practice, because this model implies numerous single-purpose smart cards with purpose specific identifier for each and every service.

Providing the introduction of a multi-purpose card, or a smart card granting access to more than one system, such card should be either enabled with more RFID chips, or with one chip containing separate applications.[15] A smart card in which even four RFID chips are embedded, was developed by Massachusetts Institute of Technology.[16] The technical separation of identification process prevents to disclose personal data not necessary for the declared purpose.

The abovementioned separation corresponds with the requirement of data minimization, that is, to require only the personal data which are indispensable for identification process. This applies both for data uploaded on the RFID chip in the card self and the data stored in a database that are connected with the individual by the time of identification. For example, for a discount on basis of age the operator should require merely a date of birth and not a personal identification number from which not only the age of the individual can be read but also other information depending on a number used in various countries.

It is not surprising that private sector operators should make use of partial identity of the individual by the identification process requiring merely the information related to a particular application, e.g. identification of em-

[15] What it can be used for, Opencard.cz. Available at: <http://opencard.praha.eu/jnp/en/uses/index.html>.

[16] Cheung, H. 15 February 2006, 'Multi-chip RFID packages to substitute multiple RFID cards' TG Daily. Available at: <http://www.tgdaily.com/trendwatch/24494-multi-chip-rfid-packages-to-substitute-multiple-rfid-cards>.

ployees, customers, club members, etc. Also public sector operators should prefer the partial identity and insist on the disclosure of the individual's full identity exceptionally, where the partial identity would not accomplish a task.

In January 2011 the Article 29 Working Party introduced the Privacy and Data Protection Impact Assessment Framework for RFID Applications (further: "PIA"). The main goals of PIA is compliance with privacy and data protection laws and as well as an effective risk management of the RFID Application.

In the initial phase operators assess whether to apply full or small scale PIA. Criteria for the full, resp. small scale PIA are specified in the risk assessment phase. The main targets of the PIA relating to privacy are particularly to safeguard quality of personal data, to legitimate the data processing, to provide information and access to the data and to safeguard confidentiality and security of processing.[17]

Providing that the RFID technology functions as a tool of unique identification, it is frequently used in the identification cards. For this reason the above described PIA should be supplemented with an Identity Impact Assessment. In the Identity Impact Assessment the principles of identity protection should be taken in the account.

The operators should assess first of all the necessity of identification of individuals in the intended application. In case that the identification is considered to be requisite, the operator should assess whether to require partial or full identity of the identification. This may be a well emphasized step especially for the public sector operators since they might tend to make use of full identity for purposes that do not require whole identity disclosure. For private sector the separation of identity for different RFID applications should be taken as a rule. The operator should also assess extend of authorization, or in other words, whether the number of required personal data and other information about the individual is proportional to the access for which the application this individual authorizes.

One of the criteria of the Identity Impact Assessment should also be a choice of an identifier or identifiers. The identifier should adhere to the principle of data minimization, in order not to reveal more information

[17] Article 29 Working Party 12 February 2011, Privacy and Data Protection Impact Assessment Framework for RFID Application, p. 13. Available at: < http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf>.

about its user than necessary for the application. The most acceptable solution is to generate a random number and uploaded it to the RFID chip in the smart card. The criterion related to the identifier is a choice of one of the three possible aforementioned models.

The individual should be provided with information concerning which persons are entitled to have access to the database in which the identifier is linked to other information about him/her, about the chosen identity and model. He/she should be also aware of the fact which data are uploaded on the RFID chip and which data are stored in the database.

8. CONCLUSION

A key attribute of the RFID technology is the unique identification of persons and/or objects at the distance. That is the reason why RFID chips are incorporated into identification smart cards and other smart devices. Since another attribute of RFID is the ability to store and subsequently transmit huge amount of data, in course of the identification process the personal data and information relating to an individual may be disclosed.

Privacy and data protection should be ensured by efficient identity management. The fundamental elements of such management is namely a voluntary use of smart cards where possible, data minimization, a purpose specific identifier instead of a general one and disclosure of a partial identity of the individual. The purpose specific identifier should be embedded in a single-purpose smart card. In case of issuing multi-purpose smart cards, these cards should contain more RFID chips or more separate applications should be uploaded on one RFID chip.

The Article 29 Working Party should adopt the Identity Impact Assessment to urge operators of identification systems to assess risks of RFID for privacy and personal data within the process of personal identification.