Medical Informatics in a United and Healthy Europe
K.-P. Adlassnig et al. (Eds.)
IOS Press, 2009

doi:10.3233/978-1-60750-044-5-43

The Second Generation Slovenian Health Insurance Card

Anka BOLKA [1]
Health Insurance Card Department,
Health Insurance Institute of Slovenia, Ljubljana, Slovenia

Abstract. Ten years have passed since the design of the Slovenian health insurance card system, which has been used daily in the entire Slovenian health sector for the last eight years. Eventually, however, a growing number of business and technical reasons arose for the gradual renovation of the system. Therefore, in 2006, on the basis of a study of feasible solutions, the Health Insurance Institute of Slovenia prepared a concept for renovation and began modernising several system components, including the new cards as the key security elements of the system. In September 2008, the first new professional cards were issued; in November 2008, the release of the new health insurance cards began.

Keywords. health insurance card, professional card, on-line system, digital signature

1. Introduction

The Slovenian health insurance card system was designed in 1996, and ultimately introduced at the national level in the summer of 2000. The card was well received by all users of the system: insured persons, health service providers and all four insurance companies; its use has become a matter of routine and is therefore securely incorporated into the Slovenian health system.

However, despite constant updates and functional expansion, especially of information technology, the card system has to be checked and updated after a longer period of use, like any other technology, in order to meet modern technological and other (e.g., legal) demands and to facilitate further development.

In 2006, the Health Insurance Institute of Slovenia (hereinafter: the Institute) therefore prepared a concept of card system updating, and in accordance with that concept, is gradually renovating the card system.

2. Reasons for the Renovation and the Renovation Concept

Since the introduction of the Health Insurance Card (HIC), an increasing number of business and technical reasons for the gradual renovation of the card system have arisen, despite constant updating and the development of new functions. The technical reasons include, notably:

[1] Corresponding Author: Head of Health Insurance Card System Development, Health Insurance Institute of Slovenia, Miklosiceva 24, SI-1507 Ljubljana, Slovenia; E-mail: anka.bolka@zzzs.si.

- The current chip card was no longer in production, so this central technical component of the system needed to be replaced with a suitable device/card enabling the incorporation of modern technology into the system, which will satisfy present needs and be open to further development;
- The card system must meet modern demands and regulations pertaining to the protection of personal data and electronic commerce;

European strategic orientations in the field of e-health [1] recommend the expedited construction of a safe health care information network, the expansion of card use in health care and the gradual establishment of on-line data access. The same trend is also seen in the guidelines for the future electronic European Health Insurance Card and the development plans of individual Member States. The HIC system renovation is directly related to the adopted strategy of Slovenian health system informatisation, the so-called "eZdravje2010" [2].

These strategic aims thus dictate the increasing informatisation of health and the standardised exchange of medical data. The renovated card system will be an infrastructure providing for the realisation of stated strategic aims on the basis of modern safety schemes, based on smart cards and an infrastructure of public keys.

The basis for the preparation of the card system renovation concept was an expert study [3] which defines four possible renovation scenarios, the basic building blocks of an individual scenario, the feasible technical solutions of individual system components, and a financial assessment.

On the basis of a detailed analysis of several aspects of individual scenarios, one including a gradual transition to the renovated system was chosen, because it assures continuity of the system, with no particular shock for users or risks of the manageability of the system's operation being interrupted, while retaining the rational usage of existing equipment in the future with replacements, which will have to be used only when they are really necessary.

3. The New HIC

At first, the new HIC will have the same role in the system as the present HIC: it is used to identify and check the identity of the insured person and serves as the medium for the current card data set. The new HIC is entirely compatible with the existing HIC and HPC and all other components of the existing system.

When all the necessary data gradually become available on-line, the new HIC will, in combination with the new HPC, ensure safe communication in the network and gradually become only a key to data, no longer serving as an information medium. The new HIC will allow the card holder to access personal data stored on servers, and allow health care workers to access insurance and personal medical data (in accordance with their authorisations as agreed upon between system users).

The data are written on the chip of the new HIC in two sets:

- The first set (in the 'compatibility applet' on the chip) includes data also written on the old card. These data are used by those providers that still operate in the present off-line mode;
- The other set (in the IASE applet on the chip) contains digital certificates. When an HIC is issued, it contains two digital certificates: one for entry to the

on-line system (it enables the identification and authentication of the HIC holder), and the other for a secure HIC holder access to their personal data;

- The HIC also contains space for downloading additional digital certificates, which will probably be used by each user individually.

The set of data on the card also contains all data required by the currently valid standards of the European Health Insurance Card.

The whole development of the new HIC was completed by November 2008, when the Institute started to issue new HICs instead of the present (old) ones. The new card version is being 'naturally' introduced into the existing system in steps: the new card is issued only for the needs of newly insured persons (mostly newborns) and the regular replacement of the currently used card (loss, change of data presented in visible form, etc.). Thus, one of the most important aims of renovation was achieved: the transition was made without burdening or making demands on the system users.

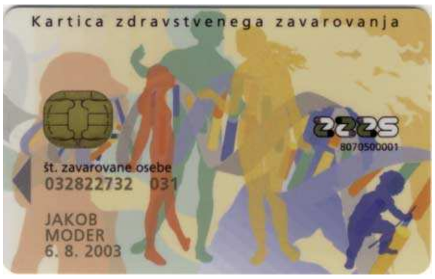

Figure 1. Front side of the new HIC

4. The New Health Professional Card

The new health professional card is the key security element of the renovated card system. The HPC is used to identify and check the identity of a health care worker, to ensure secure communications and for electronic signature.

The data are written on the chip of the new HPC in two sets:

- The first set (in the 'compatibility applet' on the chip) contains data which are also written on the old card, meaning that the new PC in the card system retains all the functions of the present HPC;
- The other set (in the 'IASE applet' on the chip) contains digital certificates. Each HPC has a (regular) digital signature, enabling the card owner to safely access data stored in the on-line system. In addition, professional cards for doctors, dentists and pharmacists also contain a qualified digital certificate, providing the user with a safe electronic signature, e.g., when prescribing a medicine or issuing a medical preparation. Digital certificates and professional cards are valid for five years from the day of personalisation. After an HPC has been issued, new or additional data or additional digital certificates cannot be uploaded.

As the issuer and system operator, the Institute has established processes for issuing HPCs and digital certificates, and for system control. For this purpose, it has developed its own application software support, one of the most important tasks being the establishment and management of the HPC holder register. The register contains integral data on HPC holders and their digital certificates (data on issuing, cancellation, etc.). The register of HPC holders is directly connected to the authorisations scheme for access to individual data sets in the on-line system. The system of certificates has a dynamic structure, allowing for simple and fast allocation, and the cancellation or changing of individual groups of system users and their authorisations.

The procedure of issuing and managing a new HPC and the certificates it contains is substantially more complex than current procedures because of the key role of HPCs in the safety scheme. The most important change regarding users is the personal registration of doctors and pharmacists for HPC acquisition.

The use of a regular digital certificate on an HPC is protected by a 4-character personal password which must be entered by the HPC holder upon registration.

The use of an electronic signature (e.g., electronic prescription) on the basis of a qualified digital certificate is protected by a 6-character password, defined by the user.

The Institute issued its first production HPCs for the hospital cooperating in the pilot introduction of the on-line system in October 2008. Minor problems were solved as they arose and the national substitution of HPC is currently continuing.

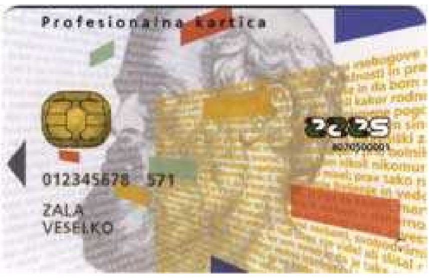

Figure 2. Front side of the new HPC

5. Technical Specifications of New Cards

The technical characteristics of the new card (HIC as well as HPC) [4] are:

- the chip has 72 Kbytes of memory (EEPROM);
- the operating system is Java (standard JavaCard 2.1.1);
- the personalisation of the chip is carried out in accordance with the standard GlobalPlatform 2.1.1.;
- the operating system with an additional crypto-processor supports cryptographic algorithms DES, DES-3 and RSA (key length 1024, 1536 and 2048b), and has compression algorithms SHA1 and SHA256;
- the card body conforms to standards ISO 7810, ISO 7816-1, ISO 7816-2;
- the card body and the chip comply with the requirements of EU Directive 2002/95, which allows only ‘environment-friendly’ new electrical and electronic equipment to be introduced to the EU market;
- the design with graphic elements and visible data on the card comply with EN 1387 (cards for health care applications);
- the card meets very high security standards (PPSSCD Type 3, EAL 4+);
- the service life of the card is 10 years.

The card supplier is the French company Gemalto, responsible for the:

- preparation of plastics,
- installation of chips (the chip manufacturer is Samsung),
- basic electrical chip initialisation and locking of the card with transport keys.

The cards are then taken over by the Slovenian company Cetis, which is responsible for:

- opening and personalising cards: (writing the holder's personal data on the chip and on the surface of the card, creating and writing digital certificates on the chip),
- sending the card with a cover note to the home address of the holder via mail.

The graphic image of the card has been changed, making it fresher and more modern. The basic data of the card holder are written on the surface of the card (first name, surname, HIIS holder number and the number of card issue). The basic instructions for the card holder and data on the manufacturer that can be used by the holder for acquisition of additional data and instructions are written on the rear side of the card.

The Institute acquired an independent opinion on the projected system from the viewpoint of security requirements, standards and recommendation fulfilment [5].

6. Conclusion

With introduction of the new version of HIC and HPC, the Institute has ensured the key security and infrastructural elements for safe electronic commerce in the Slovenian health care system. This groundwork must be used to plan and establish basic applicative solutions in health care and health insurance which will update the information flow and make the whole system more accessible, simpler and friendlier to all users – patients and insured persons, as well as medical staff.

References

[1] Action plan for a European e-Health Area, http://ec.europa.eu/information_society/activities/health/policy_action_plan/index_en.htm, 30th April 2004.

[2] Strateški načrt »e-zdravje2010« [http://www.mz.gov.si/index.php?id=9204], December 2005.

[3] Schwier, A. (2006) *ZZZS Card System Renovation Project, Expert Study*, Health Insurance Institute of Slovenia, Ljubljana.

[4] Malneršič, B. (2007) *ZZZS – HIC – HPC Technical Specification*, Health Insurance Institute of Slovenia, Ljubljana (this document is an internal literature of HIIS).

[5] Novak, R. et al. (2007) *Neodvisna varnostna presoja specifikacij sistema on-line zdravstvenega zavarovanja in prenove sistema KZZ*, Health Insurance Institute of Slovenia, Ljubljana (this document is an internal and highly confidential literature of HIIS), 2007.