ELSEVIER

International Journal of Medical Informatics 61 (2001) 33–43

International Journal of Medical Informatics

www.elsevier.com/locate/ijmedinf

Slovene smart card and IP based health-care information system infrastructure

Denis Trček [a,*], Roman Novak [a], Gorazd Kandus [a], Marjan Sušelj [b]

[a] *Department of Digital Communications and Networks, Institut 'Jožef Stefan', E6, Jamova 39, 1101 Ljubljana, Slovenia*
[b] *Zavod za zdravstveno zavarovanje Slovenije, Miklošičeva 24, 1507 Ljubljana, Slovenia*

Received 16 November 2000; accepted 7 December 2000

Abstract

Slovenia initiated a nation-wide project to introduce smart cards in the health sector in 1995 and its full-scale deployment started in September 2000. Although the basic aim of the project was to support insurance related procedures, the system was designed in a flexible and open manner to present an infrastructure for the whole health sector. The functionality of the current system is described in this paper along with lessons learned so far. The upgrade of the system is outlined, with emphasis on technical details, the objective being to provide a real-time EDI based environment for a general set of applications in the medical sector, supported by the flexibility and security of modern smart card technologies. Integration with similar systems in other EU countries is discussed. © 2001 Elsevier Science Ireland Ltd. All rights reserved.

Keywords: Smart cards; EDI; Web technology; Health-care information system infrastructure

1. Introduction

Slovenia has undergone a transition to a free market economy over the past few years. In comparison with other central and eastern European countries it has succeeded in retaining a high level of health-care services, which compares well with those in western European countries. This is partially due to the political determination that social security standards have to be high and partially to the fact that Slovenia has the largest BGP among the central and eastern European countries. However, for a national economy to be competitive in a global market, costs for the health sector had to be cut, but not at the price of quality of services. These have to be improved where possible.

With this background, the Health Insurance Institute of Slovenia (HIIS) started a project of nation-wide introduction of smart cards in 1995, called the Health Insurance Card (HIC) project. The developed infrastructure is fully operational on a national

* Corresponding author. Tel.: +386-61-1773379; fax: +386-61-1262.

E-mail addresses: denis.trcek@ijs.si (D. Trček), marjan.suselj@zzzs.si (M. Sušelj).

PII: S1386-5056(00)00132-5

scale and the first phase finished in September 2000. In addition, two new applications are already being under development.

Although Slovenia is the first country in the world with nation-wide use of smart cards in the health sector, similar projects are under way in other countries. Deployment of such cards and internet technology is common to the majority of these approaches that are typically very complex, as they have to deal with technological, organisational and legal matters on an international scale. The HIC project utilises results from international efforts in this field. Especially the Netlink Consortium has to be mentioned here [1] (the consortium includes France, Germany, Italy and the Canadian province of Quebec). The HIC project is a part of Netlink's CEE subproject, which, besides Slovenia, includes also the Czech republic. One of the main benefits of the Netlink project is a specification of a minimal set of requirements to enable interoperability of various national solutions.

The paper presents the status of the HIC project, current solutions, future directions and main benefits as well as obstacles, with an emphasis on the technology. It is structured as follows. The background of the HIC project is given in Section 2. It is followed by the general architecture in Section 3. In Section 4 security issues are discussed. In Section 5the evaluation of the project is discussed, while the conclusion is presented in Section 6.

2. Background of the HIC project

HIIS is a public institute and a statutory provider of compulsory health insurance to all residents of Slovenia. In line with this, HIIS started to equip medical service providers with PCs in the early 90s to automate and speed up administrative tasks related to evidence and payment for these services. Currently, 90% of the reports and invoices is send through EDI. Thanks to this initial step, Slovenia is now a well-developed country in terms of medical and health informatics and institutions are reasonably well equipped with personal computers.

However, nationally co-ordinated efforts and guidance of health-care IT developments were lacking, so organisations have taken different approaches. As a consequence, current health-care information systems are quite heterogeneous and the level of countrywide integration is weak. We are faced with the use of different standards, mutual incompatibility of electronic patient records, outdated technologies that form barriers to further integration or extension without a substantial re-engineering, etc. In addition, medical data, information and documents are stored on a variety of media, ranging from the classic paper based records (which still account for 70% of all data), to computer based records.

In 1995 a decision was taken to improve the situation by migration to internet technology and the introduction of smart cards. This was the beginning of the HIC project. General objectives were further reduction of administrative tasks, improvement of quality of services for insured persons (reduction of procedures, drug prescription management, medical passport etc.) and improvement of personal data security. More precisely, the initial detailed card introduction plan covered: the design of the whole HIC system (see Fig. 1), the design of the Health Professional Card (HPC) and the design of the network and self-service terminals. Draft amendments of HIIS acts and draft rules, cost benefit analysis, the plan of activities for the implementation, informing of the general/specific public and national/international project evaluation studies were covered as well.

During the first phase old paper booklets that have served for identification and compulsory insurance status were replaced and

health insurance related data were stored on smart cards. These data currently include patient identification, compulsory and voluntary health insurance status and selected personal physician. A network of self-service terminals was set up that enable HIC holders to update their insurance status. These terminals also serve as information kiosks (doctors on duty, pharmacies in the neighbourhood, etc.). They are connected through internet protocol (IP) links to the central server at HIIS premises, where the database is run. Links are protected with proprietary public key and symmetric key cryptography, based on standardised protocols. The whole network is shown in Fig. 2.

At the doctors' premises a patients' HIC is put in a reader with a HPC on the other side. After mutual authentication, relevant data become accessible. PCs use standalone (off-line) proprietary applications. Smart cards currently use symmetric key cryptography and structured access rights (seven levels actually implemented, out of fourteen foreseen), which is based on Gemplus technology. Both types of cards are ISO 7816 — 1 thru 8 conformant [2] and HIC has 16 kB of EEPROM, while HPC has 8 kB of EEPROM. The current infrastructure includes: 1 946 000 HICs, 20 000 HPCs, 5400 card readers, 270 self-service terminals at 218 locations and 1036 health-care service providers. The implementation of the first phase was finished in September 2000. In a few months the system will be upgraded with an organ and tissue donorship application. The second phase will include pharmacies and electronic prescription and will be finished within the next 2–5 years. Other applications (electronic order for technical aids, documentation of issued drugs, medical record pointers and the G7 emergency data set) are to be realised not later than 5 years from now.

The HIC project has thus introduced an operational information infrastructure that is planned to serve as a backbone for a future health-sector nation-wide information system. However, this is far from being a trivial task. Issues to be addressed include general architecture, transition to standardised solutions for authenticated access, secured transactions and smart card solutions (dynamic downloading of applications). Last but not

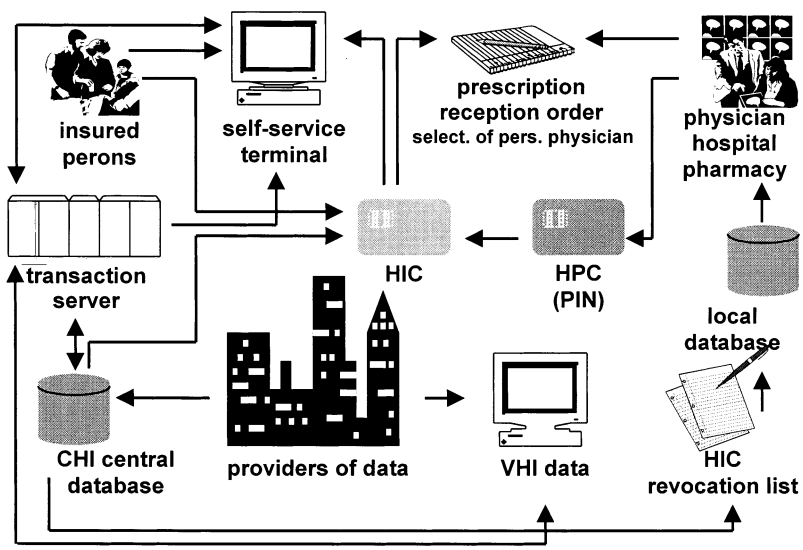

Fig. 1. HIC system: entities involved and related procedures.

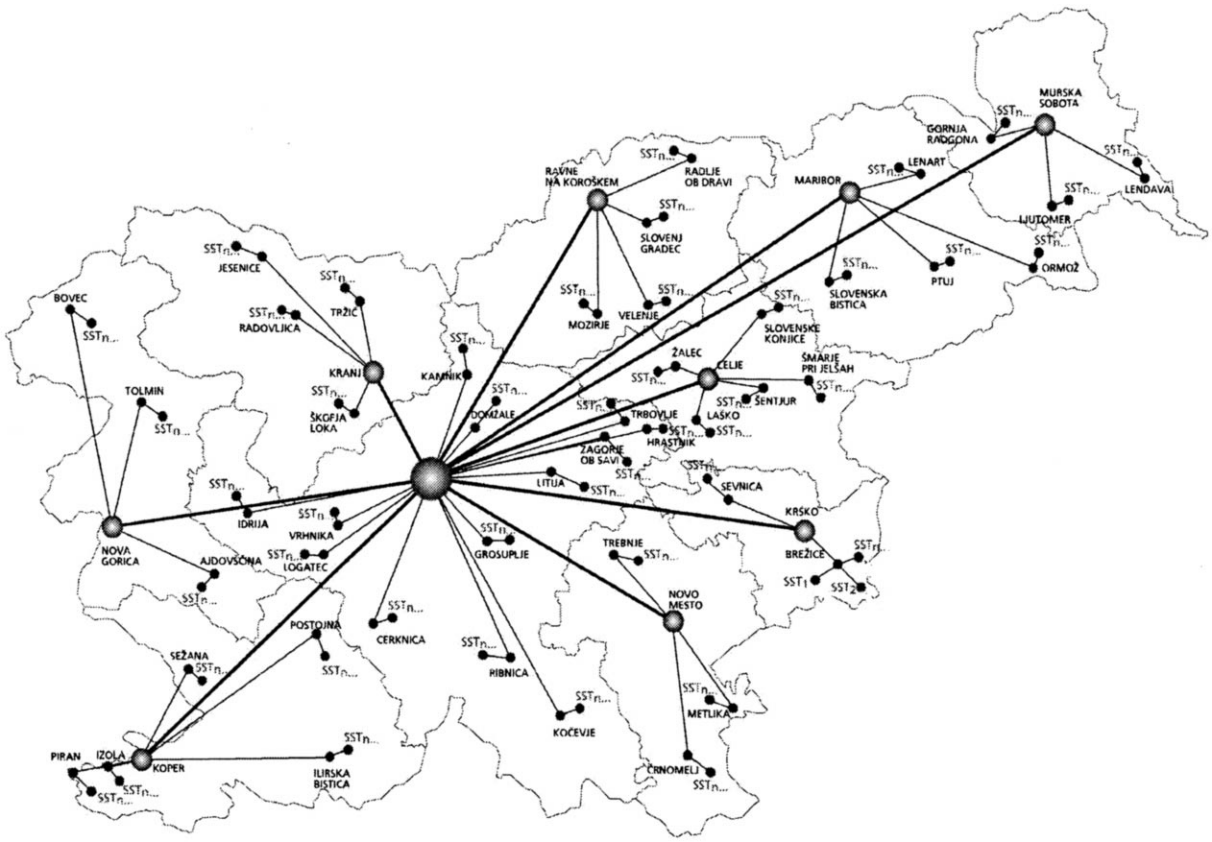

Fig. 2. The regional health-care centres and the network of HIC project.

least, the role of the insurance card is to be clearly identified and this will be discussed in the following sections.

3. General architecture

An internationally approved and recommended architecture for smart card based information systems is described in [1]. The HIC project has adopted such architecture, although current transactions are based on exchanges of small chunks of data instead of complete documents. Such a system could be described as a Data Base Management System (DBMS) transactions oriented rather than EDI oriented one. Although a general architecture proposed by Netlink is not limited to DBMS transactions, since it explicitly mentions the use of e.g. S/MIME and some electronic document forms, the HIC project remains rather confined to DBMS oriented use. The reasons are the following:

- Only a few particular EDI specifications exist that are of use in a medical sector, like physician letter (HL7 [3]), hospital to hospital documentation (EDIfact [4]), etc. Many of them are intended for other business sectors and costly converters are needed, which poses problems for true interoperability. Even some basic data sets like electronic patient records are yet to be fully standardized. But in an open environment, where various entities from dif-

ferent administrative domains exchange data (e.g. hospitals, pharmacies, and insurance companies), support of EDI is mandatory.

- There is a lack of complete procedures for accomplishing particular business tasks in the health sector — one rare exception is given in [5]. It is not only the exchange of the document itself that matters, but also the sequence and semantic/syntactic relationship between these documents along with complete organizational procedures. Security in particular can be affected in this way [6].

For the successful introduction of EDI, data sets have to be defined and they have to be stable. Appropriate documents should be defined along with transactions, i.e. the sequence of steps and corresponding documents that are exchanged. Thus complete EDI support requires a set of protocols for conducting highly structured exchanges of data between different organizations. There is currently a notable lack of such specifications in the health-care sector. This constitutes one of the basic problems for architecture definition and deployment of a nation-wide health-care information system in Slovenia.

It should be noted that basic documents in the field of smart cards and their interoperability are already 3–4 years old (see e.g. [7]). In the meantime, web technology has become an obvious choice for conducting e-business. Web technology is the most widespread and efficient technology that supports on-line transactions and it should be considered seriously. Implications for the EDI world are as follows. The above-mentioned documents need to be revised to take into account widely accepted technological changes. Data structure description using ASN.1 [8] might turn out to be outdated due to the emergence of Extended Markup Language (XML [9,10]). XML enables content description in a way that is natural to the web environment — one such initiative is described in [11]. The same holds true for coding messages. Using DER [8] is redundant in the web environment, which has its own efficient way of coding forms for their exchange, e.g. URL encoding in CGI communication [12], etc. In general, ASN.1/DER has found its place in internet mainly for digital signature related procedures (certificates, certificate revocation lists) and in network management (Simple Network Management Protocol [13]).

4. Security issues — current solutions and future upgrades

Following a 'Commercial Off The Shelve' philosophy in the future (i.e. web technology) would reduce costs and enhance reliability. It would also mean a shift to a real on-line oriented system, which is not the case with the use of e-mail (see Fig. 3).

One of main issues in the HIC project is related to the use of symmetric cryptography based smart cards that affects a large part of the whole system architecture. In the most likely transition that was discussed in the previous subsection, web servers will be used as front-ends to database management systems, while on the other side, web browsers will serve as front-ends towards smart cards. Secure channels between web browsers and servers can be established by default through SSL layer [14], which is very convenient.

It should be emphasised that patients' cards are not intended for digital signature operations. This fact significantly simplifies future upgrades of the whole system, as only professional cards, — being about 1% of all cards — will have to be upgraded. However, end-to-end secure channels are a final goal to assure security from smart cards to peer entities over the network. We are investigating possibilities of such imple-

mentation with Java cards. These are Schlumberger Cyberflex Open 16K [15] (the reason for choosing an older model is export restrictions). Our current experience is that symmetric cryptography support should not be a problem. Also asymmetric operations should be possible, although very time consuming. Java cards already exist on the market with cryptographic services available at the API level, e.g. Cyberflex Access [15], which feature RSA, 3DES and SHA-1.

Nevertheless, the basic limitation, even of the latest cards, remains processing of cryptographic protocols and, more generally, handling of communication protocols. Thus an 'off-load' scenario is investigated with a CORBA compliant environment [16], where a smart card contacts various agents for accomplishment of particular tasks. Communication with agents is to be done with HPC, as only HPC will be capable of handling asymmetric algorithms. According to access right, after the transaction is over, HPC updates appropriate data in a HIC, if necessary.

The protocol chain is structured in two segments (see Fig. 4). In the reader segment it is not possible to handle communication with classes in 'java.io' and 'java.net' packages [17]. All that remains is CyberflexAPDU class in package 'javacardx.framework' with methods 'receiveData' and 'sendData'. Thus this segment is the most critical one. The second is the network segment, where 'java.net' and 'java.io' classes are available, so it is possible to use sockets and to deploy WWW servers and clients with full security services, e.g. SSL. Let PCA stand for a PC applet, TSS for a time-stamp server, ORB for an object request broker, CERT for a certificate and TS for a time-stamp. Let K_S denote a session key, K_{E_X} a private key of entity X, K_{D_X} a public key of the same entity and let $\{M\}_K$ denote a message M encrypted with a key K. The protocol in a reader segment goes as follows (all packets are encrypted with recipients' public keys to prevent attacks on integrity and to ensure authentication):

1. HPC → PCA: $\{\text{comm\_request, find\_TSS}\}_{KE_{HPC}}$, $CERT_{HPC}$
2. PCA → HPC: $\{\{K_S, TS_1\}_{KD_{HPC}}\}_{KE_{PCA}}$, $CERT_{PCA}$
3. PCA → ORB: $\{\text{find\_TSS}\}_{KE_{PCA}}$, $CERT_{PCA}$
4. ORB → PCA: $\{\text{TSS\_address}\}_{KE_{ORB}}$, $CERT_{ORB}$
5. PCA → TSS: $\{\text{get\_TS}_2\}_{KE_{PCA}}$, $CERT_{PCA}$
6. TSS → PCA: $\{TS_2\}_{KE_{TSS}}$
7. PCA → THPC: $\{TS_2\}_{KE_{TSS}}$
8. HPC → PCA: $\{TS_2, TS_1\}_{KS}$.

In the first step HPC initialises a communication. It also sends the name of a TSS, which it trusts and for which it has a certificate. A PC applet responds with a concatenation of a time-stamp and a session key that is first encrypted with an HPC public key, and the output is encrypted with its private key. This ensures confidentiality of a session key and authentication and integrity of the whole packet. Afterwards, PC applet sends a request to an ORB to provide it with information, necessary to access the desired time-stamp server. This is required for an HPC to be assured about the freshness of the packet that includes a session key (the second step). After receiving this address, PC applet sends a request to a time stamp server and forwards the response to HPC. In the step that follows, a HPC decrypts a message and

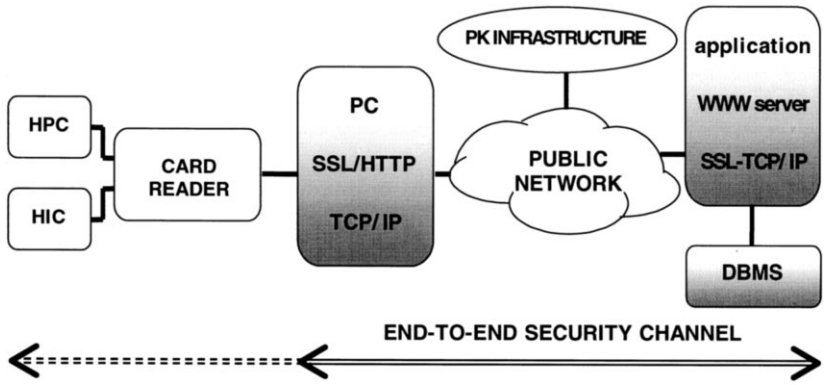

Fig. 3. A web-centric smart card based information system.

can be assured of the freshness of the packet from the second step. To conclude two-way authentication, HPC concatenates time-stamps, encrypts them with a session key and sends them to the PC applet. This way HPC and the PC applet know that they share the same session key, which is fresh.

4.1. Public key infrastructure

Much of the complexity of the above protocol is due to time stamping. The general architecture could be less complex, if random values were used. However, absolute timing reference is required because of administrative tracking of events and to deploy prevention measures more easily, when reconstructing successful attacks. Note that this protocol has some weaknesses, as certificate revocation lists are not checked. But currently this seems to be unfeasible for realisation with Java technology and this applies to digitally signed applets in general. Moreover, secure time-stamp servers are very rare.

Support of public-key operations certainly requires appropriate infrastructure [18]. For the HIC project it is likely that certification authority (CA) services [19,20] will be outsourced. But before their deployment appropriate legislation has to be accepted. Slovene's digital signature law has been passed recently in the Parliament. Public key infrastructure support is not only limited to

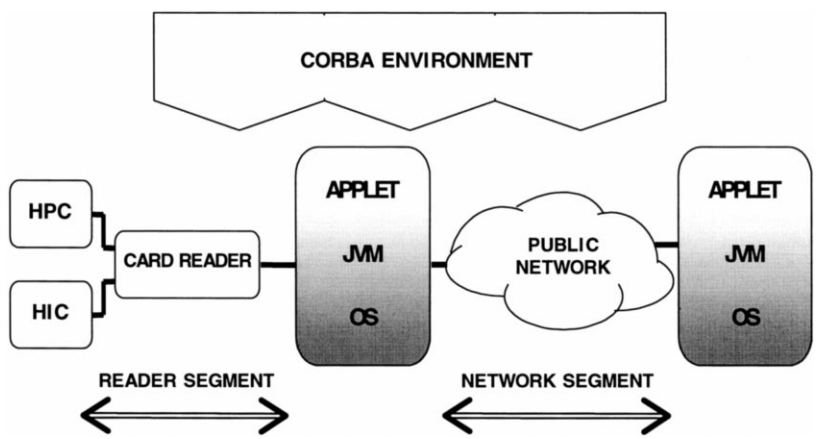

Fig. 4. End-to-end protocol scenario and infrastructure.

the application level, but also to the network level, where IPv6 [21] is in the centre of observations for future upgrades in HIC network. However, network providers are not able to offer this service and a nation-wide public key infrastructure does not yet exist.

4.2. Smart card security

The overall security of smart card based information systems relies heavily on the assumption that cards can provide a high level of protection against seizure of key material. In the HIC system, data protection requirements are set very high. Adopting a proper data security scheme requires knowledge of the card's weaknesses. It is unrealistic to assume that the information stored in a smart card can be kept from a capable, motivated opponent backed up with significant funding [22]. Furthermore, low cost non-invasive attacks are possible. The latest non-invasive attack techniques seriously threaten data security on any smart card. Differential Power Analysis (DPA) is one among them [23]. The technique is based on measuring a circuit's power consumption. In addition to large-scale power variations due to instruction sequences, there are effects correlated to data values being manipulated. When an encryption algorithm is known publicly, a relatively small number of power consumption traces is needed to test different hypotheses about key material. A similar approach may be used on electromagnetic radiation traces.

4.3. User authentication

Owning a valid insurance card authenticates a user, while authenticity of a card is verified through cryptographic algorithms. It is a fact that more medically relevant data is stored in the card, the less is the likelihood of its misuse. This data is a basis for treatment and getting blood of the wrong type, for example, could be lethal. Nevertheless, to support better authentication, PIN enabled cards are considered (this is meant for HIC, while HPC are already PIN protected). However, a PIN is easily forgotten and it also presents a problem for organ donoring, if this information is PIN protected on a smart card. More promising methods for user authentication are based on human biometry. Several approaches are being developed, e.g. fingerprint sensor, face recognition, hand geometry and retinal scans. The technology is improving very fast and error rates are becoming acceptable. Currently, the false rejection rate is typically below 0.1%, while the false acceptance rate is below 0.001%.

5. Evaluation of the HIC project

In accordance with the new health insurance card system, project complexity and its multidisciplinary nature, the evaluation addressed a range of aspects of the card system. We developed a specific evaluation model to accommodate different aspects, user groups and project phases. The model is illustrated in the figure below Fig. 5.

The above evaluation model was first tested by application on the pilot project, by making specific analyses, assessments and recommendations for each of the aspects. In the following subsections brief categorisations of the applied approaches in evaluation of individual aspects is given (other methodologies that could be used for evaluation can be found in [24,25]).

5.1. Financial aspect

Since the project engages public funds (financing from public health insurance budget), the financial aspect was very important

and accordingly analysed in great detail. With the card system design completed and prior to commitment for the pilot project, we carried out a cost benefit analysis. In this analysis, a German consultant firm was engaged, having hands-on experience in the German insurance card system. For the purposes of analysis, we collected cost/benefit data in all categories of costs and savings:

- Costs: development costs (in-house and external services), investment costs, costs of field infrastructure, costs of works, costs of training of system users (in health-care and in health insurance sector) including the costs of hours of work lost for training, costs of initial decreased productivity, costs of system operation, up-keeping and maintenance.
- Benefits (estimated based on data collected through field enquiries): time savings with health-care professionals employers previously responsible for insurance validity confirmation, time savings with insured persons.

The results of the C/B analysis indicated that the card system payback period is 3.5 years.

5.2. Technology aspect

The implemented technology solutions were reviewed against the solutions specified in the design, and recommendations were given for the system refinement for the national scale stage.

5.3. Communication aspect

The communication activities in all phases (preliminary informing during the system development, system introduction announcement phase, and the informing campaign during the system rollout) were analysed together with the reactions of media.

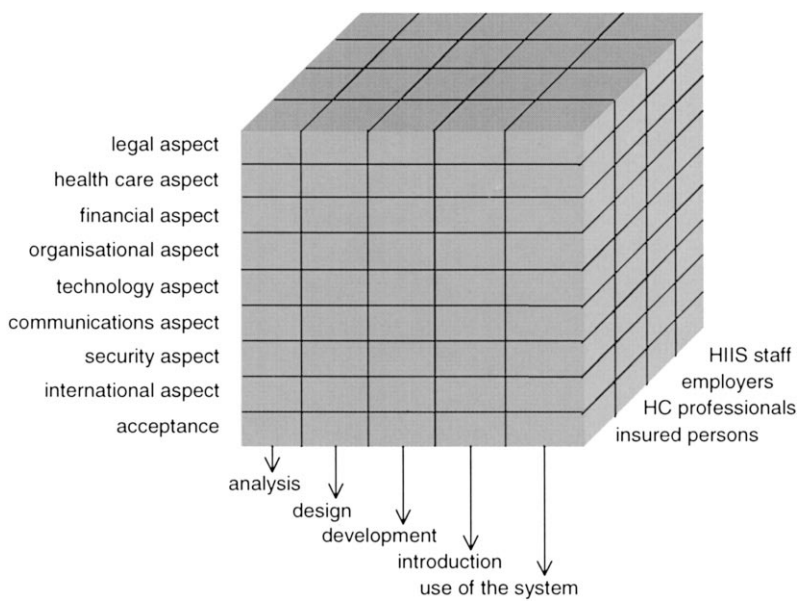

Fig. 5. HIC project evaluation methodology.

5.4. Security aspect

The security scheme was analysed and its adequacy was assessed. The passing criteria were very strict, exceeding the ones, which would be required for the system data limited to insurance data. Rather, criteria were tuned for future enhancement of system functions with selected health-care applications.

5.5. International aspect

The main topics here were the system design conformity with applicable international standards, practices and trends in other countries, and its suitability to future interoperability. Independent foreign experts in the field of health cards did the evaluation. Comments and suggestions were provided for the refinement of the system in the national scale introduction phase.

5.6. Legal aspects, health-care aspect, organisational aspects

Measures and actions completed under the project to that stage were reviewed and recommendations given for the national scale introduction phase.

5.7. Acceptance

A consulting firm carried out a study of acceptance among user groups (insured persons, health-care workers, health insurance staff and employers), in the pilot region and in a comparison region not involved in the pilot project. The analysis method was enquiry on sample groups.

The above analyses and evaluations served to assess the overall card system appropriateness and suitability of the implementation project. This assessment in turn provided the Institute's management with relevant information for launching of the national scale introduction phase.

The integral part of the overall evaluation strategy was a piloting implementation in a Krško region. This region had properties that corresponded to a nation-wide profile. After the piloting implementation proved successful (an international evaluation meeting took place in Čatež, Slovenia, in June 1998 [26]), a green light was given for a nation wide implementation, which was done step by step. Ten regions were covered in seven phases with the last region being covered recently.

6. Conclusion

The health insurance card project in Slovenia is now being deployed at full-scale. Together with networking activities it presents an infrastructure that will support further development of the national health-care information system.

Development of the Slovene health-care information system is an on-going intensive process, and at present, it is undergoing renovation, which provides a good opportunity for introducing of advanced solutions. This means full deployment of public key technology, a further transition from a DBMS transaction based system to a real EDI environment based on widely available web technology, and integration of the OCF [27] into the insurance card system architecture. Thus significant benefits are expected with the deployment of web and Java card technologies.

The goal of the whole HIC project is to reduce costs, reduce administrative work for health professionals and improve services for the patients. This means that the infrastructure will support patients' mobility and future telemedicine services. With this in mind, the role of smart cards can be clearly iden-

tified. They will serve for authentication, for storage of minimal data sets and as pointers to appropriate data sets in a network. And this is the beginning of the realisation of a medical passport for the European environment, and later for the international environment.

References

[1] Netlink Consortium, Netlink Requirements For Interoperability, WP2, H.G. Buettner, J. Sembritzki (eds.), April 1999, http://www.sesam-vitale.fr/html/projets/netlink/index.htm.

[2] ISO/IEC, IT-Identification cards-Integrated circuit cards with contacts, ISO 7816 parts 1 thru 8, Geneva, 1989.

[3] J. Sembritzki, Standards, interoperability and medical application, Health Cards 99, Milano 1999 (slide presentation).

[4] ISO, Electronic data interchange for administration, commerce and transport (EDIFACT), ISO 9735 parts 1 through 8, Geneva, 1998.

[5] B. Struif (editor), German Health Professional Card Specification (Physicians), GMD, July 1999, http://sit.darmstadt.gmd.de/cgi-bin/sit-frame/sica?link = /SICA/workshop.html.

[6] D. Trèek, Minimising the risk of electronic document forgery, in: Computer Standards and Interfaces, Elsevier, North Hollandhttp://denis.ijs.si/, 1998, pp. 161–167.

[7] D. Markwell (editor), Healthcards Interoperability of Healthcard Systems, G7 Interoperability Specification, G7 GII SP6, 1996, http://www.clinical-info.co.uk/euhci.htm.

[8] D. Steedman, ASN.1 — The Tutorial and Reference, Technology Appraisals, London 1990.

[9] T. Bray et al. (eds.), XML-Extensible Markup Language ver. 1.0, W3C Recommendation, February 1998, http://www.w3.org/TR/1998/REC-xml-19980210.

[10] J. Bosak, T. Bray, XML and the Second-Generation Web, Scientific American, No. 5, May 1999, http://www.sciam.com/1999/0599issue/0599bosak.html.

[11] Bayerische Landesarztkammer, HCP-Protokoll Specifikation v 3.0, Munchen, May 2000, http://www.hcp-protocol.de/engindex.htm.

[12] K.A.L. Coar, D.R.T Robinson, The WWW Common Gateway Interface v 1.1, IETF, Internet draft, June 1999, http://web.golux.com/coar/cgi/.

[13] J. Case et al., Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2), IETF RFC 1905, April 1993, http://noc.ucsc.edu/cie/RFC/index.htm.

[14] S. Freier, Secure Sockets Layer (SSL) v 3.01, Internet Draft, Internet Engineering Task Force, January 1996, http://home.netscape.com/eng/ssl3/ssl-toc.html.

[15] http://www.cyberflex.slb.com/.

[16] http://www.omg.org/.

[17] Sun Corp., Java Card 2.1 Platform API Specification, Final Revision 1.0, http://www.javasoft.com/javacard.

[18] S. Turner, A. Arsenault, Internet X.509 Public Key Infrastructure PKIX Roadmap, IETF, Internet Draft, March 2000, http://www.imc.org/draft-ietf-pkix-roadmap.

[19] ISO/IEC, Draft Amendments DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM1 to ISO/IEC to 9594-8 on Certificate Extensions, JTC1/SC 21, Geneva, December 1996.

[20] C. Adams, S. Farrell, Internet X.509 PKI Certificate Management Protocols, IETF RFC 2510, March 1999, http://www.ietf.org/html.charters/pkix-charter.html.

[21] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, IETF RFC 2401, November 1998, http://www.ietf.org/html.charters/ipsec-charter.html.

[22] R. Anderson, M. Kuhn, Tamper Resistance — A Cautionary Note, The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, November 1996, pp. 1–11.

[23] P. Kocher, J. Jaffe, B. Jun, Differential Power Analysis: Leaking Secrets, in: Proceedings of Crypto '99, Springer Verlag, Heidelberg, 1999, pp. 388–397.

[24] J.P. Fortin et al., Evaluation Guide, Strategies and Evaluation Methodolgy WG, Netlink Consortium, December 1999.

[25] E.M.S.J. Van Gennip, J.L. Talmon, Assessment and Evaluation of Information Technologies in Medicine, IOS Press, Amsterdamhttp://www-vatam.unimaas.nl/atim/, 1995.

[26] ZZZS, Ovrednotenje pilotnega projekta uvajanja kartice zdravstvenega zavarovanja v posavski regiji, Čatež, June 1998.

[27] http://www.opencard.org/index-docs.shtml.