Connecting Medical Informatics and Bio-Informatics
R. Engelbrecht et al. (Eds.)
ENMI, 2005

Security Infrastructure Requirements for Electronic Health Cards Communication

Peter Pharow, Bernd Blobel

Fraunhofer Institute for Integrated Circuits IIS, Erlangen, Germany

Abstract

Communication and co-operation processes in the healthcare and welfare domain require a security infrastructure based on services describing status and relation of communicating principals as well as corresponding keys and attributes. Additional services provide trustworthy information on dynamic issues of communication and co-operation such as time and location of processes, workflow relations, integrity of archives and record systems, and system behaviour. To provide this communication and co-operation in a shared care environment, smart cards are widely used. Serving as storage media and portable application systems, patient data cards enable patient-controlled exchange and use of personal health data bound to specific purposes such as prescription and disease management. Additionally, patient status data such as the emergency data set or immunization may be stored in, and communicated by, patient data cards. Another deployment field of smart cards is their token functionality within a security framework, supporting basic security services such as identification, authentication, integrity, confidentiality, or accountability using cryptographic algorithms. In that context, keys, certificates, and card holder's attributes might be stored in the card as well. As an example, the German activity of introducing patient health cards and health professional cards is presented. Specification and enrolment aspects are on-going processes.

Keywords:
Electronic Health Record, Health Network, Health Cards, Security, Infrastructure, Health Professional Card, Patient Data Cards, Policy

1. Introduction

For the purpose of increasing quality and efficiency, health systems in developed countries throughout the world tend to move towards distributed collaborative and co-ordinated care of patients in the sense of shared care. Additionally, the prevention of citizens comes into the focus of the health care administration and management.

Specialisation and de-centralisation processes in healthcare must be accompanied by comprehensive communication and co-operation in order to meet the challenge of the shared care paradigm. Communication and co-operation may be supported through any kind of networks from a departmental Local Area Network (LAN) up to the Internet. An alternative to networking is the connection of patient's information with the patient's being itself: Acting as data subject and data source but also as carrier of any data collected, the patient can realise the informational self-determination guaranteed by privacy acts and constitutions. In any case, communication and co-operation have to be provided securely.

2. Smart Cards in Healthcare

When an information system, e.g. an Electronic Health Record (EHR) shall be held by a human being, an appropriate media is needed to store data structures and applications providing the required functionality as well as to communicate data items between partners inside or outside the healthcare domain. This generally applies ranging from the use of a simple hardware token for specific functions such as identity-related services up to more or less comprehensive portable information systems carried by the information subject [1].

2.1 Card Technologies and Applications in Healthcare

Over the last 30 years, many technological solutions have been developed and implemented for possessing and using person-related administrative or health information in healthcare. Those technologies can be distinguished according to the medium deployed, according to the purpose the cards are used, or according to the mechanisms and functions provided.

Starting with simple paper cards which can only be written once and read many times, memory cards have been introduced. Providing different storage capacity, magnetic stripe cards, laser written and read optical cards or chip cards have been used to simply store the aforementioned information. Regarding the purpose of use, storage cards can be distinguished from tokens such as access cards, identity cards, authentication cards, signature cards, encoding/decoding cards, etc. Sometimes, cards are also classified by their medical dedication for supporting specific decease's care (e.g. DIABCARD for supporting the care of diabetes patients). Considering both structure and mechanisms applied, programmable processing facilities have been established forming processor cards, sometimes equipped with dedicated co-processors for supporting special complex algorithms. Processor cards are also known as smart cards. The purpose is often combined with special mechanism to provide the functions required. Frequently, several purposes and functions are realised deploying the same physical cards (multi-functional cards).

For electronic health information systems independent of whether it is possessed by patients or additionally network-based, beside the appropriate carrier also an environment must be provided for the authorised use of information in the sense of collecting, storing, processing, and communicating data. Starting in Europe, smart cards, i.e., microprocessor cards, have been used for both purposes mentioned, i.e., as Patient Data Cards (PDC) and Health Professional Cards (HPC) around the world for quite a long time [2, 3].

Generally, it should be mentioned that smart cards could be deployed in two ways. On the one hand, the card could bear all information needed, in the case of PDC, e.g., all relevant medical data as part of an EHR. On the other hand, the card can be used as a pointer providing just references and linkages to the information stored in networked systems. However, even a combination of those two principles could be imaginable.

2.2 Card-Enabled Network Security Infrastructure

In Europe and beyond, smart cards are frequently used for enabling communication and application security services for health networks and records. The basic principle consists of a certified binding of a principle (human user, organisation, device, system, application, component, or even a single object) to its electronic unique identifier or assigned properties, rights and duties, also called attributes of that principal. Communication security services concern the identification and authentication of communicating principals. In an end-to-end secure communication environment (object security), these services are used for authentication and control of access rights of principals communicating as well as integrity,

confidentiality, and accountability including non-repudiation of information exchanged. For object security, security aware principals are needed.

On the other hand, integrity and confidentiality of communicated data may also be provided at system level transparent to the application and the user – not requiring the user's specific awareness for those security measures (channel security). Application security services deal with authorisation and access control to data and functions, but also with accountability of principals, audit track and auditing of principals and services ensuring integrity, confidentiality of data and functions. In both concepts, notary's services have to be established. Another important requirement for communication and application security concerns the availability of information and services [4, 5, 6, 7].

3. The German Health Professional Card Specification

Based on results of the European TrustHealth project [3] and the Health Professional Card standard CEN ENV 13729 [2], the German HPC V 2.0 specification has been approved in July 2003 [8]. Its specification had to be linked to decisions setting up the organisational framework such as Trusted Third Party (TTP) services, Public Key Infrastructures (PKI), and related Registration and Certification Authorities (RA, CA). The legal framework for electronic signature processes became a national reality in December 1997 [9, 10, 11].

The main players in German health domain defined the Physicians' ID the first German implementation of a Health Professional Card as it is managed under the authority of the State Medical Associations. The electronic Physicians' ID is intended to completely replace the current paper-based Physicians' ID. For this reason, the Physicians' ID will have a distinctive card cover – similar to the paper-based one.

From a more technical point of view, the HPC is contact a based smart card capable to process Public Key (PK) algorithms. The physical characteristics shall comply with ISO/IEC 7816-1 and related standards. An HPC is a normal size card (ID-001 card). Other card layouts are currently under discussion, e.g. an institutional card (SMC) that could easily be considered a plug-in card (ID-000) for secure devices e.g. in pharmacies.

4. Standard Patient Data Cards and their Data Elements

When intending to generally provide open, interoperable solutions, they must be based on international standards. Regarding patient data cards, series of standards have been specified first at European level (CEN TC 251 "Health Informatics") and after its establishment at ISO TC 215 "Health Informatics" level.

4.1 Standardisation in the Patient Health Cards Domain

Developed under the Vienna Agreement by the ISO TC 215 WG "Health Cards" in collaboration with CEN TC 251, the ISO standard 21549 "Health Informatics – Patient health card data" [12] replaces the European Pre-standard ENV 12018 adopted by CEN back in 1995. ISO 21549 consists of the following parts:

- Part 1: General structure
- Part 2: Common objects
- Part 3: Limited clinical data
- Part 4: Extended clinical data
- Part 5: Identification data

- Part 6: Administrative data
- Part 7: Electronic prescription
- Part 8: Links

Person-related data carried on a data card can be categorised into three types: identification data (of the device itself and the individual to whom the data it caries relates), administrative data, and clinical data. It is important to realise that a given healthcare data card "de facto" has to contain device data and identification data and can in addition contain administrative and clinical data. Furthermore, patient data cards may support the collaboration with network-based systems. For that purpose, any type of link information has been specified. Patient data cards are widely used for a specific communication in patient's care: the electronic prescription. Because of the huge amount of performed transactions, e-prescription is indeed an important health card application, which itself guarantees the return of investment within a short time. Eventually, person-related cards analogue to HPC enable the use of established security infrastructure services.

A data card essentially provides specific answers to definite queries whilst at the same time a need to optimise the use of memory by avoiding redundancies "high level" Object Modelling Technique (OMT) has been applied with respect to the definition of healthcare data card data structures. Using a UML Class Diagram, figure 1 shows the overall structure for patient health card data according to ISO 21549 [12].

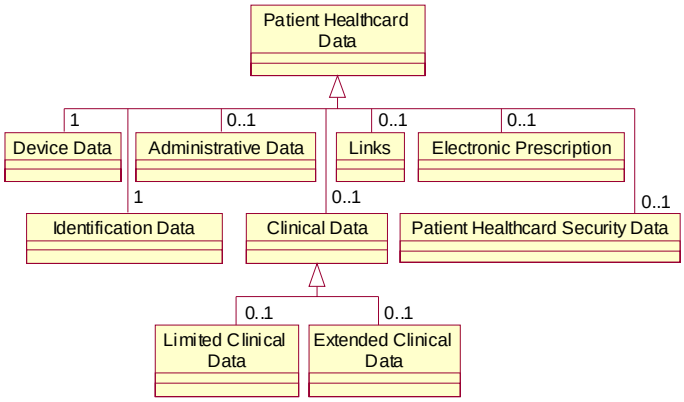

Figure 1 - General Patient Data Health Card Structure

4.2 The bIT4Health Project and the German Electronic Health Card

As many other countries, Germany has launched a national programme for establishing a health telematics platform supporting seamless care [13]. This platform combines card-enabled communication mediated by the patient with network-based interoperability between all actors involved. For the patient data card, called the German Electronic Health Card (elektronische Gesundheitskarte, eGK), a multi-purpose micro-processor card is used. It will serve as a health insurance card, an immunisation and vaccination passport, an electronic prescription carrier, a carrier for pointers to the patient's Electronic Health Record (EHR) components or related information such as drug information distributed on the net, and an information carrier for facilitating managed care and quality assurance [14].

At its backside, the German as well as the future European Electronic Health Card carries the so-called E111 form human readably containing all data needed for care of a citizen from an EU member state to be medically treated in another EU member state. Of course, this data set is also electronically stored on the smart card.

A specifically protected compartment contains information the patient likes to hide from being read by others. For any access to data others than the emergency data set, a Health Professional Card (Heilberufeausweis, HBA) is required. Additionally, the electronic health card provides basic security services based on cryptographic algorithms, such as strong authentication, integrity, accountability, and encoding / decoding services deploying the Qualified Electronic Signature [9, 10, 11] and a related Public Key Infrastructure (PKI).

The German bIT4health project will deploy the patient data card as token in prioritised applications. The priority of applications is defined by the possible savings, improvement of patient's safety as well as basic services for installing a health telematics and telemedicine platform. According to a business analysis, the replacement of the traditional paper-based prescription by electronic means will save about 700 million € a year. Expecting an amount of 1.5 billion € for implementing the health telematics infrastructural services described, the return of investments will be realised within 2 years [13].

Another aspect deals with the loss patient's safety due to medication errors or wrong information provided, which causes about 25.000 death patients a year in Germany. This number corresponds very well with the IOM study performed in the US mentioning 96.000 death patients for the same reasons in the USA. Therefore, e-prescription and medication file are prioritised. The latter may be stored on the health card or kept in a networking environment card-based pointers are referring to. Such solution can smoothly move towards the establishment of an Electronic Health Record (EHR) as the core application of any health telematics or telemedicine environment.
Without ignoring the huge social and societal savings by better patient safety avoiding harm or even death of patients (which is hard to calculate), the optimisation of medication due to the knowledge of the patient's medication applied as well as patient-related specific conditions by using medication files will easily save more than 1 billion € a year. ROI may even be realised within one year. The health card will be rolled out in 2006 replacing the currently used German health insurance card and providing added value services.

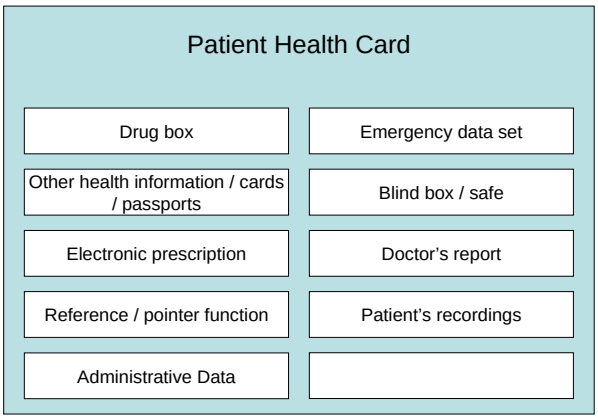

Figure 2 - Functional Blocks of the German eGK

Security services support both communication and application security services for any principals such as users, devices, systems, applications, components, or objects. Supporting trustworthy interoperability between patients and health professionals, the latter deploy Health Professional Cards (HPC) for adequate security services.

Another important aspect of the bIT4health project concerns the acceptance of offered telemedicine solutions by patients and health professionals. Earlier investigations on the acceptance of the DIABCARD demonstrated clearly that more than 95% of patients suffering from chronic diseases (e.g. diabetes) have highly appreciated or appreciated the use of specific patient health cards. For convincing citizens of storing personal health data on patient's health cards, the voluntary choice of specific applications as well as the control functions by patients or at least by trustworthy health professionals is a basic requirement.

5. Conclusions

Shared care solutions all over the world have to be based on trustworthy communication and application security services. Smart cards in general, Patient Identification Cards,

Patient Data Cards, and Health Professional Cards play an important role either as ID token or as health data carrier. Cards have an impact on the related security infrastructure, certification of processes, process interoperability (workflow), and certification of state and relations of principals in longer terms. This is especially true for the upcoming fast development on Electronic Health Record (EHR) architectures, their requirements, their design, their policy details, and their instantiation and implementation strategies.

6. Acknowledgement

The authors are in debt to the European Commission for the funding of several European research projects and especially to the project partners within the "HARP" project as well as all other partners and organisations for their support and their kind co-operation.

7. References

[1] Blobel B. Analysis, Design and Implementation of Secure and Interoperable Distributed Health Information Systems. Series "Studies in Health Technology and Informatics" Vol. 89. IOS Press, Amsterdam 2002.

[2] CEN TC 251 ENV 13729 "Health informatics - Secure user identification – Strong authentication using microprocessor cards (SEC-ID/CARDS)", 1999

[3] TrustHealth: The European TrustHealth Project (1996 – 2000). Project Description and Deliverables. http://www.ehto.org/ht_projects/initial_project_description/trusthealth.html

[4] Object Management Group, Inc.: CORBA Specifications. http://www.omg.org

[5] ISO/IEC 10746-2 "Information technology – Open Distributed Processing – Reference Model: Part 2: Foundations".

[6] Blobel B, Pharow P (Edrs.): Advanced Health Telematics and Telemedicine. The Magdeburg Expert Summit Textbook, pp. 21-28. Series "Studies in Health Technology and Informatics" Vol. 96. IOS Press, Amsterdam 2003

[7] Damianou N, Dulay N, Lupu E, Sloman M. Ponder: A Language for Specifying Security and Management Policies for Distributed Systems. The Language Specification, Version 2.3. Imperial College Research Report DoC 2000/1. 20 October, 2000.

[8] The German Specification for a Health Professional Card v 2.0. PDF Document (English version). http://www.heilberufeausweis.de/

[9] The German Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften – SigG): English version, May 16th, 2001. http://www.iid.de/iukdg/gesetz/engindex.html

[10] The German Electronic Signature Ordinance (Signaturverordnung – SigV): English version, November 2001. http://www.iid.de/iukdg/gesetz/engindex.html

[11] The European Electronic Signature Standardization Initiative (EESSI) – an Industry Initiative in Support of the European Directive on Electronic Signature. http://www.ictsb.org/EESSI_home.htm

[12] ISO standard 21549 "Health Informatics – Patient health card data", 2003

[13] bIT4Health. The German Electronic Health Card Project. Descriptions and Specifications (partly in English). http://www.dimdi.de/de/ehealth/karte/index.htm

[14] The German Specification for an Electronic Health Data Card v 1.1. PDF Document (English version). http://www.dimdi.de/de/ehealth/karte/technik/kartenspezifikation/index.htm

Address for Correspondence

Peter Pharow, Fraunhofer Institute for Integrated Circuits IIS, Image Processing and Medical Engineering Department, Health Telematics Project Group, Am Wolfsmantel 33, D-91058 Erlangen, Germany
Phone: +49-9131 / 776-7350, Fax: +49-9131 / 776-7399, E-mail: peter.pharow@iis.fraunhofer.de
URL: http://www.iis.fraunhofer.de