Integrated Circuit Health Data Cards (Smart Cards)

A Primer for Health Professionals

Technology and Health Services Delivery
Health Services Organization Unit (THS/OS)

Pan American Health Organization
Pan American Sanitary Bureau, Regional Office of the
World Health Organization

Integrated Circuit Health Data Cards (Smart Cards)

A Primer for Health Professionals

Technology and Health Services Delivery
Health Services Organization Unit (THS/OS)

Pan American Health Organization
Pan American Sanitary Bureau, Regional Office of the
World Health Organization

May 2003

Otto Rienhoff

Professor, Medical Informatics
Director, Medical Informatics Department and Head of the Hospital Computer
Center, Georg-August-University, Goettingen, Germany

Contributors

Roberto J. Rodrigues

Adjunct Professor, Science, Technology and International Affairs Program
School of Foreign Service, Georgetown University, Washington D.C., USA
Senior Consultant, The Institute for Technical Cooperation in Health Inc
(INTECH), Potomac MD, USA

Ursula Piccolo
Research Assistant, Medical Informatics Department
Georg-August-University, Goettingen, Germany

Antonio Hernandez

Regional Advisor, Clinical Engineering and Maintenance
Pan American Health Organization/World Health Organization
Washington D.C., USA

Nora Oliveri

President and Chief Executive Officer
Fundación de Informática Médica, Miami FL, USA

Acknowledgement

Contents

Foreword

The past century has witnessed significant achievements in the health status in the Americas but new and complex challenges confront the Region. Governments and other key social sectors are acutely aware of the need to reduce the existing gaps in access to health services and in the quality of care. The increasing mobility of citizens, internally in each country and internationally, the expanding process of regional integration, and the new models of health sector organization characterized by multiple public-private providers have underscored the problem of how to provide quality evidence-based care regardless of location of facilities and provider. At the same time, the international dimensions of public health and its close links with the national and local situation, also ethical and privacy issues, demand novel ways to deal with the recording, maintenance, and access to the medical life history and clinical data of individuals.

The streamlining and reduction of paper flow and traditional medical records by electronic technology solutions offer an opportunity to better balance the management of clinical and administrative data. Patient and provider "smart cards", because of their portability can effectively address some of the issues faced by the health sector in its quest for the continuous improvement of health systems, the promotion of rapid advances in securing geographical, cultural, and financial access to health services, and expansion of social protection mechanisms. The introduction of "smarts cards" was also an important step in the direction of implementing a patient-centered model of health records and stimulated many research groups to address the issues of standardization of clinical data and medical records. The benefits of this technology have already been demonstrated in the European Community.

The convergence of multiple digital technologies, the increased capacity and speed of modern computers, and the ubiquity of telecommunications affordable data processing and data communication propelled the widespread deployment of computerized information applications in the health sector of Latin America and the Caribbean. Much, however, remains to be done, as still continue to exist a dissonance between the

expressed desire for change, and the actual incorporation of information technology by the sector.

In keeping with the mandates of the Summits of Presidents and Heads of State and Government, the Pan American Health Organization has emphasized the importance of technical cooperation for capacity building and for guaranteeing self-sufficiency, autonomy, excellence, and sustainability. It is in this context that this introductory text, directed at the health professionals of the Americas, was conceived and written under the direction of Prof. Rienhoff, of the University of Goettingen, Germany, an authority in the area of health cards.

Mirta Roses Periago
Director
Pan American Health Organization

Executive Summary

This report summarizes fifteen years of international development, current status, and trends in the technology and utilization of "smart" data cards, the most successful of card–size portable devices for storage and transportation of clinical and administrative health data.

A "smart card" or "chip card" is a credit card size plastic device with one or more integrated circuit (IC) semiconductor chips embedded in its body. The IC chips store and transact data between card users. Data is associated with either monetary value or information or both and is stored and, in specific types of cards, processed within the card's integrated-circuit chip read-and-write memory or microprocessor. The card data is transacted via a card reader – a peripheral device attached to a stand-alone or networked computer system. Several related issues, such as the relation of data cards to networks, biometric identification, mobile communication, implementation issues, and regulatory and legal aspects are discussed in this publication.

Smart cards greatly improve the convenience and security of any transaction as they provide tamper-proof storage of user and account identity and personal data. Smart cards can be the core module for systems security in the exchange of distributed data throughout any type of electronic communication network. They protect against a full range of security threats, from careless custody of user passwords to sophisticated attempts to break into the stored data. Multifunction cards can, besides serving as access devices to network system, be efficiently used to store monetary value and data related to separate applications.

The potential of innovative smart card-based solutions is evidenced by the multitude of reliable and secure applications which can be implemented on a single card: identification, data sets, payments, booking, authentication, and logical and physical access to information systems, applications, databases, and facilities.

Smart cards are being used successfully to store patient medical records. The majority of the health smart card implementations are found in Europe, where the technology has achieved greater development and acceptance. Early health data cards projects started in the mid-80's were followed by implementations and pilot projects of diverse scope and size in many countries and organizational settings. Several countries have implemented card systems with different levels of success and sustainability. Since them health card projects of different types have been started at national, regional, or provincial level including functions that span more than one social area. Cards have been also extensively adopted by the private health sector, by insurance companies, and by many industry and municipal government occupational health programs.

Innovative technical development in data cards and their linkage with health networks is rapidly advancing. Although small in number, economical impact studies have shown positive results in health data card implementation projects – the most dramatic reports refer to the first generation of smart cards implemented in Germany in the mid-nineties, where the implementation costs were returned within two years by the savings accrued on administrative costs in the insurance system. Similar expectations accompany the introduction of an electronic prescription in Germany which is being planned at the time of this report (2003). Economic returns in other card projects and those related to the implementation of the much more complex card-based professional security infrastructure (health professional cards) are expected to result in a similar positive investment outcome.

Data cards must be considered as only one of a continuum of information and communication technologies (ICT) to be deployed in the context of a national health informatics infrastructure or architecture. A comprehensive review of the experiences reported at a 1994 working conference in Athens and the in depth analysis of the Maryland Blue Cross Project, done in 1996, documented that a health data card implementation requires the existence of a number of prerequisites that must be in place for successful deployment and use of the technology. Of particular consequence, data cards must be considered in the context of an overall information systems infrastructure for health and cannot be simply and economically introduced as a stand-alone or isolated solution.

2

Hundreds of small health data cards projects failed to materialize or to survive initial deployment mostly because they ignored the lessons from previous experiences and the requirement to have those essential prerequisites in place. At national level, the most striking failure was the ambitious U.S. health card project proposed during the Clinton administration and never implemented. More recently, another failure to survive initial pilot operation, this time in the Netherlands, emphasized the complexity of such projects and the difficulties in switching to generalized operation.

Health data cards have also triggered intense debates regarding data protection, privacy, patient rights and access issues to personal data, and cross-border data flows. Those ethical, regulatory, and legal discussions are compounded by the great disparity of controlling mechanisms regarding how data is regulated and ethically perceived by different societies. Besides health-related definitions and technological specifications of ethical, regulatory, and legal issues have to be dealt with, agreed upon, and consolidated in a body of regulations or laws before nationwide data cards systems containing personal data can be implemented.

Cards are part of a progressively changing healthcare information technology infrastructure. New health data card projects must consider the lessons learned from initiatives developed over the part fifteen years and look forward into the future by considering the variety of emerging technological options of the present. However, only a balanced consideration of those two perspectives – past experiences and present-day opportunities – associated with the establishment of a project environment that emphasizes consensus among stakeholders, standardization, and financial sustainability will lead to success.

The future of smart card technology in health remains bright. Application deployment, functionalities, and interactivity with applications related to other social sectors are likely to increase in both the private and public health subsectors. Public central/federal government applications are expected to materialize more slowly than local/state/county applications due to the diverse requirements and characteristics of the services that each provide. Generally speaking,

central/federal government services tend to require greater levels of security, are more sensitive to privacy issues, and are much more complex and costly to deliver. Nevertheless, central/federal government services appear to have the greatest need for the functionalities provided by smart card technology.

The collected experience of the past decade and a half recommends that the following aspects should be taken into account in the design, development, and implementation of health data card initiatives:

- Compared to conventional data transmission devices such as magnetic stripe cards, smart cards offer enhanced security, convenience, and economic benefits. In addition, smart card systems are highly configurable to suit individual needs. Finally, multifunctional capability such as storage, payment, application, and networking in a same device makes smart cards as the perfect user interface in a mobile, networked economy.

- All information and communication technology projects in health should aim to achieve quality improvement of healthcare processes, higher effectiveness and efficiency of operations and individual care, and a clear return on investment.

- In each implementation, detailed workflow analyses and a feasibility assessment that considers expected results, assumptions, and risks must be done in close cooperation with citizens, patients, professional associations, participating institutions, regulatory agencies, funding sources, and health professionals.

- Smart card-based solutions must never be considered as "off-the-shelf" products. Cards and electronic networks are two components of the same issue and both technologies should be coupled. Particularly, patient cards are one element of an integrated information and communication technologies (ICT) infrastructure in health – the success of projects depends on

the fine-tuning of goals, project resources, functionalities, interoperability, and interfaces between the card subsystem, the health information systems, and the health system in which the card applications will live.

- Implementations must, as much as possible, use well-tested technical, interface, and interoperability standards that have been developed and fully deployed in successful initiatives. Lessons from earlier card projects have been widely published and projects should build on the evaluation and evidence from such experiences and not on one-dimensional policy papers.

- Card systems consist of a mix of ICT technologies, organizational processes, and persons. Motivation, information, and training are essential to operate and reap the full benefits of new card-controlled workflows.

- The more interoperable they are, data card projects become more complex. This is not because of the card technology *per se,* but because of the need to make a large number of related medical application systems interoperable.

- Although experimentation is important, it should be left to research projects deployed in a carefully defined domain with well-controlled environmental variables.

- Notwithstanding the previous consideration of remaining with the tried and true, data cards, like all other ICT application areas, are in constant development. The life cycle of digital and telecommunications technology is very short and, although most of the times it is difficult to recognize which emerging technology will survive, projects must attempt to foresee such developments in a 5 to 10 year horizon and must imaginatively look beyond today's technological options.

- When data cards are already being in use for personal identification, motor vehicle driver's license, financial or credit transactions, etc. it is wise to investigate whether such

resources for implementation. If not available, other second best data security solutions have to be found.

- Cross-border (countries, states, provinces) solutions are difficult to implement and enforce – particularly in reference to data definition standards, security, and personal data access issues. However, on the long run they offer major benefits for citizens.

- The number of experts and companies with advanced knowledge and experience in the area is limited.

implementations could be shared with the planned health application provided that data protection for the patient is guaranteed and the project remains technically and organizationally manageable.

- The experience indicates that the implementation of card systems on a voluntary basis results in limited use and failure to reap the full benefits of the technology – the only way such benefits can be accomplished is by compulsory utilization. This strategy may conflict with personal data protection and legal issues.

- The experience has demonstrated that health data card projects must be of considerable size in order to create a significant impact on an existing health ICT environment. Functioning health ICT infrastructure and applications take a long time to develop and deploy and once implemented there is a tendency for those to continue to exist without much change and to resist potentially disruptive realignments.

- Health data card projects require long-term financial planning, a clear understanding by all stakeholders of the capital and operational costs involved, the responsibilities and commitment that must be assumed by each project participant, and the awareness that upgrades or eventual extensive and costly replacements may be necessary in a relatively short time.

- Because of the sensitivity of medical and personal data, security is an absolute requirement for the deployment of interoperable card solutions.

- Data cards containing patient medical data require a regulatory and legal infrastructure that defines who is allowed to access or change the information – including the rights of the patient to access and change personal data.

- Security infrastructures based on health professional cards (HPCs) and Public Key Infrastructures need much time and

distribution of everything from emergency data to eligibility and benefit status, rapid identification of patients, improved care, the convenience of transporting data between systems or to sites without systems, and reduction of record maintenance costs.

- Telecommuting and Corporate Network Security - business to business Intranets and Virtual Private Networks (VPNs) are enhanced by the use of smart cards. Users can be authenticated and authorized to access specific information according on predetermined privileges. Additional applications range from secure electronic mail to electronic commerce

1.2. Types of Smart (Embedded Integrated Circuit) Cards

Smart cards are defined according to the type of integrated circuit chip or chips embedded in the card and their capabilities (Figure 3).

CAPACITY
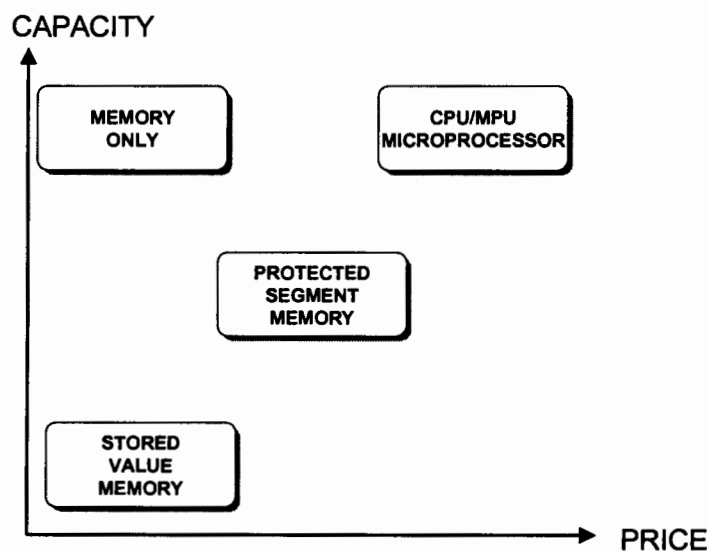
Figure 3. Functionality and Performance of Different Integrated Circuit (IC) Card Technologies

15

1. Data Card Technology Overview

A "smart card" or "chip card" is a plastic card embedded with one or more integrated circuits (IC) that store and transact data between users (Figure 1). Smart cards semiconductor chips can be linked to external reading devices, specialized terminals, or different types of computers via physical surface contact points or by contactless proximity communication through interference antennas.
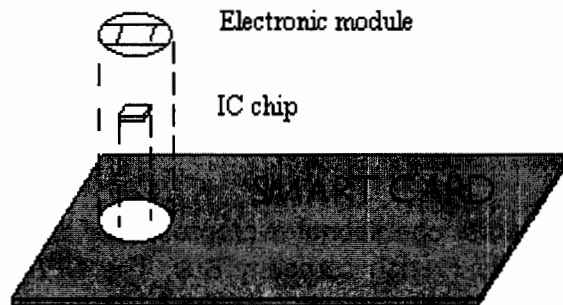
Figure 1. A smart card is a plastic card embedded with one or more integrated circuit chips. Depending on the type of the embedded chip or chips, smart cards are categorized as memory cards, processor cards, or with both types of chips

While any IC-embedded card may be called a smart card, the distinguishing feature of a smart card is its use for personal activities. For example, personal computer cards of the standard known as PCMCIA (Personal Computer Memory Card International Association) have the same technological characteristics of a smart card but they are

used as computer peripheral devices such as modems, storage devices, or game cartridges. These PC cards are never called smart cards since they are hardware extension devices without personalization. In this sense, a smart card is a processor card that allows persons to interact with others digitally in order to conduct transactions and other personal data-related activities.

Cards may have only a memory chip or both memory and microprocessor chips. Data associated with either monetary value, information, or both is stored and, in cards with microprocessor, processed within the chip. The microprocessor chip of a card is equivalent to the central processing unit (CPU) of a microcomputer and therefore capable of performing logical operations.

In microprocessor cards, a portion of the memory chip is used for the storage of programs and thus such cards can be programmed by transferring appropriately developed algorithms to its erasable programmable read-only memory area (EPROM). Normally, the IC card data is transacted via a reader that is a peripheral device in a stand-alone or networked computer system.

In 1979 the first operational microprocessor card (two-chip card) was launched by the French company Bull. The CP8 Card housed a memory chip and a microprocessor supplied by Motorola (Figure 2). The new product was built around the 3870 model monochip and a 2716 model EPROM (Erasable Programmable Read-Only Memory) addressed through the monochip's parallel input/output ports. Assembly took place according to novel techniques developed by Jacques Villières at the Toulouse Motorola plant.

By the mid-90's, cards with up to 2 K (2,000 bytes or characters) of read-and-write memory became available and heralded a sudden increase of projects in several countries. Since then the complexity and efficiency of card design has grown dramatically. Presently cards can be tailored to the needs of each specific project and even specific processors, e.g. for advanced cryptography requirements unique chips can be added to the card circuitry.

10
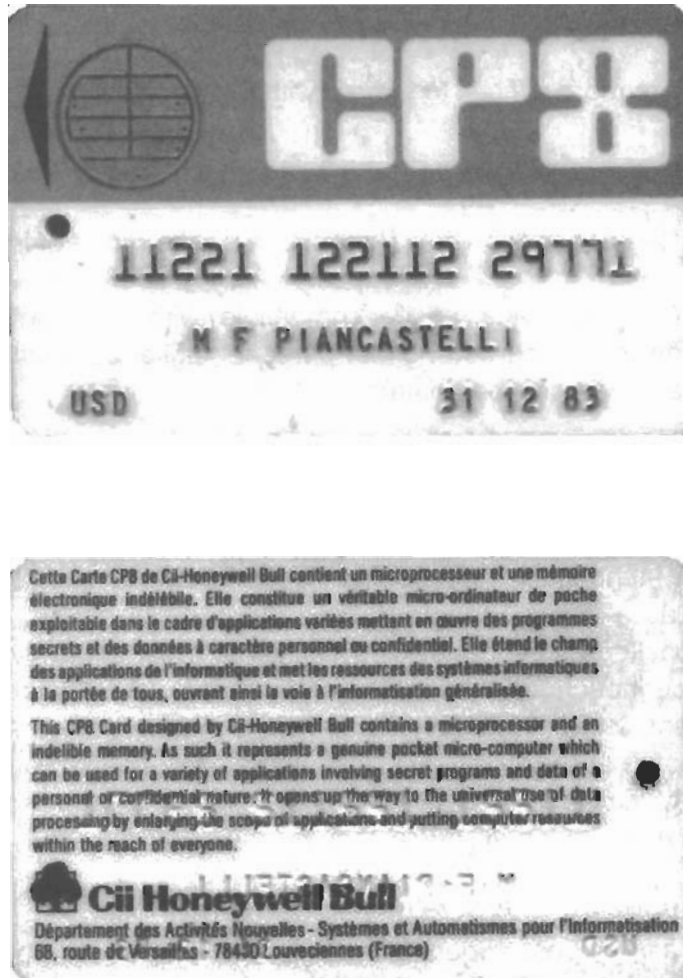
Figure 2. The Bull CP8, the first microprocessor card (1979)

The most evident benefits linked to the use of integrated circuit smart cards are:

- They a more reliable than a magnetic stripe card for identification purpose,

- Store considerably more information than magnetic stripe card,

- Are more difficult to tamper with than magnetic recordings,

- Can be disposable or reusable,

- Can perform multiple functions in a wide range of industries.

- Can be made easily compatible with portable electronic devices such as phones, personal digital assistants (PDAs), and personal computers.

1.1.   Areas of Application

First launched in Europe two decades ago, smart cards where introduced as a stored monetary value tool for pay phones to reduce theft of deposited coins. Smart card-enhanced systems are widely used today throughout several key applications, including banking, entertainment, and transportation and billions of smart cards are already in use. Western Europe accounts for about 70% of the current smart card uses, followed by South America and Asia with about 10% each, while North America languishes at less than 5%.

Most smart cards issued are memory cards with limited processing capabilities. About 75% of the cards in use are phone cards. Many industries have implemented the power of smart cards into their products such as Global System for Mobile Communications (GSM) digital cellular phones, General Packet Radio Service (GPSR) devices, and satellite television decoders. To various degrees, all applications can benefit from the added features and security that smart cards provide. In the U.S., notwithstanding the low penetration, consumers have been using integrated circuit cards for everything from secure identification, facility access control, banking, libraries, buying groceries, and attending movies. Several states have chip card initiatives in progress for government applications ranging from motor vehicle registration to Electronic Benefit Transfer (EBT).

According to Dataquest, the worldwide smart card market reached 4.7 billion units and US$ 6.8 billion by the end of 2002. Examples of well-established applications are:

- Loyalty and Stored Value - a primary use of smart cards is stored monetary value, particularly loyalty programs that track and create incentives to generate repeat customers. Stored value is more convenient and safer than cash. For the card issuers, float is realized on unspent balances and residuals on balances that are never used. For multi-chain retailers that administer loyalty programs across many different businesses and point of sale (POS) systems, smart cards assist in data tracking. The applications are numerous, from parking and laundry service to gaming, as well as all retail and entertainment uses.

- Badging and Access - businesses and organizations of all types need simple identity cards for all employees, temporary workers, students, etc. Most of these people are also granted access to certain data, equipment and departments according to their status. Multifunction, microprocessor-based contact and contactless smart cards incorporate identity with access privileges and also store value for use in various locations, such as cafeterias and stores.

- Securing Information and Physical Assets - in addition to information security, smart cards can provide high-level physical security of services and equipment since the card restricts access to all but the authorized user. E-mail and personal computers (PCs) can be locked-down with smart card, the most unobtrusive solution being the contactless proximity card. Information and entertainment being delivered to the home or PC as digital video broadcasts are using smart cards as electronic keys for protection – they control decryption of broadcast and individual subscriber access and billing for services. Smart cards can also act as keys to machine settings for sensitive laboratory equipment and for automatic dispensers of drugs, tools, library cards, health club equipment, etc.

- Portable Safe Box – smart cards can be used a sort of "safe deposit box" for encryption keys and for algorithms related to digital signatures and authentication. It is safer to carry such sensitive data in a card than in other portable devices such as palmtop computer and PDAs.

- E-Commerce - smart cards make it easier for consumers to securely store information and cash for purchases. Advantages include: the card can carry a personal accounting application, credit and buying preference information that can be accessed with a mouse click instead of filling out forms; cards can manage and control expenditures with automatic limits and reporting; Internet loyalty programs can be deployed across multiple vendors with disparate point of sale systems; and they can be used as a secure depository for points or rewards and for "micro payments", i.e., for paying nominal costs without the transaction fees normally associated with credit cards or for amounts too small for cash or credit card, like reprint charges.

- Personal Finance - as banks enter newly opened highly competitive markets, such as investment brokerages, they are at an increased rate implementing applications to support secure transactions via smart cards. This results in improved customer service and secure 24-hour electronic fund transfer over the Internet with reduced costs since transactions that normally would require a bank employee's time and paperwork can be managed electronically by the customer with a smart card.

- Health Care - the growing multi-professional health practice and the explosion of healthcare data bring about new challenges regarding access to data generated by different care-givers in many care sites, the importance of integrating clinical data for the effectiveness and efficiency of patient care, and the need to safeguard privacy in an increasingly networked environment. Smart cards have the potentiality of solving those challenges thanks to secure storage and

There is a wide range of options to choose from and increased levels of processing power, flexibility, and memory add functionalities and obviously cost. Single function cards are often the most cost-effective solution and choosing the right type of smart card for a specific application is done by the careful assessment of cost versus functionality and by determining the required level of security.

Memory Cards

Memory cards have no sophisticated processing power and cannot manage files dynamically. All memory chips communicate with readers through synchronous protocols. There are three primary types of memory cards:

- Straight Memory Cards - these cards just store data and have no data processing capabilities. These cards are the lowest cost per stored byte for user memory. They should be regarded as floppy disks of varying sizes without a security function. These cards cannot identify themselves to the reader, so the host system has to know what type of card is being inserted into a reader.

- Protected / Segmented Memory Cards - these cards have built-in logic to control the access to the card memory. Sometimes referred to as "intelligent memory" cards these devices can be set to write-protect some or all of the memory storage area. Some of these cards can be configured to restrict access to both reading and writing. This is usually done through a password or system key. Segmented memory cards can be divided into logical sections if multi-functionality is desired.

- Stored Value Memory Cards - these cards are designed for the specific purpose of storing monetary value or tokens. The cards are either disposable or rechargeable. Most cards of this type incorporate permanent security measures at the point of manufacture. These measures can include password keys and logic that is hard-coded (wired) into the chip by the manufacturer. The memory arrays on these devices are setup

as decrements or counters. There is little or no memory left for any other function. For simple applications such as a telephone card the chip has 60 or 12 memory cells, one for each telephone unit. A memory cell is cleared each time a telephone unit is used. Once all the memory units are used, the card becomes useless and is thrown away. This process can be reversed in the case of rechargeable cards.

CPU/MPU Microprocessor Multifunction Cards

These cards have on-card dynamic data processing capabilities. Multifunction smart cards allocate card memory into independent sections assigned to a specific function or application. Within the card there are one or more microprocessor or microcontroller chips that manages this memory allocation and file access. This type of chip is similar to those found inside all personal computers and when embedded in a smart card, manages data in organized file structures, via a card operating system (COS). Unlike other operating systems, this software controls access to the on-card user memory.

This capability permits different and multiple functions and different applications to reside on the same card, allowing businesses to issue and maintain a diversity of "products" through a single card. One example of this is a debit card that also enables building access on a college campus. Car applications that require high security can have a specific cryptoprocessor on board responsible for running encryption routines.

Multifunction cards benefit issuers by enabling them to market their products and services via state-of-the-art transaction technology. Specifically, the technology permits information updates without replacement of the installed card base, greatly simplifying program changes and reducing costs. For the card user, multifunction means greater convenience and security, and ultimately, consolidation of multiple cards down to a select few that serve many purposes.

A

1.3. Card Communications, Reader, and Terminal Basics

The term "reader" is used to describe a piece of hardware that interfaces with a personal computer (PC) as a peripheral device for the majority of its processing requirements. In contrast, a "terminal" is a self-contained card processing device. Both readers and terminals read and write to smart cards. Smart cards can communicate with a reader or terminal by two forms, singly or combined:

- Contact smart cards - the connection is made when the reader or terminal contacts a small gold-plated area on the front of the card.

- Contactless or proximity smart cards – These can communicate by radio frequency (RF) via an antenna, eliminating the need to insert and remove the card in a reader or terminal. With a contactless card, all one has to do is get close to a special wireless terminal, in this case a "receiver", and the card will begin communicating with it. Contactless cards can be used in applications in which card insertion and removal may be impractical or in which speed is important. Some manufacturers are making cards that function in both contact and contactless modes.

Both technologies have advantages and disadvantages. While contact cards have standardized international physical pin positioning and transmission protocols contactless RF cards are still not generally interoperable although the Philips MIFARE® solution, an ISO 14443A-compliant commercial product, seems to become widely accepted and has an immense worldwide installed base. The platform offers a full range of compatible contactless smart card and reader ICs, as well as dual interface ICs that provide a secure link between the contactless and contact card markets.

It is expected that functions that are presently still limited to contact cards, e.g. signature functions, in the near future will be realized also by contactless cards. The same applies for multi-processor cards. Years ago only one chip could be build into cards – today a card can hold several specialized chips. Integrated circuit data card are becoming

more and more a tiny highly integrated and specifically tailored computer system for well-defined functional needs.

Reader devices come in many form factors and in a wide variety of capabilities. The easiest way to describe a reader is by the method used when interfacing with a PC. Smart card readers are available with connectors for interface with the RS232 serial port, USB port, PCMCIA slot, floppy disk slot, parallel port, infrared IRDA port and keyboard wedge readers. Another differentiation regarding reader devices relates to the on-board intelligence and capabilities or lack thereof. Wide price and performance differences exist between an industrial-strength intelligent reader that supports a wide variety of card protocols and a home-use card reader, that only works with microprocessor cards and performs all processing of the data in the PC. The options for terminals are just as wide although most units have their own operating systems and software development tools. They typically support other functions such as magnetic stripe reading, modem functions, and transaction printing.

Every new card project must consider existing and coming technological possibilities and to carefully evaluate them according to project objectives and requirements. Of course costs will be the main determinant in adoption and development of a business case and overall systems costs in relation to different arrangements of components of the card system and its interfacing technology are of paramount importance in reaching a decision for one option or the other.

1.4. Standards

Initially, there was a degree of conflict between the standardization work carried out by the Comité Européen de Normalisation (CEN), the European standardization body, and the International Standards Organization (ISO). ISO started to address standardization issues of medical informatics and information and telecommunication technologies much later than its European counterpart but soon after both groups initiated a close collaboration and ISO took over the main standard development activities from CEN.

Presently, both organizations are linked to other national standard-developing organizations and mirroring bodies.

Application-specific standards have been examined and implemented by many large organizations and research groups. Some commercial products still use proprietary standards but there is a growing trend toward open systems and conformity to international standards. Open systems for card interoperability apply at several levels to the card itself, access readers and terminals, and to networks and the card issuers' own systems. Present major organizations active in smart card standardization are:

- International Standards Organization (ISO) - facilitates the creation of voluntary standards by a collaborative process open to all interested parties. ISO 7816 is the international standard for integrated circuit cards that use electrical contacts. Anyone interested in achieving a technical understanding of smart cards must become familiar with such standard.

- National Institute of Standards and Technology (NIST) - published a document known as FIPS 140-1, "Security Requirements for Cryptographic Modules". This concerns physical security of a smart card chip, defined as a type of cryptographic module.

- MasterCard, Visa, and Europay Integrated Circuit Card Specification for Payment Systems - the specification is intended to create common technical basis for card and system implementation of a stored value system. Integrated Circuit Card Specifications for Payment Systems can be obtained from a Visa, MasterCard, or Europay member bank.

- PC/SC Specification - proposed by Microsoft as a standard for cards and readers applicable to CPU/MPU Microprocessor Cards interacting with 32 bit Windows-based platforms for personal computers. PC/SC does not currently support non Win32-based systems.

20

- CEN (Comité Européen de Normalisation) and ETSI (European Telecommunications Standards Institute) – their work is focused on telecommunications standards, as the GSM SIM for cellular telephones, GSM 11.11, and ETSI300045.

- OpenCard Framework - an open standard that provides interoperability of smart card applications across networks, point of sale terminals (POS), desktops, laptops, and other digital devices. OpenCard promises to provide 100% "pure" Java-based smart card applications. Smart card applications often are not self-contained because they communicate with an external device and use libraries on the client. OpenCard also provides developers with an interface to PC/SC for use of existing devices on Win32 platform.

- eEurope Smart Cards initiative and the Open Smart Card Infrastructure for Europe (OSCIE) - the eEurope Smart Cards initiative gathered a vast community of industry experts, users, operators, and academics with the objective of accelerating and harmonizing the development and use of smart cards across Europe. It led to the production of a set of common specifications containing guidelines, best practices, technical specifications and requirements for political, legislative or technical action.

Since August 1998, the ISO Technical Committee TC215 and its five Working Groups is responsible for standardization work in the area of health informatics and information and telecommunication technologies. The Working Group 5 (Health Cards) was set up in April 1999. The ISO/TC215/WG5 focus is on standardization of content and not on its underlying technology. The Technical Committee addresses standardization issues related to machine-readable cards for healthcare use including technology-dependent data structures, interoperability and compatibility, data communication, and record linkage.

Technological standardization issues are the responsibility of other groups, the most important being the ISO JTC1/SC17 (Information Technology – Identification Cards and Related Devices), which among

others produces the 7816 standard series. Smart card standards covered by ISO 7816-1, 7816-2, and 7816-3 govern the physical properties and communication characteristics of embedded chips. The working group only considers credit-card size devices [1]. The ISO 7816 specifications cover a number of areas, some are stable and others are in revision. One should check with ISO or the American National Standards Institute (ANSI) for the most current revision. ISO 7816 has six parts, some have been completed while others are currently in draft stage:

- Part 1: Physical characteristics (ISO 7816-1:1987) - defines the physical dimensions of contact smart cards and their resistance to static electricity, electromagnetic radiation, and mechanical stress. It also describes the physical location of integrated circuitry, magnetic stripe, and embossing area.

- Part 2: Dimensions and Location of Contacts (ISO7816-2:1988) - defines the location, purpose, and electrical characteristics of the card metallic contacts.

- Part 3: Electronic Signals and Transmission Protocols (ISO 7816-3:1989) - defines the voltage and current requirements for the electrical contacts as defined in Part 2 and asynchronous half-duplex character transmission protocol (T=0). Amendment 1:1992 Protocol type T=1, asynchronous half duplex block transmission protocol. Smart cards that use a proprietary transmission protocol carry the designation, T=14. Amendment 2:1994 Revision of protocol type selection.

- Part 4: Inter-industry Commands for Interchange (ISO 7816-4) - establishes a set of commands for CPU cards across all industries to provide access, security, and transmission of card data. Within this basic kernel, for example, are commands to read, write, and update records.

- Part 5: Numbering System and Registration Procedure for Application Identifiers (ISO 7816-5:1994) - establishes standards for Application Identifiers (AIDs). An AID has two parts: the first is a Registered Application Provider Identifier

(RID) of five bytes that is unique to the vendor while the second part is a variable length field of up to eleven bytes that RIDs can use to identify specific applications.

- Part 6: Inter-industry Data Elements (ISO 7816-6) - details the physical transportation of device and transaction data, answer to reset, and transmission protocols. The specifications permit two transmission protocols: character protocol (T=0) or block protocol (T=1). A card may support either but not both. (Note: Some card manufacturers adhere to neither of these protocols. The transmission protocols for such cards are described as T=14).

1.5.   Biometrics

Biometrics is the linkage of an identification protocol to a human attribute – something that cannot be stolen, faked, or lost. A number of markets, military and national security agencies, airport security, banking, and other areas were early adopters of biometric identification and the necessary hardware and software have rapidly matured and many commercial alternatives are presently offered by the informatics industry.

Fingerprint-based biometrics is the most common solutions, primarily because multiple-workstation environments make their use easier, the technology is affordably priced, and the required sensors are small. Optical fingerprint sensors, the most prevalent and mature form use an image template. A difficulty faced by users is that changes in the skin surface produced by dirt, oils, stains, and abrasions may result in mismatches but error correction features, based on intelligent software, may be able to correct most of those mismatches. New technologies, based on ultrasound and silicon sensors, use high-frequency sound waves or radio frequency combined to video technology and electronic arrays to reach below the skin surface to capture the unique pattern of ridges in the deep skin layer and thus avoid surface anomalies or skewed finger placement on the sensor.

The human iris provides the most accurate biometric attribute that can be easily accessed but its generalized use was hindered by the expensive cameras required to capture iris images. Until recently, iris recognition technology was used primarily in physical access high-level security applications using wall-mounted units near doorways. The appearance of small new cameras with advanced but cheap technology has opened the way for the use of iris-based identification by the mainstream market.

Biometric identification is already being incorporated in handheld, laptop computers, and wireless devices and miniaturized thermal-based devices for fingerprint identification and cameras that fit in a cell phone, palmtops, and personal digital assistants (PDAs) have recently been introduced. The health sector is seen as a major market for secure identification and access control devices [2, 3].

1.6. New Technologies

Currently, smart cards have up to 128 KBytes of EPROM (Erasable Programmable Read-Only Memory) memory. This capacity is expected to be further extended. Possible long-term competitors for cards are the emerging USB-based (Universal Serial Bus) devices which can be plugged directly in any computer and, since USB ports are ubiquitous standard input-output components of desktops and laptops, their use would obviate the need for card readers or terminals.

The European countries have adopted the strategy of building a common public key infrastructure (PKI) encryption model within the context of the ISO-7816 combined with intergovernmental agreements for mutual client authorization without a standard for terminals so far. In Japan, the NICSS (Next Generation IC-Card System Study) Project is developing multiple application contactless cards for safeguarding governmental Web-based applications. The NICSS approach to interfaces is more rigorous than the European General Interoperability Framework (GIF).

The most common wireless communication offerings today are compatible with 802.11b (WiFi) wireless LANs, which provide Ethernet

speeds of up to 10 MBytes/sec. They also provide a range of up to about 100 meters from a transmitter/receiver node, depending on the construction of the walls and configuration of the electrical wiring and plumbing in a building. An inexpensive postage stamp size WiFi card can be used to provide a personal digital assistant palmtop computer (PDA) with relatively secure wireless connectivity to an appropriately configured hospital local area network (LAN).

Recently the ubiquitous availability of mobile telephones has raised the question whether they can be used more intensively for health. As a consequence, mobile telephones have been used as a communication component of monitoring systems for ambulatory or home care. Another application of interest is to use mobile telephones for payment procedures replacing credit cards by the telephone own SIM (Subscriber Identification Module) card to set up a contact between an application system and a server which triggers a payment authenticated by the SIM Application Toolkit (SAT) and protected by a mobile encrypting application managed by a public key infrastructure (PKI). Mobile telephones could also access the Web by combinations of various mobile technologies such as the Wireless Application Protocol (WAP). Despite the fact that those are promising development and that a variety of mobile and portable ICT devices are being marketed, in-depth studies of advantages and drawbacks of such approaches are still lacking.

Economy of scale features depends heavily on commercial developments without which it is difficult to foresee the advantages and impact of these solutions. To come up with realistic scenarios and answers it will be necessary to research such issues for extended periods of time in different implementation environments. The issue of scale is particularly important for the health sector – it is generally believed that widespread health applications will be economically feasible only when multifunction cards that can be used by different sectors (credit, banking, driver license, etc.) are adopted.

Examples of different generations of integrated circuit data cards are shown on Figures 4 to 8. The examples shown illustrate examples of cards of different "generations" and various functionalities.
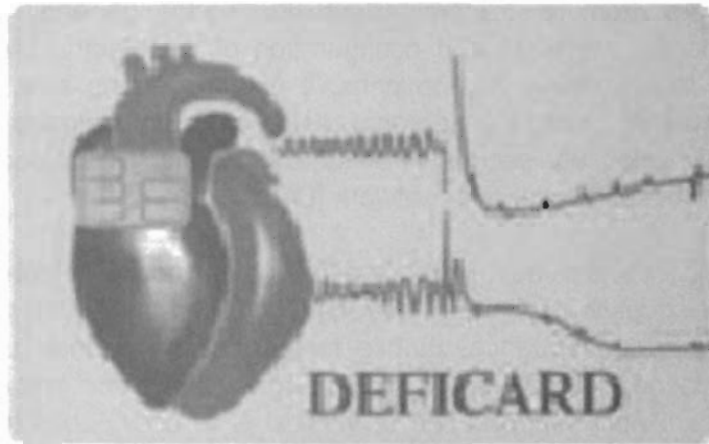
Figure 4. The DefiCard developed for patients with
implanted defibrillating devices (1993)

Figure 4 shows an example of an early successful patient smart card implemented in 1993. The "DefiCard" was developed for the approximately 70,000 patients in Germany with implanted defibrillating devices. It contained data relating to the implanted device selected as well as pre- and post-operative patient data, information on underlying illness and therapeutic interventions. This card already contained the G7-interoperability data set, a standardized set of minimal patient information, thus paving the way to future interoperable applications in an international setting.

Figure 5 depicts the first version of a health professional card following international standards in layout and content. The photo and the hologram serve security purposes. The card interfaces with ICT systems and as a regular physician identity card. Figure 6 shows the European emergency card developed in 1996 by the CARDLINK project led by a consortium of researchers in Ireland.
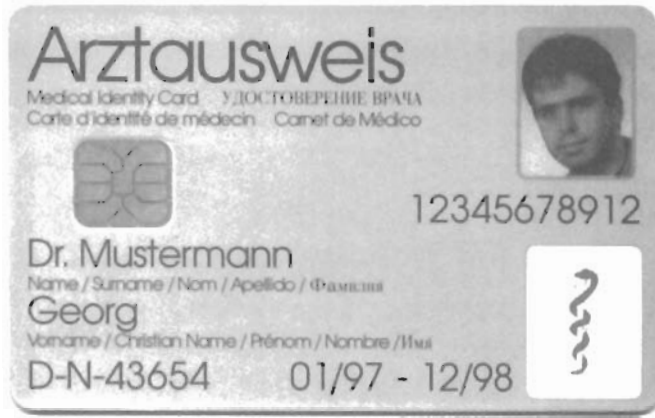
Figure 5. Early integrated circuit Health Professional Identity Card (1996)

Figure 6. European Emergency Card (CARDLINK) of 1996

Figure 7 is an example of a contactless card used by the staff card of Goettingen University Hospital in 1999. All functions are performed by radio frequency (RF) transmission. The processor and the antenna are built inside the card.

Figure 7. Contactless card of the Goettingen University Hospital (1999)

Figure 8 shows the student card of Goettingen University (2002), an example of the flexibility of modern card systems – it is a mixed technology contactless card enhanced with contacts and a separate chip for digital signatures and linkages to many campus applications. The layout is color coded and uses symbols to identify student and staff and can be worn on the coat. There is an updatable area and the back side has a barcode that links to the German library system.
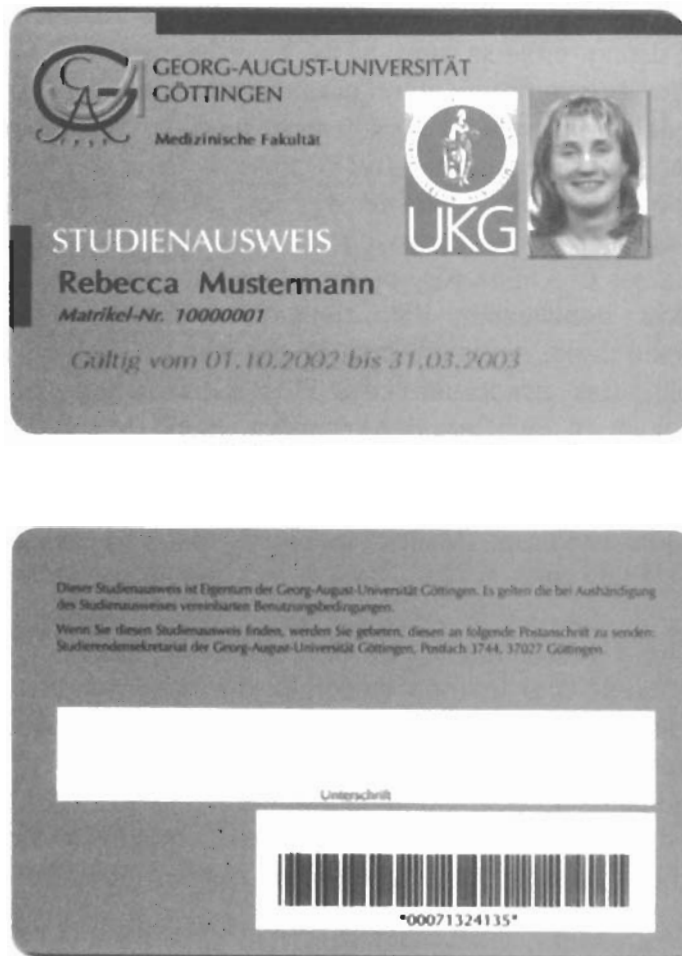
Figure 8. A mixed technology multifunction modern card systems – the student card of the Goettingen University (2002)

1.7. Technology Aspects in Existing Projects

Existing projects and pilots have shown that the technology needed for e-government smart cards is available, mature, and has had proven field experience. The cards typically used are based on proprietary operating systems with an RSA (a widely used public key encryption technology developed by RSA Data Security Inc) cryptoprocessor to allow the card to carry on digital signatures. Small memory sizes of 8 to 16 KBytes have been used allowing for the storage of general identification data, fingerprint data, compressed photo, compressed paper signature image, and two X509v3 digital certificates along with their associated keys. The reasons that prevented open systems such as JavaCard or Multos from being deployed in Europe are related to the lack of experience, questions on sustainability of the technology, the cost/features ratio, and intellectual property and fees issues. Outside Europe, Multos has been chosen by Hong-Kong for their national identity card.

There has been a lot of discussion around the necessary infrastructures. One learned lesson is the difficulty of deploying card readers and the fact that half of the users do not succeed in installing their readers without calling for support. Probably this difficulty can be minimized by using USB interface readers. The security of the readers is another much discussed issue. Secure readers have been generally chosen however they have a high cost when compared to standard readers thus presenting a barrier to entry and preventing mass deployment.

2. Data Cards in Health Practice

The proposal to abstract and record medical data on small portable wallet-size cards have been around for a long time. The idea derives from the experience with military identification tags ("dog tags"), which contain personal identification data but also the blood group of the carrier, and from the highly successful use of plastic cards or metal bracelets designed to be used by certain groups of patients suffering from life-threatening or chronic conditions and containing data on allergies, diseases (such as diabetes, epilepsy, and heart conditions), use of implanted devices (such as pacemaker, defibrillator, insulin pump, etc.), and vital medication requirements.

2.1. First Development Phase until 1995

Extensive studies were done regarding the type and level of detail of medical data that should be kept while the industry researched alternative media for data recording which quickly led to a variety of materials and formats other than embossed plastic or metal plates. The most successful of those early cards were magnetic stripe cards, due to their ubiquity and very low cost.

When the first medical emergency cards were designed, the need for a more detailed set of medical data let to innovative approaches – example of an early solution is the use of a microfilm copy of the relevant pages of the medical record attached to a paper-based health document similar in format to the small paper booklets internationally adopted for the recording of immunization. Later versions attempted to adopt the concept and physical media of the "standard" credit card and combinations of all different types of data-support media have been tried.

From the beginning, there were doubts as to whether IC card technology was the right media and hardware concept for the different perspectives and requirements of health data storage on portable

devices. Mass market products like CDs or DVDs, because of price and availability, have been promoted by some as better data storage options based on the fact that optical storage technology has been preferred by all developers who wanted to archive massive amounts of data (e.g. images). Combination devices, such as integrated circuit cards with additional optical storage media on one side of the card, were tested and researchers in Japan engineered a specific device for images (ISAC – "image save and carry"), to serve as a portable device for patients to easily transport medical images between different healthcare institutions or providers. Those media issues were never settled and, as a consequence, IC health card development has been characterized by more than 15 years of a somewhat continuous mainstream development occurring in tandem with many parallel independent developments linked to specific application ideas, data requirements, and new hardware concepts.

European projects

There is a long history of discussion in the European Parliament and European Member States, of plans and projects related to the use of smart cards in the healthcare sector. The study "A European Health Card" [4], which was commissioned by the STOA (Scientific and Technological Options Assessment Group) Program of the European Parliament documents card-related activities started as early as 1981 when the European Parliament expressed its opinion that a voluntary, unique European health card could be successfully issued only if individuals were likely to request it.

In 1983 the European Commission submitted to the Council's consideration a recommendation for adopting a multilingual paper-based emergency health card but this resolution did not take account of all the problems regarding data update and liability issues. In 1989 the European Commission wrote a report about the implementation of the Council's resolution and the conclusion was that some countries did not have in place the right implementation measures conducive to appropriate implementation while other countries, as was the case of Germany, Luxembourg, and Portugal, had them developed. The report concluded that technological improvements were needed and a program

– the Advanced Informatics in Medicine (AIM) Project was initiated to address those issues.

Several project groups in the United Kingdom, France, Italy, Germany, and other European countries attempted to use data cards for medical purposes as soon as they became available on the market [5]. In the mid-80's memory cards which could store 2 KBytes of characters as well as interface devices were generally available. Following the issuing of the first patents for microprocessor cards in France and Germany, the European Union realized that the use of such "intermittently connected devices" could offer major advantages if applied within the health communication infrastructure of the European healthcare systems [6, 7]. From 1989 onwards, a series of demonstration and evaluation projects were funded, among them the CARDLINK, DIABCARD, and EUROCARDS, the latter conceived as a European interoperable platform.

In the early nineties research groups considered patient data cards as a promising technology and started card projects, often without proper preparation. It was fashionable to use cards for medical purposes although many projects were only able to prove that their solution was "in principle" possible. Many of those projects just issued several dozens or hundreds of cards. For several years, the development focused on patient data cards and which roles they could play in interacting with existing hospital and physician's office computer systems. In addition, many research groups developed cards aimed at the insurance market to identify the beneficiary and guarantee access to services provided by the national health system. Finally, other projects tried to optimize paper and pencil methods for patient scheduling by utilization of card technology.

The results of those projects were reviewed in a conference held in 1994 in Athens, which summarized the developments of the first generation of medical data cards. A year later this report and its background papers were published by IOS Publishers, Amsterdam, in its book series "Studies in Technology and Informatics", Vol. 22 [6]. This publication is still the most comprehensive summary of the principal aspects of patient data cards for health; it contains organizational, technical, and legal aspects as they were understood in the mid-90's.

Many pioneer projects also attempted to include functionalities that allowed the storage of data from the medical record, in order to make these data available for health services anywhere they would be needed. Great potential for such medical record cards was expected, particularly in the case of tourists and mobile workers. More advanced projects, directed to patients with chronic illnesses, also included the storage of detailed treatment and medication data. Those approaches were found useful in emergency situations where information about past history and medication utilization could not be directly elicited from the patient or relatives. The European Commission identified the medical data card as a promising piece of technology and decided to systematically promote and evaluate its potential [8]. All subsequent projects build on those experiences and reports on these activities have been published in the proceedings of international conferences on health cards of Frankfurt [9] and Rotterdam [10] and by a review sponsored by the European Commission [11].

The review process had also shown that patient card systems require the implementation of a reliable security infrastructure compatible with privacy and legal demands. For the issue of security to be properly addressed, new systems being developed included health professional cards, another type of health data cards, which identified health professionals and validated their level of privilege in order to access data within medical networks.

The review and publication of experiences stimulated France and Germany to move ahead and install nationwide card systems. France was one of the first countries in the world to introduce the large-scale use of smart cards in the health insurance system. In 1993, the three major mandatory medical insurance schemes in France (wage earners, farmers, and the self-employed) created a consortium named Sesam-Vitale EIG (Economic Interest Grouping) to implement card-based solutions. The initial experiences showed that innovative engineering alone does not guarantee the success of cards systems – a broad consensus of all stakeholders is absolutely necessary to make such decentralized systems successful. The French Vitale Card system had to undergo many iterative improvements over the years and to this date, only parts of the population and health professionals use the card.

In the period 1994-1995, Germany started a large project of administrative cards to be issued to the whole population within a short timeframe. The German health insurance card (Versichertenkarte) was built around a simple memory card. Its only purpose was to reduce administrative costs within the context of the specific workflow of a healthcare system characterized by burdensome bureaucratic tasks [12]. The implementation, despite many difficulties, was highly successful and the savings on the administrative processes paid off the high initial costs in less than two years. Since then, the health insurance card has been very well received by the population, despite the fact that it is basically a fairly limited administrative card.

It is worthy of note that one element of the decision to limit the card functionalities was related to the extremely strict regulations demanded by the German data privacy commissioners and data protection groups regarding the utilization of the compulsory administrative cards which did not allow the use of the card for any other purpose [13] – a law was passed which specified the extent of data set to be captured and maintained in the card and did not permit the use the remaining bytes on the memory chip for any other purpose. Just a few months after the initial implementation a generally usable card-reader was specified but its introduction into routine use never happened.

The German population received more than 60 million cards, requiring a major organizational and technological work coordinated by a very competent national project office. The experience was a remarkable achievement but it was clear that any extension of functionality would be impossible because of the nature of the technology employed – the cards could not be adapted or have their functionality extended as it was the case with the more advanced smart cards used by the French system. The consensus for such a strategy was orchestrated by a small group of representatives of the key players in the national healthcare system. The key facilitator was Dr. Otfried P. Schaefer, one of the pioneers of medical informatics and closely linked to professional physician's organizations. The only international prize, the DROPS-Award USA, for successful work in the field of health data cards is named after him. The DROPS-Award has been awarded to Dan

Maloney of the Department of Veterans Affairs (2001) and to Peter Debold, of Debold and Lux (2003).

U.S. and Canadian projects

Around the same time, in the U.S., the BlueCross BlueShield of Maryland (now CareFirst) specified a similar card project to be implemented it in the State of Maryland. However, it was not possible to make the system work within the given environment and, in 1986, the project was moved to Canada. Like many European projects its major contribution was to provide lessons about what works and what does not in the deployment of smart card technology. The outcome of the BlueCross BlueShield of Maryland project was published at the MEDINFO Washington Conference of 1986 and discouraged other groups to follow the same path. Since then, the U.S. development of systems to provide access to clinical and administrative patient data moved away from cards and in the direction of computer networks. Only the Western Governors Association and the Veterans Affairs Administration continued to pursue the use of cards and carried it on with the Health Passport Project initiative [14, 15].

In Canada the different provinces, which are responsible for healthcare, experimented with cards and mostly decided against smart card technology. The main exception was the French-speaking province of Québec, which very closely tried to emulate the path of the developments in France and did set up several projects in close cooperation with the data protection officers within the province [16].

2.2. Developments after 1995 in Germany, France, and the United States

From 1995 to about 2000 a second generation of card systems approaches began to develop. Germany and France implemented the first comprehensive national patient card systems in the mid-90's [17]. The European projects gained so much momentum that it was possible to rapidly build up an international exchange of expertise and establish many international technical specifications. Canada, the U.S., and Japan also cooperated extensively and worked closely with ISO and CEN in the

development of global technical and operational standards. In 1996 a work area called "Harmonization of Data Cards in Healthcare" was selected as a priority domain for cooperation in the framework of the G7 initiative and the corresponding G7-CARDS Project continued the work of the EUROCARDS initiative and defined and demonstrated the interoperability of established processes at a world-wide level between European and Japanese systems.

In France, the Sesam-Vitale EIG (Economic Interest Grouping) card-based solution prompted several other health-insurance organizations to join EIG, among them all the public complementary health insurance bodies. Their common purpose is to develop a program meeting the data exchange expectations and needs of all those involved in healthcare including insured patients, health professionals, and health insurance funds.

Today's Vitale Card is a microprocessor card containing roughly 4 pages of text and replacing the standard "soft copy" individual health insurance document. The first version (Vitale 1) of the card contained administrative data, available to health professionals for reading and storage of secure electronic health care cost claim sheet during the visit. Depending on the software application and the terminal smart card reader equipment used, the "e-sheet" can be stored in programmable secure reader memory and also in the health professional computer hard disk. The claims are sent daily by secure batch mode to the Health Insurance front end servers for further automatic processing using a national health Intranet network named RSS (Réseau Santé Social). Sesam-Vitale is a highly secure dual-card system. The CPS (health professional card), a secure microprocessor card is compulsorily required for reading the patient card dataset.

The system simplifies the health care costs clearing procedure and also dramatically reduces insured patient refunding risks of delay by replacing 1 billion health care paper forms every year by electronic transactions reducing the average reimbursement time to a few days instead of the usual 4-6 weeks before card roll-out. Furthermore, the system provides health costs payment directly to health professionals by insurers and is a tool to track healthcare spending. In the future it could enable the transfer of electronic prescriptions to healthcare funds,

responsible for reimbursement. More than 64 million cards were issued. By early 2004, the Vitale Card version 1.3 will be distributed to the population.

This new card will include additional information, complementary health insurance administrative data, personal data (administrative only) and an European dataset including administrative information required either for cross-border healthcare cost reimbursement for immediate care (Form E111), programmed care (Form E112), and other resources. The second card generation (Vitale 2) - an individual health card - will include an emergency data set and possibly other medical parameters only available to health professionals using a professional health card for identification. Other medical information (e.g. patient medical history) could be stored on highly secure servers [18].

Figure 9. The French card system for the physician,
patient, and pharmacist

Perhaps the best documented application of a multifunctional smart patient data card that includes clinical information is the Santal smart health card, which is being used in the Saint-Nazaire region of France. More than 60,000 cards have been issued to almost a quarter of the population of the region. The patient card is used to store four types of information: administrative (identity, insurance, entitlements), medical

history, diagnostic, and usage of pharmaceuticals including current and previous prescriptions. The system allows secure communication between patients and healthcare professionals and enables a more comprehensive exchange of healthcare information and a simplification of administrative procedures.

In Germany, even during the implementation of the sizable administrative card system in 1994-1995 discussions began on when a second generation of the system would be necessary, with the objective of replacing the simple memory cards by advanced smart cards which would allow more intelligent functions. Although these discussions have been going on for many years it was not possible to convince the responsible decision makers and the higher management of the German healthcare system that another major investment was necessary. Politicians as well as the top management level of insurance companies and healthcare organizations agreed that a new generation of cards should be introduced only if:

- Investment could be paid off after a short period of time,

- Long-term economic effects could be confidently expected,

- Fraudulent use of the memory cards, a major problem today, would end,

- A national health professional card would be concomitantly implemented,

- Additional advantages for the patients could be guaranteed, and

- The concerns regarding data protection are met. Data protection officers were inflexible in the option that cards should not contain medical data.

Despite the fact, that Germany specified a national health professional card as early as 1996 and changed many laws accordingly, implementation processes where extremely slow. Since 1998, the unfavorable financial situation of the German healthcare system

39

changed the situation. The Christian Democrat Government had agreed during its last months in government that the infrastructure of the healthcare system required an overhaul on the basis of ICT infrastructures and the elected Social Democrat Government carried this idea forward since 1998, but was not able to bring a consensus of all parties on how such a second generation card system should be.

Nevertheless, several managerial and technical working groups carried on and linked their results with international activities. Thus, despite lack of political agreement, researchers, industry and many insurance companies in Germany are prepared for the implementation of a second generation of cards. Specifications and local test-bed implementations continued so that a second generation German system will be able to implement health professional cards on a national scale in one single "big bang" approach together with a new generation of patient cards. The German government would like to link the new card generation with the plans for a European card, as documented by the eHealth Europe Program of the European Commission. Currently (2003) the German government is preparing a law which specifies key decision points in the preparation and installation process and a first pilot roll-out of the new system is expected to take place in 2006. In the meantime an overall layout for the electronic communication functions within the German healthcare system has to be prepared and tested in detail.

Detailed specifications for emergency cards, health professional cards, administrative cards, and other components of cards systems were derived as a result of this international effort. They took off from the first versions of the mid-nineties into second and third versions five to seven years later. The resulting experience and technical specifications makes the design and implementation of present-day card technology into the overall ICT infrastructure of healthcare systems easier, more reliable, and much more cost-efficient than in the pioneering installations of a decade ago [19].

Gap between project design and state-of-the-art technology

Many of the projects implemented since 1995 still reflect the technology and interfacing solutions versions of the early 90's but important lessons have been learned. The price to be paid by

irreversible decisions and the importance of a forward view was made evident by the German Versichertenkarte experience. Soon after the launch of the German insurance card it became clear that it might have been a better idea from the beginning to introduce a smart card with built-in capability for future extensions. The lesson for later projects was that card technology for national installations, like any other innovative ICT technology, has to be planned considering longer development and implementation timeframes and not seen as a one-shot approach. An appropriate time span for national installations is about ten years. Similar lessons are true for the French systems – although they were truly pioneering in the field they revealed many design and implementation problems, functional flaws, and technical details that required attention.

Some of the problems encountered were so serious that required total redesign of previous systems. Some of these lessons took years to be understood, for instance, how administrative cards can be safeguarded against fraudulent use by persons who are not eligible to healthcare services, for instance illegal immigrants. Today both countries are in a planning process directed to overcome the drawbacks of their pioneering implementations. The changes to be introduced in current systems will require as much attention as the one needed in the initial implementations. This is another confirmation that from the moment an ICT infrastructure is widely installed in a given healthcare system constant work is required directed toward updating and new implementation cycles. All later card projects have been based on those experiences.

Biometric Identification

The question has been raised why should complex card-based identification systems be implemented when biometric identification of individuals is much easier to achieve – fingerprints, voice pattern, iris characteristics, or other biometric data is available at any point and any time and could be more generally utilized than the so called "artificial" card infrastructure. The biometric identification would replace the person identification number (PIN) which is currently used in most personal identification applications around the globe for simple access control.

Biometric identification systems have only slowly come into use in high security environments like nuclear power stations or bank vaults and they operate in high-tech environments quite different from what one would find in a generalized public sector implementation. Moreover, there are nagging technical problems even with fingerprint identification, considered to be one of the easiest ways of biometrical identification. As already indicated, fingerprint readings can be disturbed by many everyday situations and a broader usage was never possible. Biometric identification has been also perceived as intrusive and intimidating because the fact that biometric methods have been used primarily to identify criminals.

PINs, if properly protected and particularly if cross-matched to PINs of other users (e.g., providers), coupled with biometric identification have however proved to be highly secure in appropriate computer system. For instance, card systems can be used in registration processes as a preliminary transaction as a secure means to provide systems with specific access rights or qualification of the accessing person. This is followed by authentication by biometrical identification to make sure that the user of the card is indeed the legal owner of the card. In addition the process can be additionally safeguarded by printing a photo of the legal card holder on the card or by storing the corresponding digital image.

Within the card context fingerprint and iris identification are technologies that can reach a level of readiness for mass-production but there are still technical and cost problems to be overcome. As cards with biometric identification capability are much more expensive than simple smart cards, it is expected that combined cards will first be used in specific projects and in limited numbers. Although most health card systems so far implemented use identification numbers and there are no important implementations which use biometric parameters, it is expected that in the near future there will be a combination of access rights coded into cards coupled with biometric identification.

Potential of currently available cards

In the early nineties cards were extremely limited in their performance. Today all components of an IC card can be manufactured

and tailored to the specific needs of any project: the plastic body, the transmission scheme (transponder versus contacts), the type and capacity of processors in the card, the amount of storage, and the linkage of different storage and processing technologies on a single card. The same versatility applies for interfacing systems. Because card projects need high interoperability to be cost effective the issue of national and international standards for card applications and the operating systems is of paramount importance and the trend has been for IC chips to become also standardized.

The cost of cards is still substantial if cards are not used in mass applications. To reduce costs of a health sector implementation, the introduction of data cards should be linked to other wide-ranging applications such as national identification initiatives, driver's licenses, passports, credit cards, and the like. More and more projects consider combinations of very different functions on one card – a discussion in which economic and data protection aspects may clash.

The organizational and human components are critical

Experiences from the large projects in France and Germany indicate that it is essential to build a broad consensus involving all relevant players and to design a training component for all persons involved in the design, implementation, and operation of the system. The perceptions and reactions of different health professions, managers, regulators, payers, and data protection officers have a major impact on the success of a project's implementation and acceptance. Fortunately, the often heated and unproductive discussions regarding data privacy of the past have subsided and today most of the opponents have accepted that when properly deployed, integrated circuit card system works well and that many of the dangers foreseen by some privacy rights advocacy groups did not materialize. Thus it is now possible to extend the use of card technology into the clinical management of patient data without much opposition.

Ripple effect affecting other information technology applications

Another important lesson arose from the very last phase of the German card implementation. The project required that hundreds of

companies had to adapt their commercial application software for doctor's offices, hospitals, clinics, diagnostic units, etc. to the requirements and specifications of the new card interface including technical as well as functional and organizational elements.

Although the card project implementation team tried to facilitate this process by making detailed specifications available to the application programmers of all companies, many software providers underestimated the impact of the necessary changes and had difficulties to deliver adapted products on time. This effect was so massive that it nearly endangered the implementation process. It became abundantly clear that the professional orchestration of the overall change process is the key success factor for major adjustments in healthcare systems using card technology.

Development problems typical of health informatics also apply to cards

The deployment of card systems displays the same characteristics of other types of ICT implementations in the health sector:

- In most countries ICT spending in healthcare is about half of what could be expected as to be a minimal level of funding.

- Few countries have sufficient number of medical informatics specialists and healthcare managers trained in ICT management.

- Projects tend to be underfinanced and generally lack adequate professional planning, management, testing, training, maintenance, and planning for a next-generation systems migration.

- Interoperability with existing or news systems being concomitantly deployed is a major issue. Even in well-circumscribed implementation environments, e.g., a hospital or clinic, problems of interoperability between applications can easily lead to disaster. The situation is dramatically more

complex when a highly interactive ICT technology is widely deployed. The degree of detail which is necessary for a successful integration of many systems should never be underestimated. The difficulties rise proportionally to the size of the installation and with the possible numbers of systems to be interfaced.

- In well-established implementation environments with many application products of many different companies already installed, it is difficult to accomplish a detailed collaborative specification necessary for the harmonization of the new solution with existing applications. It is not uncommon that established software providers oppose the new solution as the necessary degree of changes can be life threatening to their products. This is one reason for the recent success stories of card implementations in smaller countries with a less developed ICT market and few implemented health informatics applications.

There is much to be learned from the experience with the development of imaging systems. A similar problem as the one now faced by the data card industry was encountered in the development and consolidation of the automated radiology systems. Albeit many years of successful international standardization, as for example DICOM and HL-7, standards by themselves did not lead to an complete interoperability of software products from different vendors. This situation prompted the imaging community to start the Integrated Health Enterprise (IHE) initiative, focused on the promotion of data exchanges and interoperability among different systems. An IHE-like approach still needs to be developed in the domain of patient and security data cards.

Continuity and sustainability of funding

The German and French implementations provided a good idea of the substantial costs involved in national card systems. However, the German project demonstrated also that initial costs could be recovered within two years by the savings accrued on administrative costs – the bulk of those savings were related to mailing costs of various forms used in the reimbursement and administration of payments to physicians for

45

ambulatory patient visits, necessary before the introduction of the card system. Especially in Germany, all argumentation for a second generation national smart card was restricted by limiting itself to short-term savings rather than on much more difficult to calculate long-term impacts [20].

Unfortunately, the German insurance card business case model, obsessed as it was with financial return on investment, has negatively influenced other national health card projects in three ways:

- Projects tried to make sure that a short-term amortization of implementation costs would accrue from savings in the administrative area.

- Thinking in terms of limited functions, restricted areas of application, and "big-bang" approaches prevented governments to look into the future, plan ahead for innovation, and focus on long-term change in the health sector workflow processes.

- The generalization of the erroneous concept that the build-up of ICT infrastructures in healthcare occurs by waves of massive investment instead of the more appropriate notion that ICT evolves by constant change and continuous and sustainable funding with a few peaks of higher investment in between.

Fast changing and dynamic technological environment

The history of card implementations showed that the structures of the existing healthcare systems are too static to adapt to the dynamic environment considered necessary for the implementation of advanced ICT applications, particularly the radical reengineering of workflows. There is a mistaken tendency to equate ICT to medical technology equipment (e.g. X-ray and laboratory devices), that is acquired and installed through well-defined and time-tested procedures and used for a long time, often for periods of more than a decade. The fast-changing technology cycles of ICT, the difficult implementation procedures, and

the risk of further investments after a relatively short time have discourage health managers in adopting ICT.

The security components of interoperable systems are very complex and the integration of ICT infrastructure with networks and cards leads to very dynamic environments which require constant attention, investment, and capacity to absorb change. In addition it is extremely difficult for health managers to fund capital investment and operational costs in an environment of resource restriction where an aging population and the new therapeutic and diagnostic advancements are constantly requiring more investment than the national health systems can possibly provide.

One solution is the establishment of national long-term strategies for ICT, a requirement that the World Health Organization has promoted for the past twenty years. Such strategies are, however, very difficult to define and enforce – the U.K. National Health Service is one of the few cases where it was tried, unfortunately with little success. Due to the very nature of ICT short life cycles, again and again new strategies must to be formulated, sold to the entire population, and implemented again.

The impact of the the U.S. Health Reform Initiative failure

During the Clinton Presidency an attempt was made to pass wide-ranging health reform legislation. The initiative contemplated the introduction of some short of health data card as an important component of the operational strategy of the new healthcare system. In Europe, the proposed strategy was followed with greatest interest, since a successful implementation would have led to a global upswing of the "health passport" idea. The Western Governors card implementation in a few mid-west States and a successful project of the Department of Veterans Affairs seemed to prove that the U.S. would soon join other international groups on the global standardization of health data cards.

During those years several international conferences on health data cards convened every two years. A series of research and development projects funded by the European Union[1] evaluated existing

---

[1] See annex (Websites EU-Projects)

projects, produced guidelines for implementation, harmonized architectures and data sets, and led to a very intense learning process among experts from Japan, Canada, the U.S., and many European countries. The last key activity in this context became the G-7 and later the G-8 project on health data cards that in 1998 conveyed a global conference, held in Berlin, in which the first successful interoperability field testing of cards from Europe and the US was reported.

With the legislative failure of the Clinton health reform project and its card element, and without other global projects in the horizon, the health data cards initiatives ran into a difficult period. However, the international standardization process that had started in the mid-90's continued.

The persistence of magnetic stripe cards

By the mid-90's the large credit card companies announced that they were planning to change from magnetic stripe card technology to smart card technology. This move, together with the U.S. card to be developed in the context of the Clinton Administration health reform project, was expected to push the widespread adoption of the technology. The failure of the credit card companies to follow through with those plans was the second major blow to the diffusion of IC cards. The slowing down of adoption was given a final setback by the collapse of the Internet bubble in 2001, putting on indefinite hold many projects. Only in 2003, the economic situation permitting, the credit card organizations are expected to progressively start to switch to the new technology mainly by reason of the amount of fraud currently occurring with magnetic cards that has to grown to the point that the switch is now inevitable.

By the end of the last decade all those developments led to a stagnation of the card approaches, chiefly in the pioneering countries. Due to the Europe's smart card fallout of the last few years, many observers of the U.S. health industry predict the failure of multi-function cards. Instead, it is predicted that firms would issue company-specific cards that allowed customers to access networked applications and that electronic identification would be a key functionality. Some observers got to the point of prognosticating that the idea of health cards had already

lost its fascination and that we should focus instead on networked applications.

Poor dissemination of results, lessons, and experiences

The knowledge regarding smart cards in health has mostly been published in the so-called gray literature. This can be appreciated by the great number of non-indexed sources listed in the Appendix section of this publication. Since 2000, much of the systematized knowledge is being held by large commercial providers of technical solutions and not easily accessible.

To avoid misinformation is not easy. Many reports are available in the lay press or in non-technical publications. They are usually not helpful for serious analyzes as they tend to mostly report on plans and intentions. Because many projects were funded with research and development funds, many reports are written to please the fund-giver source.

2.3. The European Community Multi-Country Perspective

One of the early decisions of the European Community was the agreement on a mechanism to reimburse costs of care incurred by citizens of a Member Country while in another Community country. Health ICT applications and card projects were expected to support and facilitate the workflow of reimbursement between the Member States and their insurance systems and make them easier and faster than the paper-based reimbursement process using the European Community Form E111.

In the beginning much attention was given to networked computerized solutions and data exchange issues. Already in early nineties patient data card promoters envisaged a European or possibly international health passport based on a multi-functional card that would ease administrative and billing procedures and, by containing key medical data, that could be used also to improve the quality of patient care. These approaches led to important decisions by the European

Parliament in Strasbourg, urging the European Commission to push the development of such cards [1, 4].

Since 2000 a card element was introduced into the redesign of the cross-border reimbursement schemes. This led to the development of a European health card publicly presented in 2002 which departed from the previous approaches developed by national patient data card initiatives. According to the Action Plan "eEurope 2005" [21], by 2005 the Member States should take advantage of additional card functionalities and, besides replacing the Form E111, new card systems should include support to medical emergency data and secure access to personal health information. The Commission will support a common approach to patient identifiers and electronic health record architecture through standardization and, if necessary, legislative action to facilitate Europe-wide use of the health card. As a demonstration of the complexity of the issues involved, during 2002, both developments and the nonspecific language used in the documents have brought in a lot of disagreement into the discussions about harmonization of European card efforts in a global context [22, 23, 24, 25, 26].

2.4. Other Noteworthy Experiences

A number of countries had shown interest in different types of health cards as stand-alone devices or as a component of network-based systems. Important contributions were made, particularly by the Nordic countries, Italy, Greece, Spain, Austria, various Canadian provinces, and some of the Eastern Europe countries, who had just come out of a painful change of their social and health systems. In the last years there has been a growing interest in health cards in Latin America.

Nordic countries

Sweden [27], Norway, and Finland have sizable areas that are sparsely populated and face similar challenges regarding the provision of health services. Besides the changing requirements consequent to health sector reform initiatives those countries were deploying a broad spectrum of telehealth applications requiring an infrastructure capable of

supporting the delivery of secure telemedicine services including the authentication of health professionals and patients.

Medical Informatics experts from those countries were responsible for several ICT security projects funded by the European Union. Two key projects called TRUSTHEALTH specified and tested card-based digital signature infrastructures and established the basis for the implementation in recent years of various health data card projects in the Nordic countries. Although not successful in achieving a general deployment, those important efforts contributed to the work of standardization committees at the international level and became the conceptual basis for most smart cards security solutions based on digital signatures. Finland recently announced it was launching a smart card-based electronic identification project known as EIDcards, issued by the Finnish Population Register (VRK), allowing holders to be positively identified over the Internet when exchanging data or using e-business applications.

Italy

Since the mid-90's, Italy has participated in international projects on smart cards in health, like the DIABCARD and the NETLINK projects. The idea to issue an electronic identity card – Carta d'Identitá Elettronica (CIE) was introduced in 1997 as part of a national effort to reform the country's public administration and a number of municipal and provincial entities. Since the end of 2000 regional administrations and institutions began working on the introduction of the CIE. Experiences gained in the NETLINK project led to the decision to make the CIE compliant with the specifications elaborated in that particular project. The first experimental phase of the CIE ended in 2001 and by that time 82 municipalities emitted about 100,000 cards. During this first phase, numerous technical and organizational problems had to be solved. From the beginning of 2002, activities have focused on the implementation of IT-based services for the citizen offered by communities and institutions on national, regional, and local levels.

The Italian government is also planning to introduce a national service card – Carta Nazionale dei Servizi (CNS) – which will allow citizens to access public services including healthcare. The CIE smart

card will contain a chip and a laser stripe, as well as digital signature keys and certificates. In order to secure interoperability between the CIE and CNS, identical structure of the microprocessor and of the software has been adopted. The bodies which deliver identification documents will distribute the CIE cards, whereas for the CNS cards a variety of different distribution channels are envisaged. Both cards will enable their holder to sign documents digitally. However, for the CIE, usage of services offered will not necessarily require a digital signature. The context of usage and the specific application will determine whether such signature is needed or not. The Italian Ministry of Interior and the Ministry of Innovation and Technologies plan to distribute 30 million CIE and CNS cards by the year 2005.

Because of their technical specifications both cards can be used in healthcare and this option is already being tested in cooperation with the Ministry of Health. The wide distribution of CIE and CNS is regarded to be an important stimulus for the establishment of ICT-based healthcare (Telesanitá) and future healthcare services for the citizens. One example of how the health smart cards will operate in the new service environment on a regional basis is the service card issued by the Lombardy Region, the Carta Regionale dei Servizi (CRS). This card is a basic component within the ICT-supported healthcare sector of that region. Cards are issued to the citizen, to service operators, and to service providers (physician, pharmacist, social workers, etc).

The functionalities of the Lombardy CRS are: the authentication of the citizen and of the service provider as well as their different access rights, keys and certificates for digital signatures, storage of administrative patient data, and prescription data. Furthermore, medical data like allergies and vaccination profile are stored to be used in case of medical emergencies. In order to upgrade its social and healthcare system the Lombardy Region has implemented a number of services for citizens as well as for institutions. Databases and information systems have been implemented to support management of administrative patient data, eligibility status for specialized medical care, prescription statistics, scheduling and booking of medical contacts, medical referrals, activities of the social and healthcare agencies, and many more. Similar efforts are being undertaken in Bolzano and Tuscany Regions.

Spain

Arguably, the most innovative use of smart cards by a government can be found in Spain, where 400,000 hybrid cards containing both an integrated circuit and a magnetic stripe, the magnetic stripe being used for compatibility with another project, have been issued to citizens in Córdoba, Montilla, and Lucena as part of a trial of a benefit-payment scheme which also incorporates fingerprint biometric identification. The Tarjeta Seguridad Social (TASS) is a multifunctional smartcard combining several government programs on one card, including pensions, unemployment and health insurance. Goals are to improve the cost– effectiveness of benefits delivery and to curb fraud in the welfare system.

The card is used to identify the holder and enable access to services and payment of benefits. The card does not hold a great deal of personal information but does act as a series of personal keys that enable card holders to access government databases. The provision of fingerprint is optional, but the Spanish government decided to limit access to general information and refuse access to personal information to those people who were unwilling to provide a fingerprint. Fingerprints are stored only on the card itself and not on a central database. Over the next few years, Spain plans to implement 3,000 self-service kiosks and over 20,000 networked PCs for health management in all health centers. When totally deployed almost 40 million cards will be issued and they will be used in 6,000 centers.

In a second phase, clinical data will be captured, following the recommendations of the European Commission and the decisions of the Barcelona European Commission Summit of March 2002. The card is compatible with the adopted European standards and users will be able to use it in other Member States to receive medical care. Such advanced clinical functions including Internet-based booking are already being used by a smart card solution being deployed by the Cantabrian Health Service (Servicio Cántabro de Salud).

Austria

About 43 million treatment and health insurance certificates are issued every year in Austria. This system is now being replaced by an integrated networked solution based on the social insurance microprocessor card, the "e-Card". The broad scope of this project includes 8 million digital signature compliant smart cards, eighteen thousand card reading devices, the introduction of an extensive computer network, and the establishment of a call center and support services covering all aspects of the project. Initially only administrative data will be stored on the card but patient's medical data (emergency data) on a voluntary basis will be stored in the near future. Starting in 2003, 8 million insured and their relatives will be equipped with e-Cards and 12,000 physicians and hospitals with terminals. This is the largest organizational and technical project of the Austrian Social Security [18].

Czech Republic

A system similar to the French Santal smart health card is being piloted in the Litomercie region of the Czech Republic. The system allows secure communication between patients and healthcare professionals and enables a more comprehensive exchange of healthcare information and a simplification of administrative procedures. About 10,000 citizens will be issued PIN-protected patient data cards. The card is being tested because the paper-based system held limited information that was frequently inaccurate, labor-intensive to update, and widely open to abuse. The Czech Government also hopes that the card will rationalize the current system, where multiple insurers issue cards to patients. If the trial is successful it is likely that the Czech Government will rollout 10 million cards by the end of next year.

Taiwan

The project in Taiwan includes nearly all possible functions of patient card systems. The National Health Insurance IC Card is one of the major projects of the Taiwan e-Government Initiative. The Bureau of National Health Insurance (BNHI) launched the project on a trial basis in Penghu in July of 1995. According to statistics compiled by BNHI, the average satisfaction rate was above 90% in each of the past five years.

In light of such a high positive response, the BNHI has held many expert workshops in related fields to collect constructive opinions for the implementation of the card project throughout the rest of Taiwan. About 7.6 million cards have been issued and about 5,000 of the 18,000 health facilities are ready to upgrade their information systems and link to the BNHI Data Center. It is hoped that the project, when completed, will help decrease the large national social and medical costs. The usage of IC Cards is expected to generate a large marketplace for electronic commerce and its application. It is expected that the National Health Insurance IC Card will completely replace the current paper card by the end of 2003.

Portugal

A smart card identification document has been designed to electronically deliver a range of government services to over five million citizens and is being launched in 2003. Certipor, a consortium of Portuguese businesses, will issue digital certificates as the country's National Certification Authority on behalf of the Imprensa Nacional, the Portuguese National Mint, which will establish the infrastructure to support the government's electronic services initiatives. Each citizen will receive a smart card with identification information to be used for voting, health services, library access, and educational activities. The Portuguese tax authority also introduced smart card technology to simplify tax payments and reduce the volume of paperwork. The project involves the Portuguese Inter-bank Consortium, which signed a contract with Bull for a first delivery of 100,000 microprocessor cards.

Netherlands

The Healthcare Card project ("the Eemland pilot") was established by the initiative of the national umbrella organizations of care consumers, care providers, care insurers, and the Netherlands Ministry of Health. The trial was conducted in the district of Eemland (Amersfoort and surrounding area) and started in May 2001 and ran for one year. The results of the trial were encouraging. Support for the use of a safe network in which messages could be exchanged electronically appeared to be considerable and the care providers stated that although the network operated rather slowly and the possibilities were limited, they

55

wished to proceed further with electronic communication. The largest care insurers in the district stated that the network contributed to an improvement of insurance data and that the trial revealed the necessity for far-reaching standardization of data.

After the evaluation trial the network has been used since September 2002 for other applications, such as an electronic letters of referral from general practitioners to specialists. The network in Eemland has continued in a modified form, giving more emphasis to mutual communication between care providers. Already in September 2002, a test has been started with general practitioners and specialists at the Meander Medisch Centrum, formerly known as the Ziekenhuis Eemland and Medisch Centrum Molendael. General practitioners are now able to send a letter of referral to the specialist electronically, instead of giving it to the patient, to read the feed-back letter of the specialist in the same way, view laboratory results, and call up radiology reports. The Healthcare Card, originally used only for checking insurance entitlement, is not necessary for communication between care providers. There are alternatives available for enabling care providers to check the insurance entitlement of their patients electronically without use of a Card. For this reason, the use of the card as proof of entitlement was cancelled on September 2002.

In recent years much work has been done on the development of a smart card for Parkinson patients, incorporating biometric identification. The background for development of such a card is that people with chronic illness often receive treatment from more than one physician or therapist. The "Parkinson Pass" is used to access an Electronic Medical Record (EMR) that provides a practical, quick and easy access to clinical data. The access is exclusive to the patients and their care providers. Without one of the two keys there can be no access to the data stored in the card. The Parkinson Pass contains both a built-in memory chip and a processor chip, the former linked to a sensor for biometric identification (fingerprint). Information from the medical record which is stored on the card is only made available if the fingerprint corresponds to the one registered on the card. In addition, smart cards are also issued to all care providers. Only if both cards are used simultaneously can data from the card be made accessible [18].

Netlink

NETLINK was a project funded by the European Commission that ran from July 1998 to November 2000. The project developed concepts and technology to pave the way for implementation of interoperable data card systems and Internet/Intranet solutions, before nationwide use in the healthcare sector. In order to support healthcare services to the fullest extent, a secure health passport based on card technology was designed. In the field of health care systems interoperability, NETLINK developed specifications for common solutions, particularly in security architecture, networks, health professional cards, and patient data cards. The feasibility and economic viability of these integrated solutions was demonstrated in several implemented pilot sites.

Countries participating in the NETLINK consortium (France, Germany, Italy and the Canadian Province of Quebec) had already set up nationwide information systems in the healthcare sector. The NETLINK implementations were to be based on the use of modern technologies: smart cards used by health professionals and patients; networked health professionals, hospitals and health insurance funds; and trusted third parties for security and authentication purposes. The objective was to make these new nationwide information systems interoperable for the benefit of (a) patients by supporting continuity of care, enhancement of quality of care, and simplification of administrative procedures; (b) health practitioners by facilitation of communication, continuity of care, and simplification of administrative procedures; and (c) health insurance funds by facilitation of communication and simplification of administrative procedures.

The NETLINK project produced and maintained the NETLINK "Requirements for Interoperability" specification and promoted it to the G8 countries and other nations involved in implementing health card solutions. Several pilot sites were implemented to assure the feasibility and the economical viability of the solution. A guideline for the development of future projects compliant with the NETLINK specifications was produced and an evaluation methodology was developed, assuring the certification of reliability and interoperability of future card projects following the NETLINK requirements [18].

Cards and international organizations

The World Health Organization (WHO), particularly through its Regional Offices for the Americas (Pan American Health Organization), Europe, and for the Western Pacific have early and intensively addressed health informatics issues and promoted studies for development of appropriate ICT technology. For WHO and other international organizations like the International Telecommunication Union (ITU), telemedicine functionalities have been a major focus of the last years. However, international organizations have been careful in not promoting specific types of technology and rather remained on a general level of recommendations regarding implementations. The same is true for the European Community, which is cautiously addressing a broad range of healthcare aspects and questions of how ICT must be introduced to support national healthcare systems [22]. Most of those recommendations do not address specific technological solutions, e.g. cards, by the reason is that the documents produced by international organizations are mostly directed to policy and decision makers and not formulated to specific technical tools to achieve the objectives of a health policy.

3. Key Issues Related to Patient Data Cards

Physicians always wanted to record and store as much patient history details as possible. This stance is related to the yearning for reducing uncertainty in the clinical decision-making process – more data very often provides more confidence in reaching the right answers. In addition, medical investigation requires large data sets to support comparative or statistically valid conclusions.

The major shortcoming of the traditional patient medical history is that it is recorded in paper as hand-written observations and diagnostic data and stored at the different points where a patient had contacts with the medical care system. The distributed storage of paper records has the attending problem of how to access, or better yet, integrate a patient's clinical observations made over a period of time by different professionals at different sites.

3.1. Storing and Recovering Medical Data

Data cards have been proposed and indeed used to address, at least partially, the problems of storage and recovery of clinical data just mentioned. As cards have limited storage capacity, approaches have been devised and tested to structure medical content and to condense the usually massive amounts of individual patient data into the limited storage on patient cards – the option of using cards as data carriers. Other solutions used cards as a key to access individual patient data electronically stored in local or remote server computers databases that are logically integrated, even if physically distributed – the option of using cards as pointers to data stored elsewhere.

One particularly attractive idea is to use patient data cards for different purposes: administrative data for service access, emergency data to treat acute episodes, and as a source of pointers to medical files that would remain stored in hospitals, doctors' offices, and other medical units where care was or is being provided to a particular patient. This

59

concept of having detailed patient data stored in a decentralized manner and using a networked systems allowing secure concurrent access from anywhere at anytime has gained momentum in the last decade. The "card as pointer" idea is, however, infinitely more difficult to implement than just recording a minimum set of medical data on a IC card memory with the hope that this very limited medical history would be adequate for the great variety of clinical requirements of practice.

Cards as data carriers

Implementation of cards as data carriers can be rapidly accomplished and be successful if the overall system has been set up the right way. This is facilitated by the general acceptance of carry-on personal documentation – for several generations most Western societies have been taught to handle documents and passports for various purposes: personal identification, driving vehicles, emergency, insurance, military service, etc. In addition, Western countries are familiar with credit cards. In military organizations and among specific groups of individuals (e.g., persons with diabetes, epilepsy, pacemakers, life-threatening allergies, etc), analog cards have been in widespread use to document important emergency medical data.

The idea to have an emergency data set recorded on patient cards is not new. Around 1995, during the development of the G-8 card project it was decided that emergency data on cards should not only contain risk information but also relevant data for health professionals to be able to deal with medical emergencies. Civil service agencies and search-and-rescue personnel around the world are trained to look for such information carried by the patient as bracelets, "dog tags", wallet cards, etc.

It is of great advantage for health data cards acceptance that such functions can be either directly mapped onto health data cards by printing key information in analog format (printed or embossed text) on the card and also by digitally recording relevant medical data into the card electronic memory for use by health professionals. It will definitely take many years before network systems can reach the level of credibility and acceptability which cards already have.

Patients can benefit from carrying a portable device that points to places where data is legally held. Emergency data on health cards should allow a health professional to interpret symptoms and signs presented by the patient even in the absence of specific diagnostic resources (e.g., in plane or ships). The specification for an international emergency data set is in its final phase of specification and is expected to be available by the end of 2003.

Cards as a navigation tool in networked data systems

New diagnostic and therapeutic procedures and interventions such as functional imaging studies and molecular medicine will result in massive amounts of data that must be stored in the individual medical record. The increasing amount of clinical data will make medical decision processes even more complex.

When one looks over a patient's lifetime and with the growing utilization of imaging and laboratory diagnostic procedures it becomes evident that alongside with the issue of fast growing volume of patient-related clinical data, it is extremely important to provide health professionals with resources that allow them to browse and selectively navigate through these decentralized data elements in chronological, source, and problem orientation modes. Facing this situation health professionals need more clarity of what is available and at which data quality level, in the poorly structured and unsorted way in which such decentralized data is stored, maintained, and retrieved [28, 29, 30].

The idea of pointer cards has been developed in several projects in many countries and options are being tested on how to best aggregate patient data which resides in several physical sites over a long period of time. Medical data cards of this type may well form highly integrated healthcare environments, a 4th generation of cards, to be launched between 2005 and 2010 (Figure 10).
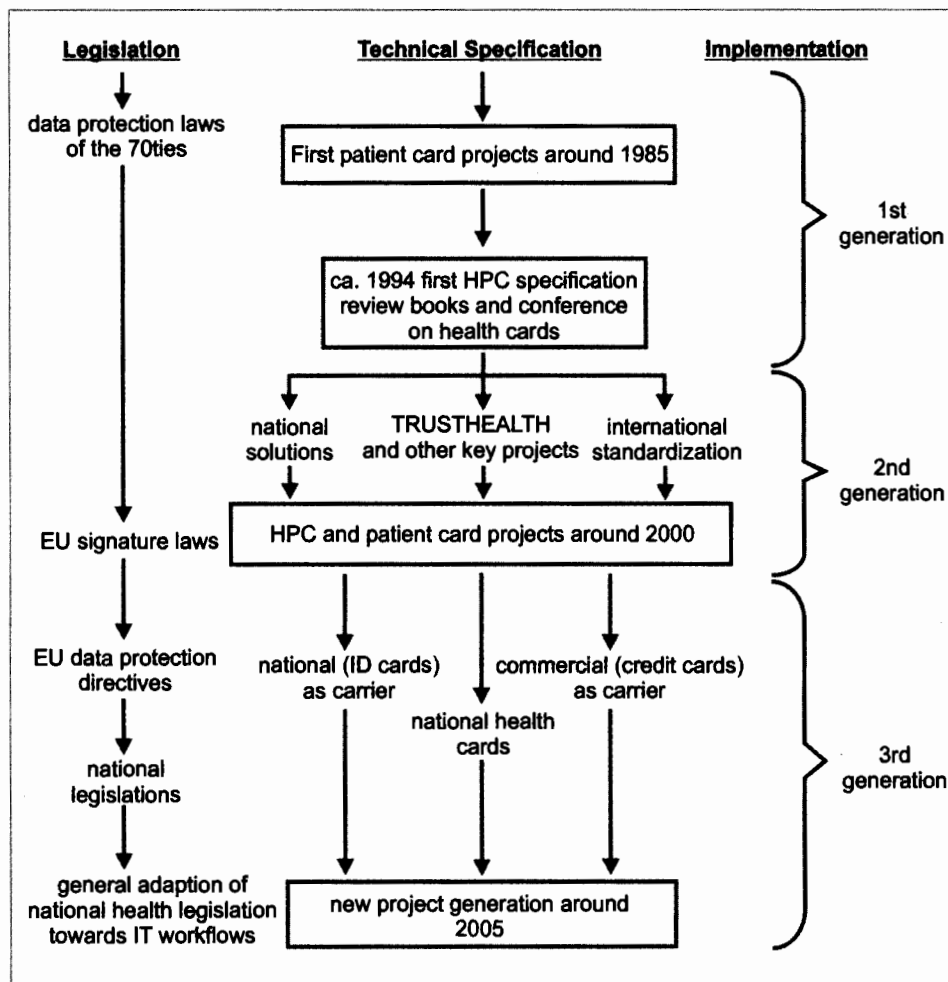
Fig 10. Schematic representation of 15 years of health data card development. Initially, pure patient data cards dominated. In the 2nd generation health professional cards and patient data cards were combined with networks to achieve secure implementation. The 3rd generation is now on its way using cards for patients and professionals that integrate into other public or private services from governments and private provider organizations.

Imaging technology and cards

Patient data cards have also been used for the communication of digital images specifically x-ray images. This application has been the most controversial as images usually need much more memory space than smart cards can offer. Therefore specific combinations of optical storage on smart cards have been proposed. Another option is to store the images with a reduced resolution, just to give the recipient a general idea of the image. Both approaches did not prove to be adequate to the requirements of clinical practice. Physicians and payers want to have access to all images of a study and also would not accept low-resolution representations of high-resolution images. In the case of medical imaging technology, networks proved to be much more efficient in communicating images than cards.

A somewhat middle ground approach regarding images can be found in cardiology – the most common interface between cardiology picture archiving and communication systems is currently a CD format. In Japan, a similar approach has been tried by suppliers of radiological equipment and for several years they have been promoting the "image safe and carry" standard, a method to store medical images on CD-ROMs. Presently, it looks very probable that digital images will be transported through networks and that cards will contain links to such image sources or at a maximum only a few relevant images of key importance for a specific treatment program.

As more diagnostic images are produced doctors must have means to identify and directly access the relatively small number of relevant images from each study. The imaging issue must be dealt with in close collaboration with the evolving radiological information systems and picture archiving and communication systems (RIS/PACS) that are rapidly developing new ways of presenting relevant extracts for specific purposes out of the massive amount of data which the imaging modalities produce. This process will very likely will lead to results helpful for the overall architecture of health communication systems and which will be also helpful for the discussion of what has to go on cards, what should be communicated by networked solutions, and what should remain as "raw data" archived in the imaging departments.

It may well be that the further growing amount of image data in healthcare and the technical availability of mass storage and broadband communication technology may together reach a "tipping point", where it becomes absolutely clear that conventional data processing tools in healthcare are obsolete. The theory of tipping point suggests that massive changes in systems only occur if several factors influencing the development combine in such a way that suddenly a new development is possible and will generally occur. Tipping point theory explains why mobile phones suddenly became ubiquitous despite the fact that mobile phones have been in the market for many years before they became a widely distributed commodity [31].

Authentication and signatures

In the mid-90's it became clear that health professionals and patients would require a solution to allow the digital signature of electronic documents. There are initiatives directed to the introduction of civil service cards which contain a digital signature which could be used for many purposes including healthcare and more modern concepts of credit cards have followed a similar path. Currently it seems clear that all citizens must be provided with digital signatures. Whether the patient health cards may be one carrier of such signatures is still open to discussion. The experience of Sweden shows that it is possible to use national solutions for digital signature within the health sector without the necessity to build a specific public key infrastructure for healthcare [27].

Prescriptions

It is possible to use cards as carriers for prescriptions and this has been done in Germany and Taiwan. Cost-benefit calculations in Germany compared costs and savings between moving prescriptions to cards or moving prescriptions through networks with comparable results. PCU Italia, Finsiel and the Italian Healthcare Ministry are cooperating on an international healthcare project involving Italy, Germany, France and Canada. The cards include 32KByte EPROM Java Smart Cards and cryptocards. They will store personal data, emergency data and other significant health data and, in the future, will be used for storing

prescriptions. The Italian Healthcare Ministry forecasts a national roll-out involving more than 50 million cards and 200,000 terminals by 2003.

Transnational reimbursement

Several project such as NETLINK and TESS (TESS/SOSENET Telematics for Social Security/Social Security Network, an IDA Program of the European Commission) have been analyzing and testing options regarding transnational billing for health services. Currently it appears that health IC data cards will be the preferred carrier of such application. However, current solutions need consolidation.

3.2.   Cards versus Networks

In the mid-90's, at the beginning of the controversy between those that favored cards and others that preferred network solutions, networks were quickly expanding and cards had just become a feasible option. Today, networks and cards are commodity elements of the mass market segments of the ICT industry. The bandwidth of networks is growing so quickly that – as long as they are continuously financed – there is no limit for their carrying capacity. The variability of cards is also nearly unlimited, making them an easily customized component of ICT infrastructures.

The availability of these technologies in different geographical, political, and economic regions is quite different and often depends on national strategies for economic development. Illustrative example is the cases of Estonia that, like Finland, has promoted Internet access with the result that about 40% of the adult population uses the resource. Meanwhile, the neighboring Baltic countries, with different priorities, have much lower Internet usage rates. Another example is the widespread card usage in Germany and France introduced partly to promote the national technology industrial base.

Arguments comparing cards and networks as they relate to the handling of patient data have, however, remained the same during the last 15 years, as described in Table 1, where differences and similarities of pure network-based and pure card-based solutions for making ICT

65

systems interoperable are detailed. It can be said that both approaches have appeal and can be combined. Cards improve the security of network solutions, can offer functions when networks are not available, and can serve as carrier for other information and data formats (e.g. barcode).

Table 1. Comparison Between Network- and Card-based solutions

Criteria	Network	Data Card
Bandwidth	Variable, if necessary very high	Not applicable, see storage
Availability	Advanced telecommunications	Minimal infrastructure except for card readers or
Passport functions	Not possible	Easy to realize
Storage capacity	Unlimited	Limited
Prerequisites necessary	Network access, network card in computer	Card reader or terminal
Application programs	Must be adapted	Must be adapted
Costs of access	Medium	Low
Costs of infrastructure	Very high	Low
Flexibility of functions	Very high	Limited to card layout
Security	Needs specific attention, if not low	Needs specific attention, easier to achieve
Efficiency in health application	Depends on concrete solution in a defined	Depends on concrete solution in a defined

It is assumed, as already indicated, that card services are better accepted by the population of Western countries than pure network services. The general agreement is to use cards for organization purposes, urgent information, and for situations without networks availability and conversely use networks to access and communicate massive data volume (e.g., images) or accessing geographically distributed databases.

Cards are linked to other information systems applications

It is essential for any card project to analyze the technical aspects of the implementation environment as they relate to functionalities, workflow, and to economic and regulatory aspects. Card infrastructures are directly related to other key components of health information systems, namely the architecture of the electronic patient record, workflows in disease management, computerized physician order entry, transaction processing, and web services. All of these elements are interoperable in the limits of interface standards and agreed workflow at the organizational level. However, without global or national interoperability solutions it will be most difficult to interconnect such "deployment islands" with a broader regional or national system.

In the European context projects like PROREC or SYNAPSIS have developed architectures which guarantee such interoperability. PROREC (PROmotion Strategy for a European Healthcare RECord) is a European Union project managed by Sadiel of Spain and probably the most up to date approach to derive a common architecture for the European healthcare market. SYNAPSIS (1996-1998), another European Union project managed by the Trinity College of Dublin, formulated the structure of a "federated electronic patient record" which provided important insights regarding pointer cards. So far, it has been very difficult to develop national health systems to such high interoperability level and large countries with heterogeneous health infrastructures seem to have more difficulties than smaller countries to evolve from traditional workflows to a comprehensive ICT-supported integrated healthcare system. Likewise, health maintenance organizations (HMOs) or occupational health plans in large organizations offer easier conditions and clearer benefits for the implementation of card systems.

67

4. Health Professional Cards

The idea of providing cards for the care professionals (health professional card or HPC) is nearly as old as the concepts of patient data cards. Health professional cards are designed to identify and authenticate healthcare professionals in an electronic network or in the context of smart card utilization. They serve two purposes: to indicate who is the professional accessing the patient card and associated database, to specify which level of access is authorized, and the role that the professional has. The concept of health professional cards follows the practice, in use for decades in many countries, of issuing a physician's identity card by professional accreditation authorities.

In the last five years implementation of electronic health professional card solutions on a broader scale have been tried in several countries. These projects had major difficulties and often were restricted to the scope of pilot implementations. The reasoning is that it is impossible to finance a public key secure transaction infrastructure for the healthcare sector alone and it is necessary to engage all the business and social sectors into electronic communication before it becomes practical in setting up a public key infrastructure for health. With this in mind, several countries in Northern Europe have started to build a national public key infrastructure to be used by national identity card projects. The upgrading of the national electronic infrastructure from paper and pencil signatures to electronic signatures will eventually allow the healthcare sector to make use of this complex technology.

A further problem is related to the variety of regulatory and licensing principles in different countries. A study conducted in Europe revealed that except for physicians and pharmacists all other health professionals have substantially different training, job description, and legal status in each country. Within the national context different organizations are responsible for the registration and licensing and they are expected to maintain updated records on the registered professionals.
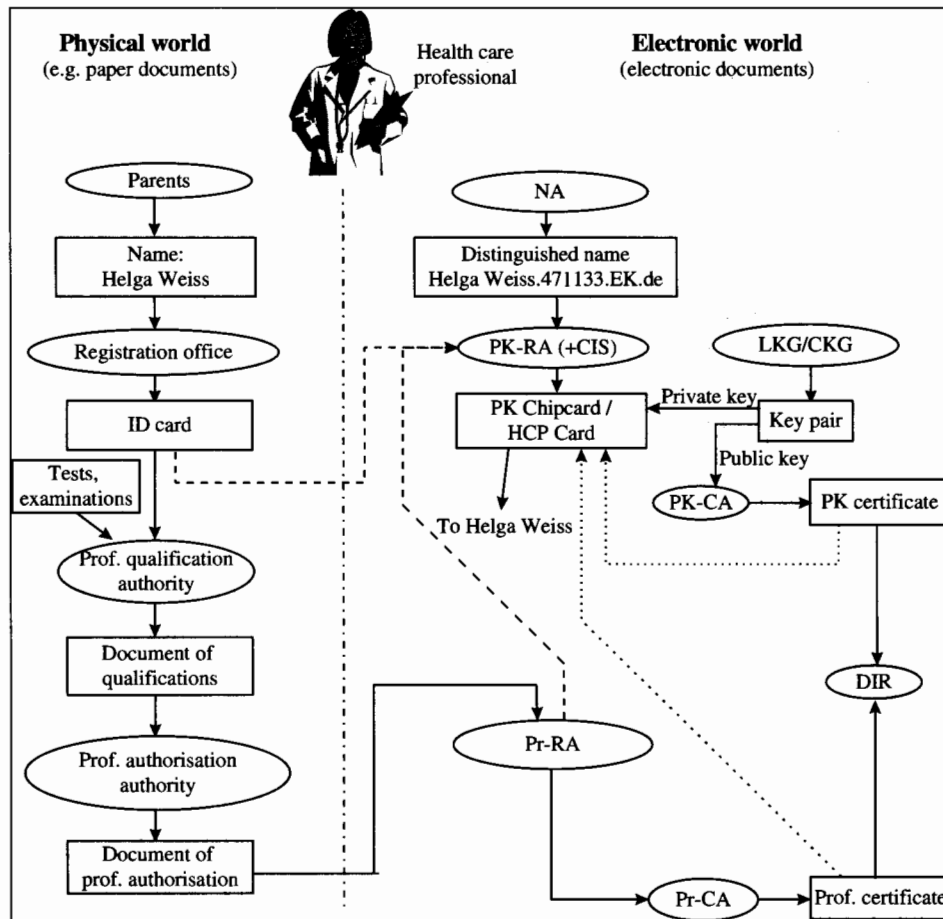
Figure 11. Traditional and electronic ways of describing the status
and identity of a health professional (Wenzlaff et al., modified)

Pr-RA: Professional Registration Authority
LKG/CKG: Local or Central Key-generation Facility
NA: Naming Authority
PK-CA: Public Key Certification Authority
DIR: Directories (storing public key certificates or
professional certificates)
Pr-CA: Professional Certification Authority
CIS: Card Issuing Office

Studies in Germany showed that although the physician's associations responsible for professional certification and licensing maintained reliable records they were not prepared to assume the role of a certification authority in an automatic electronic world. One of the first countries that addressed this aspect is Italy which started to establish or harmonize certification authorities for all relevant health professions.

Nearly ten years of research into this issue and into the field of public key infrastructure have demonstrated that to implement an electronic system for physician identification is not easily accomplished (Figure 11) and it becomes even more complex if one wants to apply such a health professional card in a cross-border international context. Moreover, the design of appropriate a security infrastructure to provide a digital signature to the physician based on smart card technology makes the whole approach technically very complex.

5. Organizational Requirements

5.1. General Issues

Patient identification

Studies have shown that secure mass communication of medical data can only be made with appropriate patient identification. Ideally patient identification should be accomplished by a numeric identifier that will uniquely link to all data sets associated to an individual person. A personal unique identifier is the most critical element to be maintained uniformly in an information system. Without a universal unique identifier or a set of data items that can consistently generate a unique identifier, it will be impossible to link data across the myriad of healthcare locations and data storage arrangements.

There are many options regarding the generation of identification numbers and once implemented they ideally should be assigned to individuals at birth. Potential problems in the assignment of unique identifiers include legal and illegal non-citizens and persons who wish to hide their identity as well as the need to have a parallel system to assign and track dummy numbers to individuals that do not have a *bona fide* identification number. Legal limitations may be a barrier to the deployment of unique identifiers – countries like Germany and the Netherlands do not allow the establishment of single national identifiers and this certainly create problems to card system developers.

Whichever identifier generation system is chosen, attention must be paid to which sets of personal data will be permitted access and for what purposes. Development of a unique identifier does not necessarily mean that the individual is always "identifiable" to users. There is a general recognition of the vital importance of maintaining confidentiality and when possible any public use of a unique identifier should be in an encrypted form. The unique identifier must be developed and protected in such a way that the public is assured that their privacy will be protected.

73

Consensus, culture, support, and training

Many card projects have shown that improved communication in healthcare, whether it is based on cards or networks require a broad consensus of all stakeholders. It is not possible to deploy communication project in institutions, professional groups, and with patients that are not willing to use the resources, abide by the established workflows, and cooperate in the operation of implemented solutions. All stakeholders, the civil society, providers, payers, and regulators have to become familiar with the new approach and have to agree on and trust the methodology employed. Consensus building and extensive training of different user groups are fundamental for successful implementation and utilization. Many project failures can be ascribed to overemphasis on technical aspects and lack of understanding and actions directed to the organizational and human component aspects of the implementations.

Card issuing organizations, certification authorities

Several organizations are needed in the deployment and operation of IC card systems. For patient cards it is necessary to have a card issuing organization to handle the delivery and recall of cards, the management of defective cards, and other administrative action. If one looks into the more complex issue of health professional cards, to shape a trusted network additional levels of certification authorities are necessary. For a full-fledged system it is necessary to build up several institutions capable of providing the functions and support for effective and reliable operation.

Even after nearly two decades of experience, some of the preconditions required for deployment need much time to define, design, develop, and implement. This is especially true for non-technical issues like legislation and consensus of all relevant parties. New projects must carefully review the lessons learned in earlier projects to avoid repeating fatal errors and build on proven experiences (Figure 12). It is likely that about 30 percent of project work and time will have to be spent on setting up an appropriate organization even for small projects with up to a couple of a hundred thousand of cards [20].

74
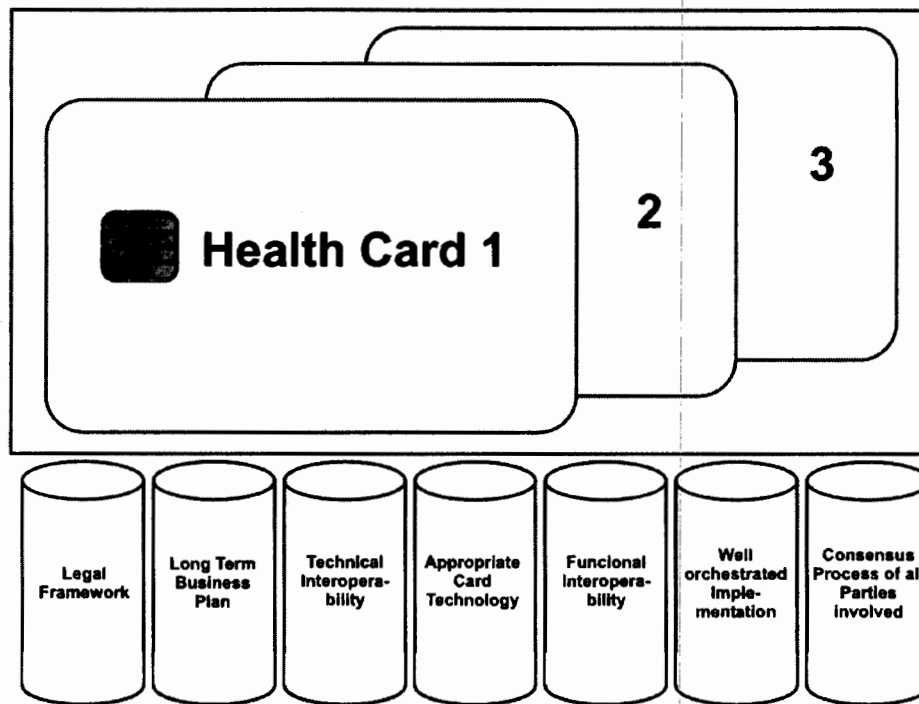
Figure 12. Health card applications are based on preconditions
without which implementation becomes risky

Card management and backup

It is expected that patients will lose or mislay their cards and will
ask for replacement – from the start the problem of issuing a copy of the
lost card (backup) has to be solved. Backup solutions involve
organizational as well as technical aspects. The backup routine will be
easier if highly standardized data sets and a well-defined operation
routine are used. Conversely, the backup question becomes very difficult
if the recorded medical data is unstructured or when many institutions
write data on the card. Difficulties in recovering medical data and issuing
backup cards are reasons used by those who argue that only emergency
data and pointers to detailed data residing in servers should be stored

on a medical card. The backup problem of medical data illustrates how deeply the data card is linked to the environment where it is used.

Timeliness and completeness of health data

It is of fundamental importance for decision making that health professionals accessing medical data recorded in a patient data card have an indication of the chronology of the information and how recently it was updated. The proper timing of information is linked to data relevance, particularly when dealing with diagnostic tests and medications – if the physician does not trust the recorded data his tendency is to repeat diagnostic procedures or request medical records filed in other sites with resulting delays and unnecessary repeated tests. It is extremely important that the system guarantees that the data is recorded in a timely and complete fashion.

Economy of scale

A review of projects implemented during the past fifteen years indicates that large projects involving major changes in workflows and practice are as successful as very limited projects that have minimal interactivity with the general clinical practice environment. An example of such limited but successful projects is the card system carried by patients with an implanted defibrillator – in this case the card is akin to an analog emergency card extended with technical details about implanted instruments and thus does not need to change other application systems except those ones which read a relatively simple data set.

Risky approaches seem to be somewhere in between. Failed projects often do not have enough impact to force the environment to adapt to the communication approaches of the card system and usually are too small to be cost-effective and have a limited impact on the existing paper and pencil routines or on the electronic infrastructure. As the health sector tends to be very conservative in the adoption of information systems and technology, national card systems are sometimes seen as an initial step into more efficient use of ICT. However, a complex and large card system implementation requires significant investment, wide consensus among stakeholders, and

76

compulsory utilization to avoid long delays, loss of momentum, and inefficient solutions.

5.2. The Business Case for Smart Cards

For many years cards were just another technological tool in the history of health informatics. Early projects assumed that the implementation of health cards would primarily result in long-term improvement in patient care. For a number of reasons, among which difficulties regarding achieving consensus related to clinical specifications and concerns about privacy and data protection, the direction taken by many pioneer projects was to focus on administrative and logistic issues.

The introduction of the German insurance card, essentially an administrative tool, established that cards could improve the economics of medical care – just the savings in mailing costs in two years paid for the 500 Million German Marks of implementation costs. Although economically successful, this rather limited project provided five lessons for the design of future projects:

- One should pursue the latest technology available.

- Savings depend on working out the details of national healthcare workflow involving administrative and clinical functionalities.

- Successful implementation requires major validation and streamlining of administrative and logistic activities.

- Card projects that consider only administrative functionalities produce limited changes on the national health information and telecommunication technologies infrastructure.

- Changes are difficult to achieve in the dynamic infrastructure of healthcare if projects address only administrative functions.

A much discussed issue is the price of the smart card technology. In 2002, the price of a card chip was around 2 euros, which is very low compared to the overall cost of the project. The total cost of the manufactured card, including the above mentioned price of the chip, but also the cost of the secure plastic card body and the general issuing costs is considered to account for less than 10% of the costs for large projects.

During the studies for the second generation of the German health card initiative, expected to be fully operational by 2006, again economic considerations were central. The new systems is expected to cost about 550 Million Euros and it is expected that within five years 3 Billion Euros could be saved despite annual operational costs of about 120-150 Million Euros. This positive outlook, however, depends on the need to reengineer the poorly organized German care system. The main savings will come out of the introduction of electronic prescriptions regardless whether the card carries the data or will be used as a pointer to a server. A breakdown of development expenses indicates that 44% of the investment costs will go to telecommunication and public key infrastructures needed for the deployment of health professional cards and 33% to the card technology itself [20].

Investment, operating costs, and savings involve different players. Physicians, health organizations, and pharmacies have the largest investments and operating costs, but only enjoy marginal savings of less than 2% on their investment. Health insurance companies, on the other hand, invest about 20% less but their annual savings represent a return of 180% on their investment. The model – from a political viewpoint – only has a real future if transfer payments are used to reduce the asymmetrical allocation of burdens and benefits to socially acceptable levels. The expected general economic benefits of the German initiative possibly will not be realized without reaching a consensus among the health insurance companies and health professionals about the responsibilities for the operating costs – those that correspond to business benefits must be proportionately assumed by the business sector and not transferred to other beneficiaries that collect only marginal returns.

Besides the purely economic aspects it must be emphasized that the patient is also one of the beneficiaries, primarily by enhanced medication quality and the reduction of related risks, but also from the fact that patients are given a valid instrument for communicating within the healthcare system. Evidence from studies conducted in different countries, particularly in the U.S., have shown that medical error and related costs can be reduced by the use of computerized physician order entry system. Decision makers have to think about card project deployment not only on in terms of economic return on investment but also as social impact and value added for the users [32].

Table 2. Examples of Implementation Strategies in
Health Card Projects

Type	Main Objective	Example
1	Health functions as part of HMO, institutional, and municipal approach or specific disease groups	Quebec, Canada Rimouski, Canada Diabetes: European Union's Diabcard
2	Regional service improvement as model for national strategies	Lombardy, Italy Andalusia, Spain Schleswig-Holstein, Germany Western Governors Association, USA
3	Nationally coordinated approach focused on improvement of health cards functionalities	France, Germany, Taiwan, Slovenia
4	Nationally coordinated approach focused on secure communication	Nordic countries
5	Health passports as functional extension of identity cards	Italy, Sweden
6	Cards as basis for cross-border payment schemes or as institutional emerging passports	Netlink Project, European Union Health Passport, European Union Cardlink Project, European Union
7	Health functions as extension of credit card systems	In development

In Table 2 are presented different implementation strategies for health cards. Type 1 projects have been numerous but resulted in many failures, Type 2 initiatives have been less frequent but more successful, Type 3 to 7 projects are much more difficult to establish but have more chances to be successful on a national level.

Overcoming unrealistic expectations

Any application, based on a new technology, is known to go through the "hype" cycle. First, the applications gain early interest, where specialists begin to understand the benefit it could bring. Then, as more people get involved in the development, enthusiasm grows and generates unrealistic expectations. As a consequence of this second phase a third and often long phase of disillusionment sets in. As the application continues to be developed on solid basis, the productivity phase comes in and here mass deployment occurs and the technology becomes part of mainstream operations.

Today, e-government applications are in the unrealistic expectations phase, where we would like to see state of the art technologies doing anything possible for e-government and we tend to forget the vision that ICT is a support function that primarily must address citizens, businesses, and governance needs. In order to go as fast as possible to the productivity phase, a pragmatic approach should be adopted. The use of smart cards should be promoted in a limited number of highly visible environments, a minimum set of interoperability should be defined, and consistent user experience should be preserved. These factors are vital for the success of smart card based e-government [32].

6.   Regulatory and Legal Aspects of Patient Cards

The emergence of health databanks to support electronic health records, health data cards, networked and decision support application, and health e-commerce has raised serious data security and privacy concerns. There is growing consensus that the creation, maintenance, and operation of databases containing individual patient data must be subject to regulations [33, 34, 35, 36].

In the early days of health card projects many data protection officers were afraid that card technology would produce major privacy breaches and there were many concerns regarding patient data safety [13]. The technology and the interfacing techniques with the surrounding ICT environment were considered to be not save enough for sensible patient data. In addition, data protection officers were afraid that patient cards could lead to the following dangerous situations for patients:

- Insurance companies or employers could ask citizens to show their patient cards as a prerequisite for any change of insurance or employment.

- Patients could be attracted by illegal approaches to buy their data from their cards without being able to judge about possible future damages and risks.

- Medical data aggregated on one card could be much more sensitive than current systems because presently it is difficult to access patient data as it is safeguarded by different institutions.

6.1.   Data Protection

In many countries, proposals and actual reform of the laws have been introduced according to which individuals are entitled to know what information is stored, who accessed a particular database containing

person-identifiable information, what use was made of the particular set of data accessed, and what mechanisms are available to correct erroneous information. The purpose of these regulations is to guarantee that medical data are used in a secure and ethical manner ensuring optimum medical care and services that fully respects the data subject's dignity and rights [37, 38, 39].

Safeguarding patient rights

Data protection pervades all aspects of medical practice and cards are not a special issue of the data protection problem. The objective is how to make sure that the overall handling of patient data in all ICT systems and applications can be safeguarded against abuse or manipulation. Health database regulations and standards being proposed or implemented contain provisions on:

- Specific purpose(s);

- Finality of purpose;

- Categories of information recorded;

- Body or person for and by whom the database is established and operated;

- Who is competent to decide which categories of data should be processed;

- Person(s) in charge of the day-to-day operation;

- Person(s) in charge of privacy maintenance and ethical utilization;

- Categories of persons who are entitled to cause data to be placed in storage, modified, and erased ("originators of the data");

82

- Person(s) or body to whom certain decisions must be submitted for approval, supervision of use, and to whom appeal may be made in the event of dispute;

- Categories of persons who have access to the data bank in the course of their work and the categories of data to which they are entitled to have access;

- Disclosure of information to third parties;

- Disclosure of information to the individuals concerned ("data subjects");

- Rights of data subjects to have errors corrected or data segments removed from their record;

- Long-term conservation of data; procedure concerning requests for use of data for purpose other than those for which they have been collected;

- Mechanisms for physical security of data and installations; and

- Whether and on which conditions the linkage with other data banks is permitted.

It is recognized that the strict application of rules based on some of the above provisions may cause difficulties to clinical practice, lead to poor individual patient care, and paradoxically even be responsible for unethical situations, e.g., creating barriers for a professional to assess data related to a patient under his/her care.

Record ownership

Patient data cards have been understood by patient rights organizations as an empowerment tool by putting the medical record physically into the patient's hand. Such positions were praised as a major step ahead to allow patients to govern the utilization of their personal data. Entitlement could extend not only to access to data but

include the right to change data and the control of what data could be accessed by a given healthcare organization or professional. The discussions on this matter so far has led to the assumption that on the long run health professionals and patients will have to agree on what data from the life-long medical record should be made available in each instance for specific administrative or treatment purposes by a contracted professional or organization.

A very sensitive legal issue is the question of who owns the card and who owns the data. Cards are usually owned by the organizations which issue them. This is necessary to keep control over the many card-supported processes and to prevent irregular use. However, due to data protection rights in most Western countries the data on the card belongs to the patient. This double-ownership may create problems when the card is used by more than one organization and access and retrieval of stored medical data may be the cause of conflicts of interest when patients change card holding organizations, for instance medical care groups or insurance companies.

Standardization and data security

The design of information and telecommunication systems and network technology influences which personal health data are collected, stored, and maintained and who should or could have access to them. One main effect of the development of such technologies is the globalization of standards and procedures, which may be used, for example, in the determination of protocols for diagnosis and treatment. Standards and protocols can serve as tools for good practice [40] and constitute an important component of quality assurance.

The collection of standardized data and the use of such protocols require that the practitioner/patient interaction must be structured according to a pre-set format. Standards are not neutral – they embody the ethical, social, economic, political, and epistemological choices of their creators and will necessarily favor or reject particular views of patients, diseases, and how private patient data is shared [34]. The cultural understanding of privacy and data protection is different between countries, as exemplified by the conflicts between countries regarding access to and dissemination of person-identified data. Still today the

84

right of the patient to see his own data is very differently coded in the legal systems of Western countries. Thus the data protection issue has not disappeared but has moved from a highly politicized debate to a more technical and legal study.

Many nations share concerns about the impact of the expansion of electronic networks on information privacy. How to deal with privacy issues of cross-border data flows has been a major issue between the European Union and the United States. Those conflicting perspectives are expected to expand to other countries due to globalized commerce and more and more countries, health organizations, and insurers becoming electronically integrated. A comprehensive review from an international perspective on the technical, regulatory, and legal aspects of data protection and privacy in the use of electronic health information was published by the Pan American Health Organization [41].

Fraud

The experience with the German administrative card system points to a high level of fraudulent utilization. As the card allows easy access to the free services of the healthcare system without proof of the correct identity of the card holder the cards have been traded in the black market opening the system for many illegal immigrants who use the services. Another aspect was increased demand of specialist services – before the introduction of the card system direct access to secondary level ambulatory services remained very limited because a request by a primary care physician was required. Since the introduction of the card the primary care gatekeeper was abolished and patients can directly approach different specialists and many patients visit several doctors in a row ("doctor hopping").

The fraudulent use of cards and doctor hopping are the key arguments that led to the proposal to replace the German administrative card by a new smart card system which, hopefully, will prevent abuse. The resulting increased costs for the healthcare system illustrates the importance of giving careful consideration to the organizational and regulatory aspects before embarking in projects that require reengineering of workflows and routines in a very short timeframe.

85

6.2. Ethical Issues

During the initial implementations of patient health data cards the ethical issue of cards being perceived as a "human analogue" was raised. The issues are not specifically related to cards and concern the fear that intelligent arrangement of medical data in digital systems, could expand so much as to provide such a comprehensive source of information that health professionals would focus on the "data case" instead on the real patient. Some have raised the issue whether condensed information for patient cards could eventually negatively impact the professional-client relationship.

After several years of discussion, recently the International Medical Informatics Association (IMIA) issued ethical guidelines for health information systems. They may serve as other papers, e.g. from the International Federation of Information Processing (IFIP) as guidelines for systems implementations.

There has been much argumentation regarding the issue of volunteer or compulsory utilization of data cards. In October 1981 the European Parliament expressed the opinion that cards should only be issued on a voluntary basis and only to individuals that formally requested them. If implemented on a volunteer model the patient could decide on whether to present his card to a health professional or not and it would allow him to tell an insurance company or an employer that he does not own a health data card. On the other hand, broad deployment, rationalization and quality improvement in healthcare, and effective use of the technology can only be expected from information systems using cards or networks on a compulsory basis.

Glossary

This glossary contains definitions from the much more extensive EUROCARDS volume of 1995 [6]. The definition of the smart card is cited partially from the European Commission DG Information Society's Telemedicine Glossary, 4th Edition, Brussels 2002. The list was compiled to explain important terms in the context of health cards. It can be used as a first check list for defining card applications.

ASYMMETRIC ENCRYPTION ALGORITHM: Mathematical procedure which requires for encryption a secret key and for decryption a public key which need not be secret but is known to everybody (therefore "public"). The use of an asymmetric algorithm avoids the problem of distributing secret keys to the receivers of messages as is the case with symmetric algorithms.

CARD ACCESS DEVICE (CAD): A logical and/or physical device capable of communicating with a patient data card (PDC).

CARD DISTRIBUTION: The process of delivering a card to the card holder.

CARD EXPIRY: A predetermined ending of the period of use or validity of a card.

CARD INITIALIZATION: Preparation of new cards for their application. Preparation and checking of memory areas, protected memory areas, etc. Initialization is usually done by the card manufacturer.

CARD OPERATING SYSTEM (COS): Smart Card Operating System (SCOS), the operating system implemented on a microprocessor-based integrated circuit card.

87

CARD PERSONALIZATION: Establishes the link between a particular data card and the respective card holder. In a wider sense it refers to the process or processes carried out after card manufacture and before card distribution. These may comprise card initialization and initial data entry and formatting. Part of these processes may be the recording of card serial numbers, setting or establishing security features such as a Personal Identification Number (PIN) code, writing visible data to the card (e.g. printing, engraving or embossing, writing initial data on the computer-readable card medium, etc.

CARD REPLACEMENT: The manufacture, preparation, and distribution of cards to users whose cards are full, have expired, failed, have been lost or if visible data on the card changes.

CARD SYSTEM: Any information system using data cards irrespective of the card technology used.

CARD SYSTEM ARCHITECTURE: The basic functional and structural setup of a card system, including the roles of the card holders that determine where and how the cards are being used as portable data storage devices or intermittently connected devices.

CARD SYSTEM USER: A person who uses one or more card system.

CARD USE: Handling the card for card reading, card writing, data modification, card updating, card copy, and deletion operations. A card is usually used by the card holder or somebody entrusted by the card holder to do so, e.g. healthcare personnel.

CRYPTO CENTER (Trust Center): Service provider which produces the keys and algorithms to be implemented on health cards and handles the key management necessary during the operation of a health card system.

DIGITAL CERTIFICATE: A public key directory entry that has been signed or validated by a certification authority. Digital certificates are used to verify digital signatures.

DIGITAL SIGNATURE: Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of that a data packet to prove the origin, i.e. authenticity, and the integrity of the data unit. It protects against forgery, even by the recipient himself (ISO 7498-2).

ELECTRONIC SIGNATURE: An electronic equivalent of a handwritten signature on a paper document. It protects data Integrity and provides authentication of the signing person/entity. In the context of health cards, digital signatures are generally considered for use as electronic signatures. In this case an asymmetric algorithm is used to encrypt a message with a private key. This signature is added to the message itself. The receiver decrypts the signature using the public key of the sender. Then the receiver is able to compare whether the result of decryption is identical to the text sent and hence whether the text is authentic.

EMBOSSED CARD: A card on which some data is present as raised characters that can be copied onto pressure sensitive paper.

INTEGRATED CIRCUIT (IC) CARD (or chip-card): A data card containing a single or several integrated circuits used to store data and perform specific functions.

IC MEMORY CARD (OR MEMORY CARD): An integrated circuit card without a processor.

IC PROCESSOR CARD (OR PROCESSOR CARD): Cards that have an embedded processing unit.

INTERMITTENTLY CONNECTED DEVICE (ICD): A portable technical device storing information in a computer readable form which supports data interchange and does not depend on the originator of the information when passing on the information. Usually an ICD will be physically connected to another device only during data exchange.

MAGNETIC STRIPE CARD:
- ISO STANDARD MAGNETIC STRIPE CARD: Data card with a single magnetic stripe on which data is formatted in conformance with EN 27811-2.
- NON-ISO MAGNETIC STRIPE CARD: Data card containing magnetic stripes in other locations or with data formatted in other ways.

MEDICAL NICHE: A particular disease or group of patients (e.g. patients with pacemakers, epileptics, diabetics, hemophiliacs, dialysis, etc.).

NAMING: Specification and certification of the qualifications and rights, in particular access rights, of a specific card holder which are to be documented on the card. Naming can be done by a person or organization legally entitled to do so.

NAMING AUTHORITY: Person or organization legally entitled to state, specify, and certify the qualifications and rights (in particular access rights) of a card holder which are to be documented on the card.

NETWORK: In a wider sense, several computers, digital systems, telecommunications equipment and lines, information systems, or any combination thereof linked to each other by communication pathways permitting data transmission. In a narrower sense, a network can be defined as a specific set of communication services along with the hardware and software necessary to provide these services. In this case the network itself is to be distinguished from the terminals or computer systems of the end users.

OPTICAL CARD (laser card): Data cards on which data is stored in a form that can be read and written by scanning the card surface with a laser beam.

PATIENT CARD SYSTEM (PCS): A system that uses patient data cards (PDCs) and comprising all the components required for the implementation, use, and support of a defined set of PDC functions within the geographical or organizational boundaries defined by the customer of a PCS management organization.

PCS SERVICE PROVIDER: An organization that provides a service or product required to support a PCS. These services include the card manufacturing, card personalization, issuing, card updating and card withdrawal, the development of other hardware and software, the provision of services such as training, help-desks for troubleshooting and promotion of use of the PCS.

PDC: Patient data card

PDC HOLDER (or card holder): The patient whose data is recorded on the card.

PDC ISSUER (Trust Center): A PCS service provider which may be an organization or group of organizations responsible for issuing PDCs. A single organization may be identified by more than one issuer identification if they issue cards for several purposes (e.g. PDCs and healthcare professional cards).

PDC OWNER (or card owner): The person or organization who owns the physical PDC.

PERSONALIZATION CENTER (Trust Center): Service provider which implements the security features on each health card as well as the permanent data of the card holder and his rights and qualifications as specified by the naming authority. It includes the implementation of workstations for health cards and their physical or virtual interconnections that conforms the architecture of a health card system. This architecture must be defined according to the functional requirements of the card system. It comprises the communication links necessary for data exchange and management: health cards to workstations, workstations to workstations, workstations to host computers. These links do not depend on the media used..

TRUST CENTER: Service provider which provides the services of a crypto center, personalization center, card issuer, trusted third party, or any combination of these in a high security environment.

TRUSTED THIRD PARTY: An organization or person entrusted with providing a security service, which is independent of two or more parties. It has a more limited role than a trust center, as the term "Trusted Third Party" emphasizes the mediating role between communication partners.

References

[1]   eEurope Smart Cards (2002). *Smart Cards Evolution in the Health Area – A Requirements Survey*. TrailBlazer 11 Health White Paper v.0.55 (July 2002)

[2]   Allied Business Intelligence Inc (2002). *Biometric Systems: Worldwide Deployment, Market Drivers, and Major Players*. ABI, Oyster Bay, New York

[3]   Tabar, P (2003). *Biometrics*. Healthcare Informatics February 2003: 46-47

[4]   Chambers G [Editor] (2001). *A European Health Card – Final Study*. European Parliament, DG for Research, Directorate A, STOA Unit. Reference PE 296.701/Fin.St., Luxemburg, (March 2001)

[5]   Rey JC and Frischknecht B (2001). *Zur Opportunität der Einführung einer Gesundheits-Chipkarte in der Schweiz. Aktualisierung der Studie "Un carnet de santé en Suisse: étude d'opportunité"*. Institut de santé et d'économie – ISE, Prilly

[6]   Pernice A, Doare H, Rienhoff O [Editors] (1995). *Healthcare Card Systems – EUROCARDS Concerted Action Results and Recommendations*. Studies in Health Technology and Informatics, Vol. 22, IOS Press, Amsterdam

[7]   Pernice A, Doare H, Rienhoff O [Editors] (1995). *The Potential for Healthcare Cards in Europe: EUROCARDS Concerted Action on Patient Data Cards*. European Commission, DG XIII-C4, Brussels

[8]   EUROCARDS Working Group 6 (1995). *Evaluation Methodology for Systems Applying Data Cards in Health Care. Final Deliverable*. European Commission, DG XIII-Health Telematics (AIM)

[9]   Köhler CO, Rienhoff O, Schaefer OP [Editors] (1995). *Health Cards 95*. Studies in Health Technology and Informatics, Vol. 26, IOS Press, Amsterdam

[10]   Van den Broek L and Sikkel AJ [Editors] (1997). *Health Cards 97*. Studies in Health Technology and Informatics, Vol. 49, IOS Press, Amsterdam

[11]   European Commission (1996). *Health Datacards Harmonisation and Interoperability: A Review of European and G-7 Initiatives.* DG XIII-Health Telematics (AIM). Brussels

[12]   PraxisComputer 2'95 (1995). *Chipkartenprojekte: Der grosse Aufbruch.* Deutscher Ärzteverlag, Köln

[13]   Konferenz der Datenschutzbeauftragten (1995). *Entschliessung: Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen.* 5. Konferenz der Datenschutzbeauftragten des Bundes und der Länder. 9./10. November 1995, Bremerhaven

[14]   Western Governors Association (1995). *Western Governors Association Health Passport Project. Executive Summary. Phase 1: Feasibility Study and Technical Design.* Denver (June 1995)

[15]   Western Governors Association (2001). *The Health Passport Project: Assessment and Recommendations. Executive Summary,* The Urban Institute Washington, DC and MAXIMUS Rockville, MD (December 2001)

[16]   Régie de l'Assurance-Maladie du Quebec (1996). *Évaluation du Projet Québécois d'Experimentation de la Carte Santé à Microprocesseur. Rapport Final.* ISBN 2 9803225 5 5

[17]   Forum Info 2000 (1998). *Telematikanwendungen im Gesundheitswesen. Arbeitsgruppenbericht AG 7.* May 1998, Bonn

[18]   eEurope Smart Cards (2002). *Smart Cards as Enabling Technology for Future-Proof Healthcare: A Requirements Survey.* Trailblazer 11Health White Paper, OSCIE Volume 1 Part 4 (15 November 2002).

[19]   German Federal Ministry of Economics and Technology (1999). *Global Healthcare Applications (GHAP).* In: Towards a Global Information Society – Final Report on the G-8 Global Information Society Pilot Projects. Press and PR Office, June 1999 Bonn

[20]   Debold P (2001). *Communications Platform in Health Care: Cost Benefit Analysis. New Health Insurance Card and Electronic Prescription.* Debold & Lux GmbH

[21]   European Commission (2002). *eEurope 2005: An Information Society for All.* Action Plan May 2002. DG Information Society, Luxembourg

[22]   European Commission (2001). *Healthcare Telematics Projects – Final Report*. DG Information Society, Brussels

[23]   European Commission (2001). *Building Consensus on Smart Cards*. In: IST 2001 - Technologies Serving People. DG Information Society, Luxembourg

[24]   European Commission (2002). *Information Society Technologies*. 2003-2004 Work Programme. DG Information Society, Brussels

[25]   European Commission (2002). *Maintaining Leadership in Smart Cards*. In: IST 2002 - Partnership for the Future. DG Information Society, Luxembourg

[26]   European Commission (2002). *Health Telematics Policy Working Group of the High Level Committee on Health: Final Report*. Directorate G – Public Health, Luxembourg

[27]   Ribbegard G (2002). *Swedish Experience in Secure Health Telematics Applications*. The Swedish Agency for Public Management. Internal Report, 2002

[28]   Pan American Health Organization (1999). *Setting Up Healthcare Services Information Systems: A Guide for Requirement Analysis, Application Specification, and Procurement*. Essential Drugs and Technology Program, Division of Health Systems and Services Development. PAHO/WHO, Washington, DC; ISBN 92 75 12266 0

[29]   Rodrigues RJ (2000). *Telemedicine and the transformation of healthcare practice in the information age*. In: Speakers' Book of the International Telecommunication Union (ITU) Telecom Americas 2000; Telecom Development Symposium, Session TDS.2; Rio de Janeiro, April 10-15, 2000, pages 91-105

[30]   Institute of Medicine (2001). *Crossing the Quality Chasm: A New Health System for the 21st Century*. Committee on Quality of Health Care in America, Institute of Medicine. National Academy Press, Washington, DC; ISBN 0 309 07280 8

[31]   Gladwell, M (2000). *The Tipping Point*. Little, Brown and Company, Boston, USA

95

[32]   eEurope Smart Cards (2002). Open Smart Card Infrastructure for
         Europe. eGovernment white paper on smart card applications and
         evolution. Part 1: Analysis of developments .Draft TB 10 white paper,
         OSCIE Volume 1 Part 1-1 (15 Nov 2002)

[33]   U.S. Department of Health and Human Services (1999). *Proposed
         Standards for Privacy of Individually Identifiable Health Information*.
         Document can be found online at the site:
         http://aspe.hhs.gov/admnsimp/pvcsumm.htm

[34]   European Commission Group on Ethics in Science and New
         Technologies (1999*). Ethical Issues of Healthcare in the Information
         Society*. Report # 13, Prof. Ina Wagner (Rapporteur) July 30, 1999

[35]   IITF (1995). *Privacy and the NII: Safeguarding Telecommunications-
         Related Personal Information*. Report of the Information Infrastructure
         Task Force (IITF). National Telecommunications and Information
         Agency, U.S. Department of Commerce, Washington, DC, October

[36]   Institute of Medicine (1994). *Health data in the Information Age: Use,
         Disclosure, and Privacy*. Donaldson MD and. Lohr KN (Editors.).
         Washington, DC, National Academy Press

[37]   European Union (1995). *Directive 95/46/EC of the European Parliament
         and of the Council of 24 October 1995 on the protection of individuals
         with regard to the processing of personal data and on the free
         movement of such data*.

[38]   Walker P (1998). *Status of Data Protection in the United Kingdom*.
         Document can be found online at the site: http://www.ehto.org/

[39]   Laske C (1996). *Legal issues in medical informatics: a bird's eye view*.
         In: Barber B, Treacher A, Louwerse K (Editors). *Towards Security in
         Medical Informatics: Legal and Ethical Aspects*. ISO Press, Oxford

[40]   Rodrigues RJ (2000). *Information systems: the key to evidence-based
         health practice*. Bull World Health Org 78(11): 1344-1351

[41]   Rodrigues RJ, Wilson P, Schanz SJ (2001). *The Regulation of Privacy
         and Data Protection in the Use of Electronic Health Information: An
         International Perspective and Reference Source on Regulatory and
         Legal Issues Related to Person-Identifiable Health Databases*. Pan
         American Health Organization, Washington DC, 217 p. ISBN 92 75
         12385 3

Web Resources

- Associazione Nazionale Comuni Italiani – ANCI:
  http://www.anci.it/cie

- Autorità per l'Informatica nella Pubblica Amministrazione:
  http://www.aipa.it

- Bürgerkarte:
  http://www.buergerkarte.at

- Carta Regionale dei Servizi – Lombardia:
  http://www.crs.lombardia.it/

- Carte Santé Québec:
  http://www.ramq.gouv.qc.ca/crc/reg/doss.shtml

- Carte SIS:
  http://ksz-bcss.fgov.be/fr/carteSIS/sis_home.htm

- Carnet de Santé:
  http://www.hospvd.ch/public/ise/carte_sante/index.htm

- Comité Européen de Normalisation – CEN:
  http://www.cenorm.be

- eCard:
  http://www.e-card.co.at/

- EC Projects on Smart Cards Compendium:
  ftp://ftp.cordis.lu/pub/ist/docs/cpa5compendium-final-april02.pdf

- eEurope Smart Card Charter:
  http://eeurope-smartcards.org/

97

- Elektronische Gesundheitskarte:
  http://www.bundesregierung.de/Themen-A-Z/Gesundheit-und-
  Soziales-7209/Arzneimittel-und-Gesundheitspa.htm

- EHTEL – European Health Telematics Association:
  http://www.ehtel.org

- EU IST-Website:
  http://www.cordis.lu/ist/ka2/smartcards.html

- EU Projects:
  Eurocards: http://www.ehto.org/aim/volume2/eurocards.html
  Diabcard 3: http://www-mi.gsf.de/diabcard
  Cardlink 2: http://www.ehto.org/ht_projects/html/dynamic/19.html
  Diabcare Q-net: http://www.diabcare.de
  Netlink: : http://www.sesam-vitale.fr/html/projets/netlink/index.htm
  Trusthealth: http://www.ramit.be/trusthealth/deliver.html
  TrusthealthII: http://www.ehto.be/projects/trusthealth
  Healthplans: http://www.ehto.be/ht_projects/htm/dynamic/58.html
  G-8-Cards: http://www.va.gov/card
  Synapses: www.cs.tcd.ie/synapses/public/
  Siren:
  http://www.ogc.be/hometelecare/hometelenet/articles/eua1005.ht
  ml
  ProRec: http://www.sadiel.es/europa/prorec/
  Meditrav: http://www.cordis.lu/ist
  Mobi-Dev: http://www.mobi-dev.arakne.it/
  Reshen: http://www.biomed.ntua.gr/reshen
  Transcards: http://www.sesam-
  vitale.fr/html/projets/transcards/tcd_historique_eng.htm
  Netcards: http://www.sesam-
  vitale.fr/html/projets/netcards/Netcards_2002_09_05_fr.pdf
  Setic: http://www.iaik.tugraz.at/research/
  Combiceps: http://www.diffuse.org/FP5.html#COMBICEPS
  Fingercard: http://www.infineon.com
  Usb-Crypt: http://www.usb-crypt.org
  Verificard – http://www.verificard.com
  Sabrina: http://www.cordis.lu/ist
  Smart-USB: http://www.cordis.lu/ist

- Gesundheitscard International:
  http://www.aok-rheinland.de/service/modellprojekte/euregio.pdf

- Health Care Professions' Protocol:
  http://www.hcp-protokoll.de

- Health Card Vital:
  http://www.sesam-vitale.fr/

- Health Insurance Card Slovenia:
  http://www.debold-lux.com/

- Health Professional Card – CPS:
  http://www.gip-cps.fr/intro/SYS_cadres.htm

- Integrating the Health Enterprise – IHE:
  www.rsna.org/IHE/ihe_index.html

- Institut de santé et d'économie – ISE:
  http://www.hospvd.ch/public/ise/carte_sante/index.htm

- International Medical Informatics Association – IMIA:
  http://www.imia.org

- International Federation of Information Processing - IFIP:
  http://www.ifip.org

- International Organization for Standardization - ISO:
  http://www.iso.org/iso/en/ISOOnline.frontpage

- Italian Ministry for Innovation and Technology:
  http://innovazione.ov.it/ita/egovenment/infrastrutture/cns_cie.sht
  ml

- International Telecommunication Union:
  http://www.itu.int/home/index.html

- Netlink:
  http://www.sesam-vitale.fr/html/projets/netlink/index.htm

- Régie de l'Assurance Maladie du Québec (CA):
  http://www.ramq.gouv.qc.ca/crc/reg/doss.shtml

- Sanacard:
  http://www.euler-institute.ch/SanaDeu.html

- Social Security Card of Finland:
  http://www.makropilotti.fi

- TESS Program:
  http://www.ministerosalute.it/assistenza/resources/documenti/Tess-B5-prean-2000.pdf

- United States Department of Veterans Affairs:
  http://www.va.gov/card

- Western Governors Association:
  http://www.westgov.org/wga/initiatives/hpp/default.htm

- ZorgPas Groep:
  http://www.zorgpas.nl/zp

About the Principal Author

Otto Rienhoff is a physician and Full Professor of Medical Informatics at Goettingen University in Germany. He is the Director of the Medical Informatics Department and Head of the Hospital Computer Center, a servicing unit for the whole university.

His experience with IC cards date back to the mid-80's when at the Marburg University. There, in collaboration with I.Suenkeler, a first approach for an application for hemophiliacs was programmed and tested. Since then Prof. Rienhoff has been part of several research and development projects of the European Community and of the G-8 countries. In 1995, together with A. Pernice and H. Doare he published a pioneer book on health card issues as a result of one of the European Union projects. Another publication followed as a result of the First International Health Cards Conference in Frankfurt. In those years the G-8 activities led to a revised understanding of the different roles of patient and professional cards and especially of emergency cards. Those works contributed to several subsequent standardization activities which are still ongoing.

Since the mid-90's Prof. Rienhoff focused his work on the question of how to establish security infrastructures based on the concept of health professional cards. Together with the physicians organizations in Germany this approach has been used for several years. Currently he is the Chairperson of a coordination committee of German research networks and at the same time actively engaged in the establishment of a national information and telecommunication infrastructure for the German health system. Both approaches use cards as one key component within their corresponding architectures.

Prof. Rienhoff was President of the International Medical Informatics Association from 1995 to 1998 and in 1997 he co-chaired the first telemedicine conference of the World Health Organization. Besides many other affiliations he is an international associate (fellow) of the American Medical Informatics Association.