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

PAHO Library Cataloguing-in-Publication

Rienhoff, Otto
Integrated Circuit Health Data Cards (Smart Cards): A Primer for Health Professionals
Washington, D.C.: PAHO, © 2003. 102 pages

ISBN 92 75 12463 9

I. Title II. Rodrigues, Roberto J. III. Piccolo, Ursula
IV. Hernandez, Antonio V. Oliveri, Nora

1. MEDICAL INFORMATICS
2. INFORMATION SYSTEMS
3. AUTOMATIC DATA PROCESSING
4. INFORMATION STORAGE AND RETRIEVAL
5. HEALTH PERSONNEL

NLM WA26.5.R557i

ISBN 92 75 12463 9

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

The authors wish to express their appreciation to the following professionals that collaborated in the preparation of this publication

S.Y. Chang

P. Debold

H. Doaré

U. Sax

J. Sembritzki

P. Wenzlaff

S. Dessi

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.

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).

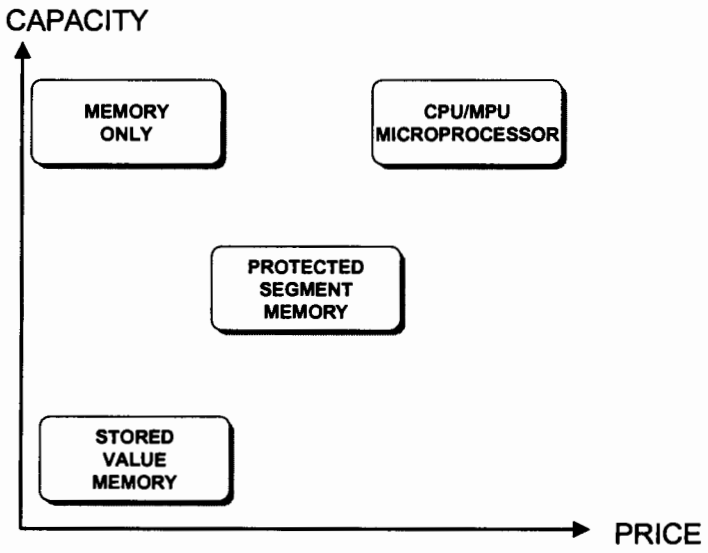

Figure 3. Functionality and Performance of Different Integrated Circuit (IC) Card Technologies

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.

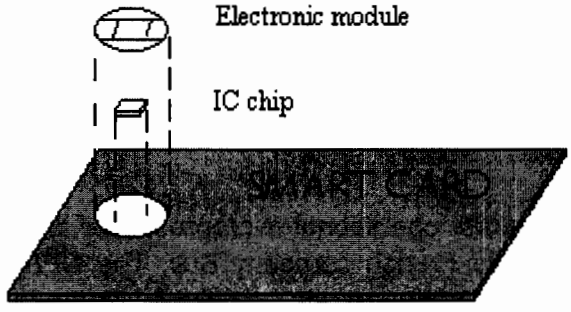

Figure 1. A smart card is a plastic card embedded with one or more integrated circuit chips. Depending on the type of the embedded chip or chips, smart cards are categorized as memory cards, processor cards, or with both types of chips

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.

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.

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.

- 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.

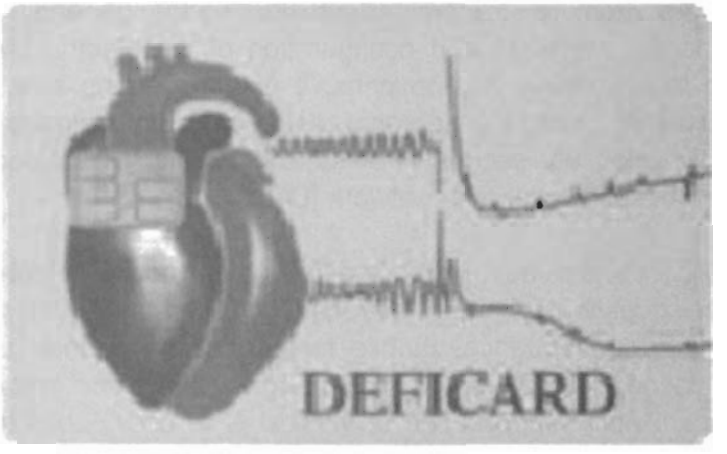

Figure 4. The DefiCard developed for patients with implanted defibrillating devices (1993)

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.

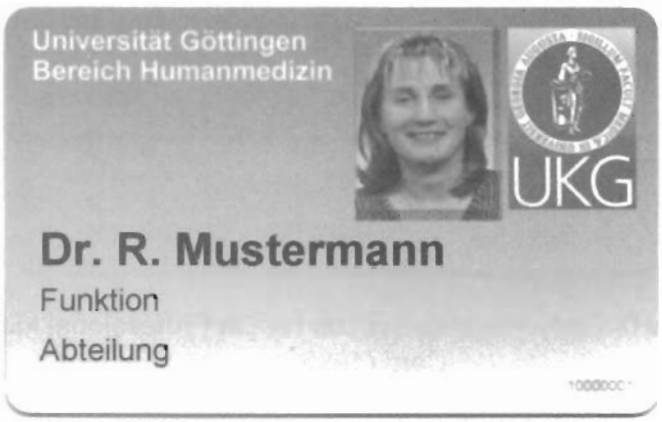

Figure 7. Contactless card of the Goettingen University Hospital (1999)

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,

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

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