# Cryptographic Mechanisms for Health Care IT-Systems

Gerrit Bleumer

Institut für Informatik, Universität Hildesheim, Samelsonplatz 1, D-31141 Hildesheim, Germany, Fax: ++49 5121 883-732, e-mail: bleumer@informatik.uni-hildesheim.de

**Abstract**

Present health care information and communication systems sufficiently respect neither the interests of the professional users (physicians, nurses, etc.) nor those of the usees (patients) concerning informational self-determination, integrity, and non-repudiation. The EU-AIM-SEISMED project has attacked this challenge. There is consensus that legal regulations and organisational measures around health care IT-systems have to be revisited and harmonised. However, the increasing processing capacities of IT-systems demand that the legitimate security interests of users and usees are enforced in advance — not only after the fact. This cannot be achieved against IT-systems but only by the help of IT-systems. Since cryptographic mechanisms are an essential tool to this end SEISMED provides guidelines and technical recommendations on cryptographic mechanisms.

## 1. TRENDS AND RISKS IN HEALTH CARE INFORMATION PROCESSING

The world of health care is on its way to be transformed by the advent of more and more integrated and powerful IT-systems [2]. Multinational industries are establishing information highways and double the computing power available per ECU by every 12 to 18 months. This induces not only a trend towards more and more complex and integrated applications, but creates new *virtual environments*. World-wide observation of diseases like cancer, AIDS, etc. will be possible as well as distance surgery or remote consultation and distance learning in medical education. These services have the potential to create rapidly growing markets of health care technology and promise to support the health care of patients. Although these promising economical prospects have led to a highly fragmented health care market up to now [3] it will pay off to the vendors even more, if they integrate their solutions and services. Hence, it is likely that virtual medical environments will become reality even if they bear the danger to reduce the autonomy and privacy of all its *usees* and *users*.

Conventionally, health care professionals are regarded as users, i.e., those who actively process data, whereas patients are regarded as usees, i.e., those whose data is used. Note, however, that these roles are not innate but that the progress in health care IT endows, for example, patients with sophisticated “digital organs”, i.e., personal computing devices like advanced cards [4, 5] enabling them to act as users.

These devices will significantly enhance the patients’ potential to process and to communicate data in digital form and thereby will increase the effectiveness of how patients, i.e., every human individual, participate in the forthcoming virtual medical environments. In many European countries patients already carry chip cards containing their personal administrative or medical data. On the one hand, patients will hardly refuse to link into virtual medical environments since this would at the same time exclude them from many valuable services. On the other hand, patients will feel uncomfortable being connected to a “medical big brother”.

The development of virtual medical environments aggravates the problem of how the interests and the self-determination of patients can be protected and balanced against the interests of physicians, hospitals, health care institutions, employers and health insurances. Patients can enforce their informational self-determination only if they realise themselves as active users of the virtual medical environments rather than only as passive usees. The ultimate task of designers, engineers and manufacturers is then to provide personal devices in which users may trust and integrated IT-systems which cooperate with the personal devices in such a way that the whole distributed system is credible to all its users, i.e. patients and professionals, etc. [6]

## 2 THE UNSATISFYING PRESENT SITUATION

Today, many hospitals utilise combinations of mainframes and PC-based local area networks which together form large, distributed information and communication systems. Often, these systems coordinate different operating systems, databases, etc., neither of which is really secure. Besides, these local distributed systems get linked to other insecure systems by wide area networks like Internet, etc. There are a lot of proposals to deal with the emerging security problems, e.g., [7, 8, 9, 10]. From the viewpoint of security these distributed systems can be understood best by a kind of *post-box analogy* (Fig. 1). The personal PCs and workstations compare to different post-boxes, which integrate the functions of a mailbox and a P.O. Box. Digital messages which are directed to certain recipients compare to postcards. The user interfaces compare to the front doors of the post-boxes. The users' passwords compare to physical keys matching the locks of the front doors. The operating systems and networks compare to the conventional mailing system which collects, transports, and distributes postcards.

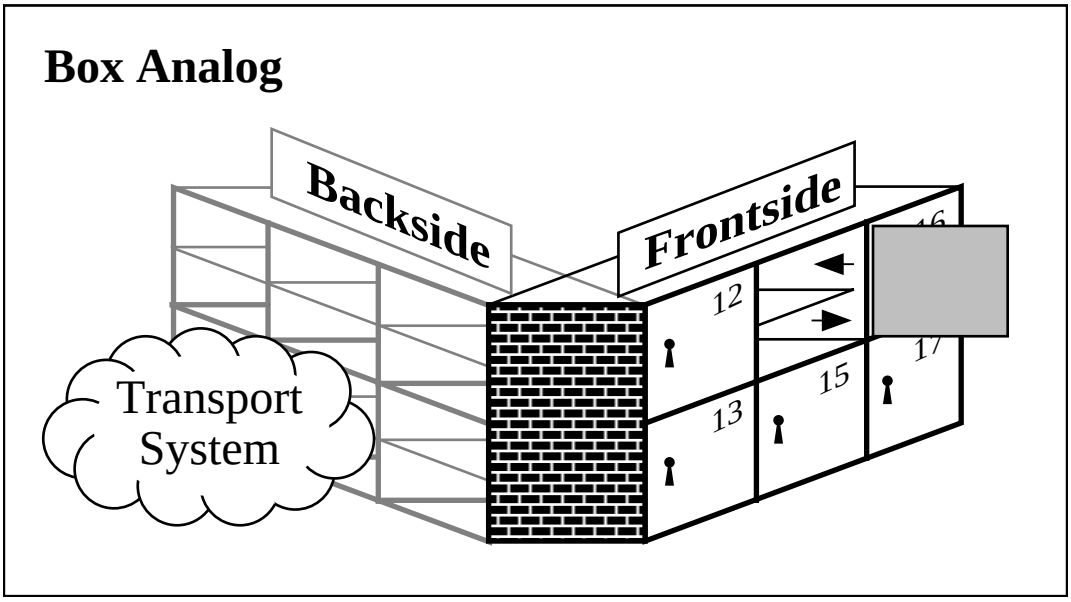


Fig. 1 Box Analogy for a Multi-User IT system

The present, widely used, distributed systems (e.g., client-server systems) are thus characterised by a large central backbone unit (the mailing system of the post-box analogy) which is shielded against unauthorized users (Fig. 2) and has to be trusted by every user with respect to confidentiality, integrity, and availability. The central backbone unit could read any message as well as modifying or destroying it. Since users can neither prove that they have done something, e.g., put in a particular message, nor that they have stayed away from something, e.g., from modifying a file, non-repudiation cannot be provided by these systems either. Even if none of the passwords is figured out illegitimately the users of such systems run significant risks — even more if they are personally liable for the actions they take, e.g. physicians who store diagnoses, therapy plans, etc. into a hospital's information system [11]. The popular firewall concepts are just another method to shield a system, namely against users who have access to the system by means of a gateway (e.g., dial in lines). In the postbox analogy implementing a firewall simply means that new postboxes are created for remote users. The remaining risks like system software malfunction, penetrating system software to reach supervisor privileges, worms and viruses are far from purely academic or unrealistic. In fact there are many parties involved in installing, running, upgrading and maintaining the central backbone units. All of them have to be trusted by the end users of the distributed system in question.

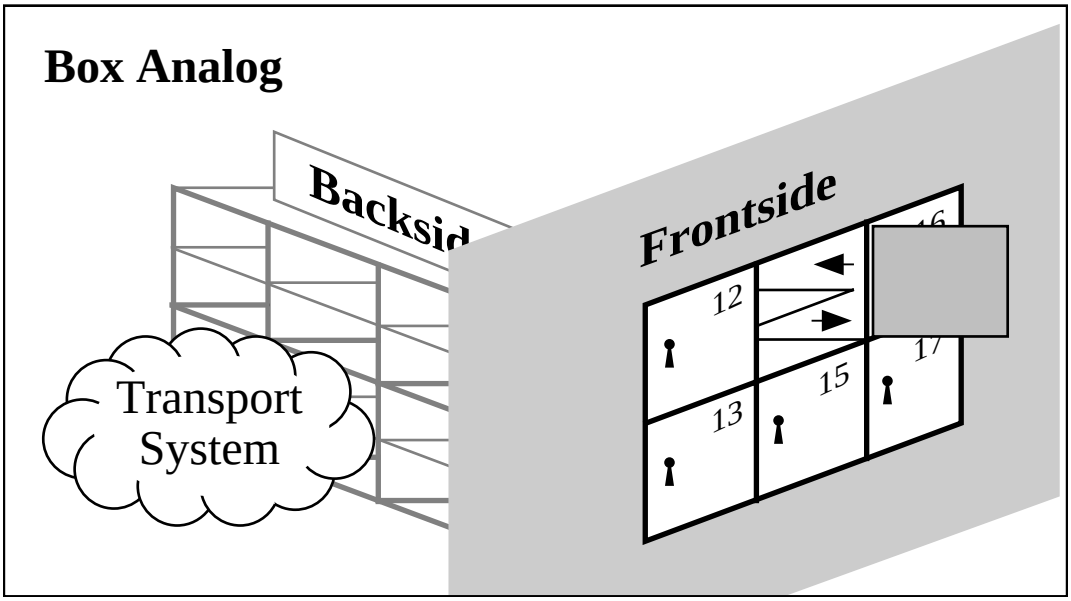


Fig. 2 Shielding a Multi-User IT-system

## 3 SECURE HEALTH CARE IT AND THE ROLE OF CRYPTOGRAPHY

It is widely agreed and becomes more and more apparent that the position of the usees of medical information systems has to strengthened — not only by legal regulations and organisational measures but also by the evolving IT-systems themselves [12]. One if not the way to achieve this is to encourage and enable every usee to act as a user of the IT-systems by equip-

ping her/him with a personal IT-device under her/his own control. Speaking in the post-box analogy these devices must be capable to envelop messages or to prove their origin by a signature before passing them to a mailing system. Both has to be done in such a way that the mailing system (and other users) cannot subvert it (Fig. 3). Note, that each box with its enveloping and signing facility is now under the exclusive control of its user rather than under the control of the transport system as in Fig. 2. Introducing digital signatures allows for non-repudiation by setting up an independent third party, called "court", which is to ultimately decide on the validity of digital signatures. Naturally, it has to be respected by the system managers and administrators as well as by the users and usees.

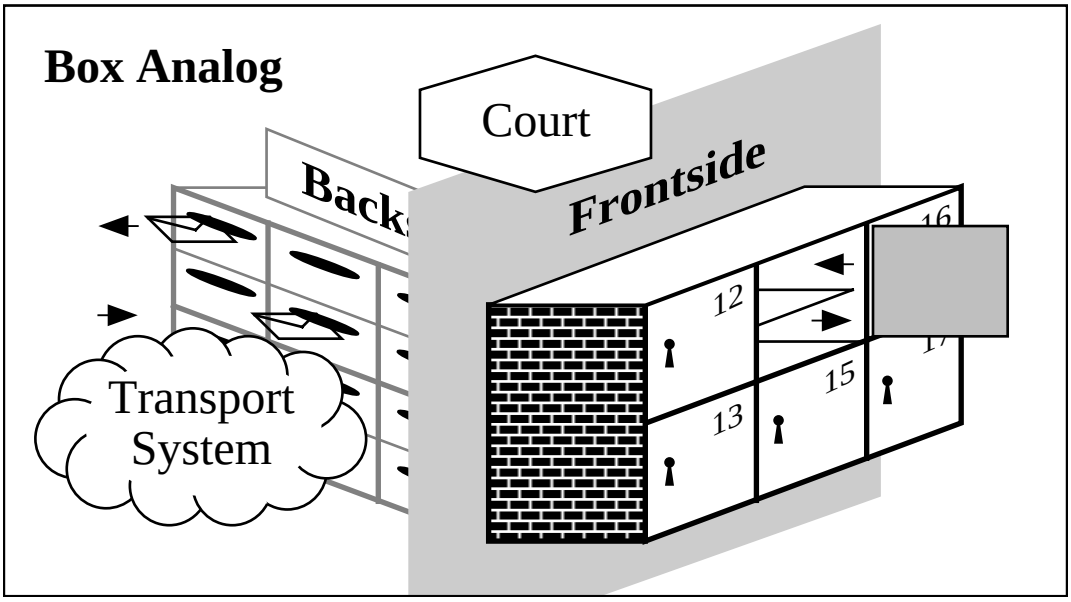


Fig. 3 Postboxes under the Control of their Respective Users

Digital assistants, palmtops, and advanced cards can form the hardware basis for these solutions, whereas cryptography provides the practical protocols and mechanisms as well as the theoretical foundations. In the postbox analogy the personal devices are represented by self controlled postboxes. (Fig. 3)

The statement here is that the legitimate security requirements of the various participants of a health care community can be fairly met only by a separation of power: Those who are in charge of transmitting and processing personal medical information must not be the same as those in charge of protecting that information or as those who ultimately decide about disputes. In contrast the originators of personal data have to be supported to protect that data by themselves.

Patients having all personal medical data about them by means of, e.g., some digital assistant, or having all their personal medical data stored in hospital information systems are only the extremes of a scale. A better balance between availability and confidentiality of personal medical data might be achieved if a patient's record is enveloped (enciphered) and the deenveloping key resides not only with the patient but is also shared, for example, to the doctor and the nurse in charge of that patient. This setting prevents the doctor and the nurse to read the

patient data individually but allows them to do so in cooperation. Threshold cryptography provides the means for more sophisticated delegations of access rights as well [13].

So far, principle insufficiencies of modern health care IT have been analyzed and technical means have been sketched to overcome them. Moreover, it has been agreed that these mechanisms should be integrated into operational health care IT. The EU-AIM-SEISMED project was formed with this clear intention and has — in addition to a security framework — come up with guidelines and technical recommendations about cryptographic mechanisms. Reflecting the current situation that it is too expensive for most health care environments to afford special hardware for every PC or workstation SEISMED pushed the development of a software library of cryptographic mechanisms for standard hardware. The efficiency of that library has been demonstrated by SECURE Talk, a prototype for secure file transfer [14].

## ACKNOWLEDGEMENT

Many thanks go to Erik Flikkenschild and Kees Louwerse who gave me a lot of insight into operational health care IT systems and the practical clinical situation. Joachim Biskup and Michael Hortmann provided interesting comments and Andreas Pfitzmann introduced me to German initiatives about chip cards for health care.

## REFERENCES

1. Barber B, Bakker AR, Bengtsson S (ed.): Caring for Health Information: Safety, Security and Secrecy, Elsevier Amsterdam 1994.
2. Rienhoff O: Digital archives and communication highways in health care require a second look at the legal framework of the seventies; in [1], 13-19.
3. Rienhoff O: Health Informatics Methodology and the Fragmented Health Care Market; K. Brunnstein, E. Raubold (ed.): Applications and Impacts, Proceedings of the IFIP 13th World Computer Congress, IFIP Transactions A-52, Elsevier 1994, 494-501.
4. Klein GO: Smart cards — a security tool for Health Information Systems; in [1], 147-151.
5. Kühnel E, Klepser G, Engelbrecht R: Smart Cards and their Opportunities for Controling Health Information Systems; in [1], 153-157.
6. Biskup J, Bleumer G: Reflections on Security of Database and Datatransfer Systems in Health Care; K. Brunnstein, E. Raubold (ed.): Applications and Impacts, Proceedings of the IFIP 13th World Computer Congress, IFIP Transactions A-52, Elsevier 1994, 549-556.
7. Castano S, Fugini MG, Martella G, Samarati P: Database Security; Addison Wesley - ACM Press, 1995.
8. Garfinkel S: PGP Pretty Good Privacy; O'Reilly & Associates, Sebastopol 1995.
9. Stallings W: Network and Internetwork Security - Principles and Practice; Prentice Hall - IEEE Press, Englewood Cliffs 1995.
10. Biskup J: Medical Database Security; Data Protection and Confidentiality in Health Informatics – Handling Health Data in Europe in the Future, Edited by the Commission of the European Communities DG XIII/F AIM, Proc. of the AIM Working Conference, Brussels, 19-21 March 1990, IOS Press, Amsterdam 1991, 214-230.
11. Gaunt N, France FR: The need for security - a clinical view; in [1], 189-194.

12. Kluge EH: Advanced patient records: Some ethical and legal considerations touching medical Information Space; Methods of Information in Medicine 32 (1993), 95-103.
13. Desmedt YG: Threshold Cryptography; European Transactions on Telecommunications 5/4 (1994) 449-457.
14. Bleumer G: Security for decentralised health information systems; in [1], 139-146.