AIM (Advanced Informatics in Medicine)
Secure Environment for Information Systems in MEDicine
SEISMED (A2033)

Document Reference	SEISMED(A2033) / SP08.09 / HILD / DEL / 08.03.1995		
Deliverable No.	29	Distribution	All parties
Deliverable Type	Deliverable	Status	Final
Activity			

Title

Guideline for cryptographic mechanisms
— IT-system end-users —

Author

Gerrit Bleumer, University of Hildesheim,
Institute for Computer Science
Samelsonplatz 1, D-31141 Hildesheim, Germany,
bleumer@informatik.uni-hildesheim.de

Keywords: Secure IT-systems; Encipherment mechanism; Digital signature mechanisms

Collaborators: Erik Flikkenschild (AZL), John Fowler (RLT)

EXECUTIVE SUMMARY

The comprehensive objective of SEISMED (a Secure Environment for Information Systems in MEDicine) was to elaborate a consistent, harmonized framework for medical data protection throughout Europe. The specific technical proposals of SEISMED are thus accompanied by a high level security policy which presents the underlying principles. This approach is consistent with the forthcoming European ITSEC activity.

SEISMED proposes a suite of cryptographic mechanisms in order to provide sufficient flexibility to meet the characteristic challenges of health care data processing:

- A long tradition of decentralized processing of health care data with multilateral and legitimate interests.
- Ultra high sensitivity of personal medical data whose disclosure might not be repairable by, e.g. smart-money.
- Long periods of time (up to 30 years) over which health care data must be archived in its original state.

A 20 man-month workpackage evaluated the pertinent cryptographic literature, other relevant EC-projects (RACE Integrity Primitives Evaluation project RIPE), and renowned conferences (IACR Crypto, IACR Eurocrypt, ACM Symposium on Theory of Computing, Symposium on the Foundations of Computer Science, IEEE Symposium on Research in Security and Privacy, etc.). The result is a cryptographic guideline which is presented by separate documents to three different target audiences.

Cryptographic guideline of SEISMED

Audience	**Document Title**	**Content**
Health Care Management	Guideline for Cryptographic Mechanisms —Health Care Management—	Odds and ends of cryptography: The use for health care IT-systems
IT-system end-users	Guideline for Cryptographic Mechanisms —IT-system end-users—	Odds and ends of cryptography: The benefits for IT-system end-users
IT and security personnel	Technical Recommendations for Cryptographic Mechanisms —IT and security personnel—	Suite of proposed cryptographic mechanisms

Health Care Management

This part addresses the management of a health care environment. While a rapidly evolving information technology often leaves the management confused, the management is responsible for keeping its health care environment working efficiently. To this end, *integrated IT systems* appear to be the ideal solution. This report identifies their specific risks which should be considered when deciding about new systems or upgrades of existing ones. This is even more important since indeed the management decides about IT-system installation, but in many cases the medical end-users like physicians are accountable for breaches of security of these systems. Hence, a management will only succeed in installing integrated IT-systems if it succeeds in inspiring the confidence of the end-users into these systems. Severe limitations of conventional security measures like passwords are identified and it is shown how these limitation can be overcome by applying cryptographic mechanisms. General aspects of integrating cryptography into existing applications are discussed.

IT-system end-users

This part addresses IT-system end-users, like physicians, medical staff, etc. who deal with sensitive medical data. Normally, these end-users are *personally* responsible for the medical data they input and process. Complementary, they are also responsible if such data is modified or misused by other users. Hence, system end-users are particularly anxious about the risks which stem from the use of IT-systems. A conclusive introduction to the fundamental benefits of cryptography is provided which outlines how the identified risks can be reduced or eliminated.

IT and security personnel

This part addresses software and hardware designers and implementors who are responsible for the security of an IT-system. A suite of cryptographic mechanisms is proposed to be used by health care IT-systems.

First, the identified security requirements are mapped to cryptographic building blocks. Second, a few alternative cryptographic mechanisms are proposed to implement each building block. This two-step approach was found useful to make the document more readable and adaptable to future results in cryptologic research. In order to support the selection of mechanisms that comply with a given security policy, this report analyses explicitly how strong an adversary the proposed mechanisms resist. Two key applications in health care data processing are digital networks and databases. Specific proposals outline how these key applications can make use of the proposed cryptographic mechanisms.

Demonstrator

In order to demonstrate the functionality and efficiency of the recommended mechanisms, a software prototype (SECURE Talk) was built that protects data transferred through (linked) Apple Talk networks from unauthorised disclosure and undetectable modification. The demonstrator also provides an automatic key management for all cryptographic mechanisms. All results are documented in the document “Technical Recommendations for Cryptographic Mechanisms —IT and security personnel—”. SECURE Talk is available as a software application for Apple Macintosh from the author.

CONTENTS

1 INTRODUCTION

Processing of health care data involves medical, social, administrational, and business aspects. The on-going increase of medical treatment forces the health care environments to rationalize their organization, medical treatment, communication, and documentation. This is the driving force to employ IT-systems in health care. Some characteristic problems of processing medical data are:

1. Highly sensitive data (severe patient interest),
2. Potential misuse of Health care IT-systems (organized crime),
3. Long periods of archiving and authentication of data

Whenever end-users are liable for health care data they should and will use only IT-systems they trust. IT-systems which are simply protected by password mechanisms and audit facilities do not deserve this trust by end-users. More sophisticated countermeasures like cryptographic mechanisms are necessary.

2 SECURITY OF MEDICAL RECORDS IN THE INFORMATION AGE

Naturally, health care professionals are aware about the sensitivity of the medical records of their patients. Caring and healing can only be successful if the relationships between patients and physicians are protected by strong privacy. Hence, there is a long tradition of professional secrecy in health care.

It is generally agreed that this principle must of course not be violated by the advent of IT-systems in health care. Nevertheless, many health care professionals as end-users of IT-systems feel that this violation is exactly what happens. They do not trust into networked IT-systems since they have no sufficient control over other persons' access to “their” data. From the viewpoint of a health care professional, e.g., a system manager is as little authorized to inspect “his” data as any other ordinary end-user is. Unfortunately, this feeling of mistrust into most of today's IT-systems is fairly justified.

IT-systems in health care tend to integrate more and more departments, they connect more and more end-users by communication facilities, but they suffer from low credibility with respect to confidentiality, accountability, and maybe even availability. Would you really put some sensitive piece of data about your patient into a networked IT-system to which thousands of users from around the world have remote access via e-mail, fax, etc.? Or would you accuse another college for some wrong input if the only hint you have is an audit trail presenting his password? Finally, would you rely on the availability of an IT-system in an emergency situation where seconds or minutes count?

Presumably, the answer to all the above questions is NO. Nevertheless, many health care professionals do not want to miss the obvious advantages of IT-systems and, hence, one often finds the situation of many separated PCs, workstations, etc. in health care environments. The objective of SEISMED was to investigate the conditions under which integrated IT-systems can be reliably secure. Not surprisingly, it turned out that cryptography can help a lot to ensure confidentiality and accountability. The aspect of availability, however, cannot be improved by cryptography. This remains an issue to fault tolerance.

3 WHY ARE PASSWORDS INSUFFICIENT?

From the viewpoint of a health care professional IT-systems can be of significant help for documentation, communication, image processing, information retrieval, and many other tasks. However, processing health care data is embedded into a legal framework which must be respected regardless of the technology applied. A crucial point of such legal framework is how the cooperations of end-users like internal and external health care professionals, administration staff, etc. is regulated. These regulations state, for example, who may or must create, update, or maintain which documents; who may or must read and consult which documents; who must not read which documents. Usually, these regulations only take the end-users into account, but not the producers, operators, and maintainers of these systems.

A distributed IT-system [Sand1_94, Sand2_94, Sand3_94, PaKa1_94, PaKa2_94] can be understood by a “box analog”. Consider a set of users who store, retrieve, and communicate their data by means of some box-system, e.g., a system of post office boxes. This box-system can handle postcards only, not enveloped letters. Each user has one box associated. The front ends of the boxes serve as interfaces to the users and each user is provided with a key matching the lock of the front door of his own box. The back ends of the boxes are simply open. A transport service is provided which collects input postcards through the back of the boxes and drops them into the addressed boxes.

The boxes and keys correspond to accounts and passwords, the postcards correspond to text files or image files, etc. With the box-analog in mind, distributed systems obviously bear a variety of new problems and risks.

Breaches of user and data authentication: Often, for medical documents a proof of origin is required in order to provide accountability. Conventionally, such a proof is provided by a handwritten signature under a document. Even if documents would exclusively be handled by the above box-system signatures would by no means be superfluous. For example, if a doctor Alice finds a medical diagnosis in his box indicating that it was sent by doctor Bob, what worth is that diagnosis? Nearly nothing; doctor Bob is not provided with any *proof* neither that the data received is the one sent (the reliability of the transport service must not be presumed), nor that the de-facto sender is indeed the one claimed (some doctor Charlie might have masqueraded as doctor Bob.).

Breaches of confidentiality: Often, medical documents are confidential. Conventionally, such a document would be enveloped before it is transported. Even if documents would exclusively be handled by the above box-system envelops would by no means be superfluous. The content of postcards could be inspected by the transport service, and hence, it would be uncertain who will get to know the transported data except the intended recipient. The transport service of the box-analog corresponds to public transmission lines, operators and maintenance personnel of transmission and storage devices, etc.

Unauthorized access: More and more health care IT-systems are being opened to worldwide communication networks and, hence, provide remote access. In the box-analog this means that there are some boxes whose front ends are unlocked. For users who gain access to them the locks of other boxes are no longer relevant. Conventionally, unauthorized access and misbehavior is tried to be detected by audit trails. Although necessary, they are not satisfactory. In the best case they can prove a suspicion, but they do rarely *raise* it. For example, a security manager who has to scan hundreds of pages of an audit trail in order to detect any breaches of security is likely to overlook suspicious entries. Let alone that he gets bored and stops reading after only a few pages.

Thus in principle, it is desirable to install —whenever possible—

preventive countermeasures rather than **subsequent** ones and

interior countermeasures, which are implanted within the IT-systems rather than **exterior** countermeasures, which support the organizational environment into which an IT-system is embedded.

Cryptographic mechanisms are a suitable means to reduce or to eliminate the above mentioned risks and to enhance the security of open distributed systems.

User and data authentication can be achieved by so-called **digital signatures**. A digital signature can be *produced* and *verified* only by some electronic device. To produce a signature, this device has to “know” the personal signing key of the respective signer. The digital signature itself is a string of at least say 700 bit and thus cannot comfortably be verified simply by looking at it. Hence, it is verified by a device which moreover has to “know” the verifying key of the signer.

Digital signature mechanisms provide an even stronger authentication than handwritten signatures can because they are specific not only for the originating user, but also for the message signed. An originator produces a different digital signature for every message he signs. Thus, if a message is modified after it has been signed this modification will be detected by the verifier. It should be clear, that digital signatures are completely different from “digitized signatures” which are simply digitally represented handwritten signatures.

Confidentiality can be achieved by so-called **encipherment mechanisms**. Data can be enciphered and deciphered by some electronic device; possibly the same which produces or verifies signatures. Enciphering corresponds to enveloping the postcards of the box-system above.

A strong encipherment mechanism can prevent users to read data which they are not authorized to read although they might be able to read the enciphered form of that data. This applies e.g. to wiretappers in digital networks or intruders of database systems.

4 WHEN AND HOW TO USE CRYPTOGRAPHY?

Cryptography is a feature most parts of which can be made transparent to the system end users. But for example, as you remember how to produce your handwritten signature, you will have to “remember” the way how to produce your digital signatures. Since it is your own interest not to give away this knowledge you should not even pass it to an IT-system component that you do not trust. End users like physicians, nurses, and patients will hold some kind of **personal, physical device** which is capable to hold a user's personal data and to produce the corresponding digital signatures or to decipher the messages received. Such personal devices can be smart-cards, advanced cards, handheld pen-computers, etc.

Since the personal devices are under the exclusive control of the end users they can and should apply them to sign or envelop digital documents whenever they would do so with paper based documents. Of course, these personal devices must be supported by every day's health care applications. For example, if you intend to send some digital image to a college, a dialog might ask you for an explicit signature. Alternatively, a user might wish to sign all his messages by default. Only in special cases he might want to omit a signature. The same applies to enveloping data. The integration of security features into existing applications is an rapidly evolving field of standardization and, hence, needs the discussions of end-users and system developers.

Applying cryptography is a technical means which must be supported by **training and awareness programs**. All parties involved must be informed about their benefits and must be motivated to use the new features appropriately. For example, social and legal impacts of digital signatures [KaGr_94] should be anticipated by the trainers and should be discussed by the end-users.

BIBLIOGRAPHY

KaGr 94 — AIM SEISMED: Katsikas S: High level security policy for health care establishments, Deliverable 14, SP04.03; ©University of the Aegean, Greece, 1994.

PaKa1 94 — AIM SEISMED: Patel A: Guidelines of the possible implementation of the security mechanisms and protocols by the reference centres —Health Care Management—, Deliverable 27, SP09; ©University College Dublin, Ireland, 1994.

PaKa2 94 — AIM SEISMED: Patel A: Guidelines of the possible implementation of the security mechanisms and protocols by the reference centres —IT and Security Personnel—, Deliverable 27, SP09; ©University College Dublin, Ireland, 1994.

Sand1 94 — AIM SEISMED: Sanders P: Baseline security guidelines for existing systems —Health Care Management—, Deliverable 26, SP07; ©University of Plymouth, England, 1994.

Sand2 94 — AIM SEISMED: Sanders P: Baseline security guidelines for existing systems —IT-system end-users—, Deliverable 26, SP07; ©University of Plymouth, England, 1994.

Sand3 94 — AIM SEISMED: Sanders P: Baseline security guidelines for existing systems —IT and Security Personnel—, Deliverable 26, SP07; ©University of Plymouth, England, 1994.