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

Document Reference SEISMED(A2033) / SP14 / HILD / DEL / 05.07.95

Deliverable No. 32 Distribution All parties

Deliverable Type Report Status Final

Title **Introduction to the SEISMED Guidelines**

Author Gerrit Bleumer,
Universität Hildesheim, Institut für Informatik
Samelsonplatz 1, D-31141 Hildesheim, Germany

Abstract The efficiency of modern health care relies more and more upon a computerised infrastructure. Open distributed IT-systems have started to bring professionals together from all over the world. On the one hand easy processing and communication of images, sounds, and texts will help to represent and treat illnesses and diseases efficiently, on the other hand they may threaten the privacy of patients, and the accountability and professional secrecy of health care professionals. The European Union has initiated a multi disciplinary project to come up with practical guidelines how to achieve a Secure Environment for Information Systems in MEDicine (SEISMED). It has taken into account the traditional and proved principles of health care data processing, the various legislations within the EU, the enormous and subtle risks of health care IT-systems, and the cost of changing existing technology. Four Reference Centres in Europe have validated most of the guidelines.

Collaborators Barry Barber, John Davey, Kees Louwerse

Guidelines for a Secure Environment for Information Systems in Medicine — SEISMED

Abstract

The efficiency of modern health care relies more and more upon a computerised infrastructure. Open distributed IT-systems have started to bring professionals together from all over the world. On the one hand easy processing and communication of images, sounds, and texts will help to represent and treat illnesses and diseases efficiently, on the other hand they may threaten the privacy of patients, and the accountability and professional secrecy of health care professionals. The European Union has initiated a multi disciplinary project to come up with practical guidelines how to achieve a Secure Environment for Information Systems in MEDicine (SEISMED). It has taken into account the traditional and proved principles of health care data processing, the various legislations within the EU, the enormous and subtle risks of health care IT-systems, and the cost of changing existing technology. Four Reference Centres in Europe have validated most of the guidelines.

1 Introduction

One of the causes of the crisis of modern health care (in industrial countries) is that the enourmous increase in diagostic and therapeutic achievements is not backed by an equally efficient management of the resulting information. For example, several mega-bytes of patient data are produced within seconds by imaging facilities but the storage, update, retrieval and communication of this data is often done on a material basis like written or printed documents or slides. Obviously, all kinds of data processing are speeded up by some orders of magnitude if the information is represented digitally instead. Moreover, patients will become more mobile in the forthcoming European market, medical treatment is divided into ever more specialized steps, and the obligations for handling and archiving medical data tend to become more professional and thereby more ambitious. In effect, information technology becomes ever more closely involved with the detailed processes of the delivery of health care whether in terms of contributing to the diagnosis or treatment of patients.

1.1 Need for security

As is the case with any development in health care, the introduction of information technology should focus primarily on the improvement of the health of patients. This means that the right data has to be available to the right person at the right time (**availability**). Information technology deeply affects the confidential relationship between patient and doctor, since it increasingly surrounds and mediates it. Hence, the protection of personal medical data (**confidentiality**) is a necessity without which medical treatment will hardly be successful. This will sometimes include the **anonymity** of a patient. In addition to the protection of data from unauthorized reading it also has to be protected against unauthorized modification (**integrity**). The subtlety of these notions is that unauthorized action is not restricted to unauthorized people only — like visitors to a hospital or burglars. Even authorized users or, worse, system administrators might attempt to perform unauthorized actions. Unlike the legal situation of employees in commerce (not to mention the military) health care professionals are personnally responsible and mostly liable for their decisions in favour of a particular action or against it. This raises the need for IT which is capable of providing an individual with undoubtable proof that he or she took a certain action or did not (**accountability**). If safety critical medical IT-systems which are relied upon by health professionals in their clinical work, e.g., radiation therapeutic systems, fail in terms of integrity or accuracy, then patients will be incorrectly treated with all the consequences that this may have [11]. This may happen particularly when staff are under pressure in terms of work load or patient condition. Additional cross checks may not be applied and the system may be believed with potential dangerous results. A more informative clinical view about security needs is provided by [12].

1.2 European challenges

The IT-systems in health care establishments develop towards an increasingly integrated system by which various users interact and communicate. This process of integration is going to cross the borders of local health care establishments and will integrate them as well as, e.g., patients' homes, into a **European health care community**, in order to support the mobility of patients, the exchange of medical and administrational data, transfer of bills and money, etc. At the same time the term "user" gets a broader meaning; it will comprise patients, health care professionals, clerks, maybe even health authorities and insurances. The integration of different health care services and a minimum of equity of health care quality can only be achieved by harmonisation on legal, organisational and technical levels and in particular with respect to security.

1.3 Managing security

In order to protect the assets of a health care establishment the management has to balance the overall targets, the estimated risks, and the levels up to which the security requirements are to be met. This balance is documented by the **security policy** of a health care establishment. Of course, the security policy has to conform to all regulations of higher precedence like legal regulations.

One of the most sensitive targets of a health care establishment is its operational quality and reputation and thereby the trust of patients and the acceptance by the medical community of the region or country where it is located. Surely, reputation cannot be measured accurately, but there are counter indications like a bad press. These targets can only be met if the security policy of a health care environment reflect the personal security requirements of all individuals affected, namely the **users**, e.g., health care professionals and the **usees**, e.g. patients and employees whose personal data is processed.

Hence, the security policy cannot be independent from the technical system in use since, obviously, not all the affected indivduals do trust the technical system in the same way and to the same extent. If at all, they trust in different and overseeable components (hard- or software) of a large internetworked and distributed IT-system. Thus, the security policy must adopt a **decentralized view** stating explicitly which subjects or groups of subjects should be able to enforce which security requirements [17]. To the contrary, most of today's security policies adopt a centralistic view, i.e., they prescribe which individuals or groups of individuals have to trust which objects, e.g., hardware or software components, or other privileged individuals. Without saying so, the centralistic approach assumes a “friendly big brother” trusted by every user, whereas the decentralistic approach assumes collaborating user agents each of which is trusted by its own user only. Clearly, a centralistic security policy will subvert the acceptance of an IT-system and thereby of a health care establishment since trust of individuals cannot be prescribed — it can only be taken into account.

1.4 Putting security into practice

A health care establishment has to put its security policy to practice by training personnel, organisational measures and technical means. This is the focus of the guidelines at hand. Chapter 2 outlines the basic categories of guidelines, their interrelationship and content (Fig. 1).

The legal and organisational recommendations, guidelines on risk analysis and reports on validation directly address the health care establishments, whereas the technical guidelines and recommendations address the designers and developers of IT-systems in the first place. Since most health care establishments do not develop IT-components by themselves they are interested in system and application products that conform to their specific security policies. This problem, however, is not attacked by the SEISMED guidelines but is the subject of several national initiatives who developed **criteria for the evaluation of information technology**. See for example the US, Canadian and European approaches [13, 14, 15]. A landmark harmonizing effort are the Common Criteria on the Evaluation of Information Technology [16], based on the above mentioned activities.

SEISMED has identified different **target audiences** within health care environments, each of which is addressed by a separate package of guidelines. The mapping of **guideline packages** to target audiences is found in chapter 3. Finally, chapter 4 gives the background and dissemination effort of the SEISMED project.

Appendix A provides a glossary of security terms which have been adopted by CEN TC251 working group 6 (security).

2 Overview

SEISMED provides four categories of guidelines each of which consists of a set of specific guidelines. The categories are explained in the following and Fig 1. presents their interdependencies and contents.

2.1 Legal analysis and guidance

The legal regulations of health care data processing in the EU member states (including a few Swiss Kantons) have been studied and summarised. A DEONTOLOGY CODE for health care and legal professionals is developed and proposed for use throughout Europe. It represents the major ethical principles which conform more or less to the legislation of every EU-country. This code is intended to be invariant against organizational and technological development. On the one hand, fundamental changes of legislation should be reflected by the DEONTOLOGY CODE, on the other hand, the DEONTOLOGY CODE might itself lead to further legislation. The upcoming EU-directive [19] on the protection of individuals with regard to the processing of personal data and on the free movement of such data has taken into account the processing of medical data (art. 8). However, the directive still refers to the national law or rules established by national competent bodies to the obligations of professional secrecy for the processing of medical data health professional subject. Therefore, the DEONTOLOGY CODE with its more specific stipulations will offer guidance to national legislators and the health care personnel. The code should be largely discussed and reviewed in order to establish at the end a Community code which may be submitted to the Working Party on the Protection of Individuals with regard to the processing of personal data as provided in the upcoming directive (art. 27, 29) [23].

Given a DEONTOLOGY CODE it has to be translated into a (High Level) Security Policy for a specific health care establishment. SEISMED has adopted a layered approach [20]. At the top level Generic Principles are stated, which depend on the societal and cultural background considered. These Generic Principles basicly coincide with the essence of the Deontology Code. Given an administrational framework, the Generic Principles are further translated into specific Principles, which, given a technological context are further translated into specific Guidelines. At the bottom level, where a particular technical installation is given, the Guidelines are finally translated into specific Measures.

Guidelines provided:

1) Health Informatics DEONTOLOGY CODE [21],
2) HIGH LEVEL SECURITY POLICY for Health Care Establishments [22].

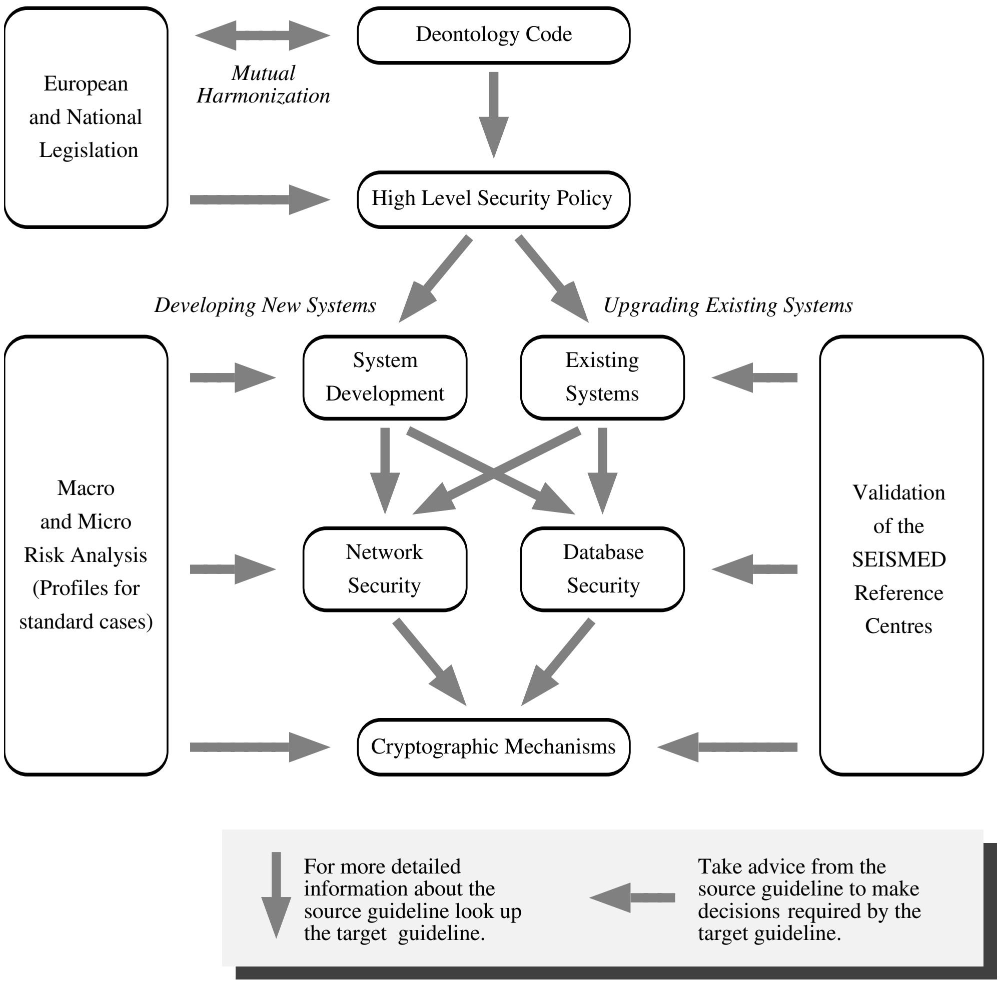

Fig. 1 Interdependencies of the SEISMED guidelines

2.2 Support of risk analysis

During the work using CRAMM [7] within the Health Care environment in England it had become apparent that the lowest levels of security measure (1 on a scale of 1 to 5) were not always in place within Health Care Information Systems. It was therefore decided to publish a brief outline of these basic security measures as a starting point for HCE security [8]. This monograph was to improve security levels without waiting for detailed security reviews. “Baseline Security” is certainly not enough but the uniform implementation of all the Basic Security Measures would, at least, be an improvement in many cases! However, the SEISMED Guidelines allow us to go much further than this because they are derived from a wider experience across Europe. An examination of the detailed CRAMM countermeasures recommended at the four reference sites confirmed earlier work that showed that the security requirements of systems utilised for the diagnosis and treatment of patients demanded much higher levels of security than had previously been contemplated [4,8]. It, also, indicated that these requirements were remarkably consistent between the four reference centres, and work is currently in hand to develop a standardised classification system to facilitate the implementation of a small number of security profiles for HCEs.

The result of this analysis is intended to supervise further decisions during the development or upgrade of the IT-system(s) in question.

Guidelines provided:
1) RISK ANALYSIS GUIDELINES for the relevant target audiences [24, 25, 26].

2.3 Technical guidelines and recommendations

The technical guidelines address both the secure upgrade of existing operational IT-systems as well as the design and development of new ones. Since most design, development and upgrade of IT-systems is not done by health care establishments themselves but rather complete solutions are purchased, this category of guidelines also addresses those vendors who develop IT-systems for health care establishments.

Particularly, the core IT-components of distributed systems or IT-system clusters are addressed: digital networks and databases. The main result was that for sensitive medical data conventional security mechanisms like passwords and classical access control are insufficient. A separate guideline recommends cryptographic mechanisms basically for authentication and encipherment purposes. So far, the recommended mechanisms have not been integrated into an operational system at one of the reference centres. Instead, a separate demonstrator [18, 41] was built that shows how digital communication can be enciphered and signed electronically at minimal additional involvement of the user.

Guidelines provided:

1) Guidelines for SYSTEM DEVELOPMENT, design and implementation [27, 28],
2) Security of MEDICAL DATABASE SYSTEMS [31, 32, 33],
3) Baseline security guidelines for EXISTING SYSTEMS [34, 35, 36],
4) Guidelines for NETWORK SECURITY[1] [37, 38, 47],

---

[1] The actual working title of the documents is ”Guidelines of the possible implementation of the security mechanisms and protocols by the reference centres”.

5) Guideline for CRYPTOGRAPHIC MECHANISMS [39, 40, 41].

2.4 Practical validation

Four reference centres in Europe have validated the proposed guidelines. They have continuously fed back their requirements and findings in order to arrive at “practical” guidelines. Their experiences and critique is explicitly provided and resulted in an approved version of final guidelines. These practical experiences should also be consulted when developing or upgrading Health Care IT-systems.

Guidelines provided:

1) THE NEED FOR SECURITY — A clinical view [12, 42],
2) PRACTICAL EXPERIENCE at the reference centres [43].

3 Roadmap

In order to provide the relevant material with respect to the specific interests and expectations of different readers, **colored guideline packages** have been compiled for the three major target audiences addressed by SEISMED:

BLUE	Health Care Management (e.g., hospital managers),
YELLOW	IT-System End-Users (health care professionals, nurses, clerks, patients, etc.),
PURPLE	IT and security personnel (system operators, in-house and external software developers, etc.), and
PINK	General interest.

Each package contains an **appropriate view to each of the guidelines**. Only for some guidelines there may not be a requirement to be known by every target audience. However, where a particular individual finds herself acting in a wider capacity, it will be necessary to explore the guidelines addressed to other groups. However, each HCE has to have a complete understanding of all the issues by utilising all the expertise available to cover the total picture. The collaborative effort is outlined in Fig 3.

The SEISMED guidelines apply to the **operational phase** and to the **development phase** of a health care IT-system. For IT-systems in operation, the successive implementation of the requirements of the DEONTOLOGY CODE, the HIGH LEVEL SECURITY POLICY followed by the EXISTING SYSTEMS guidelines will progressively upgrade the security measures installed within the HCE. For an IT-system, namely the system software under development, the guidelines on SYSTEM DEVELOPMENT are more important than those on EXISTING SYSTEMS. The guideline on CRYPTOGRAPHIC MECHANISMS is applicable to both phases.

Tab. 1 presents the material contained in each of the guideline packages. So far there is a coarse global table of contents for the set of all guideline packages but no global subject index. However, a local table of contents and subject index is found within each guideline itself.

The terminology in particular with respect to security might not be completely consistent throughout all the guidelines. For example, there are separate traditions to approach security in the domain of database security, network security or operating system’s security. Even international standards have not always agreed on a consistent terminology. For the time being these guidelines adopt the definitions given by the CEN TC251 working group 6 (security) which conforms to ISO definitions. Appendix A presents the respective glossary of security terms.

Category	**Guideline package**		
	Health Care Management	**IT-System End-Users**	**IT and Security Personnel**
General	The Need for Security — A Clinical View [12]		
Legal Analysis and Guidance	Health Informatics Deontology Code [21] High Level Security Policy for Health Care Establishments [22] Recommendations for European Health Data Protection Legislation [23]		
Risk Analysis	• Risk Analysis Guidelines [24]	• Risk Analysis Guidelines [25]	• Risk Analysis Guidelines [26]
Technical Guidelines and Recommendations	• Guidelines for System Procurement and Development [27]	—	• Guidelines for System Development and Design [28]
	• Guidelines for Secure Implementation [29]	—	• Guidelines for Secure Implementation [30]
	• Security of Medical Database Systems [31]	• Security of Medical Database Systems [32]	• Security of Medical Database Systems [33]
	• Baseline Security Guidelines for Existing Systems [34]	• Baseline Security Guidelines for Existing Systems [35]	• Baseline Security Guidelines for Existing Systems [36]
	• Guidelines for Network Security[1] [37, 46]	—[2]	• Guidelines for Network Security [38, 46]
	• Guideline for Cryptographic Mechanisms [39]	• Guideline for Cryptographic Mechanisms [40]	• Technical Recommendations for Cryptographic Mechanisms [41]
Practical Validation	Reference Centre Report on the Risk Analysis and High Level Security Policy [42] Reference Centre Report on Operational Security [43] Reference Centre Report on Implementation of Network Security [44, 47]		

Tab. 1 Guideline packages and their target audiences

In order to **draw the greatest advantage from these guidelines** hospitals and clinics are advised to first apply “Getting started with SEISMED guidelines” [46]. The **accompanying tool** “SIDERO” (Security Information Database Experimental Reference Centre Outcome) [45] assists to manage the various guidelines and their results in a particular health care environment. It also takes into account the more general recommendations of the Infosec Business Advisory Group (IBAG).

2 IT-System End-Users can find practical and useful information in [46].

4 Background and Dissemination

The European Commission established an R&D programme of Advanced Informatics in Medicine (AIM) during the late 1980s in order to explore within a harmonised European environment what results could be achieved by the application of informatics to the Health Care environment. The initial investment was quite modest at 20 MECU for projects that involved several member States of the European Community with funding on the basis of 50% of overheaded costs. At this stage 42 projects were funded to initiate this work [1]. At the same time the Commission established a group to explore the impacts of such work on the activities of Health Care and the future development of such work. This group examined a number of issues [2] but, in particular, it appreciated for the first time that there were safety issues in terms of the utilisation of information systems in Health Care. This led to the enunciation of the “Six Safety First Principles for European Health Information Systems” which placed safety as a key issue in the consideration of such systems [3]. At about this same time practical work was suggesting that the security requirements of Health Information Systems needed to be considerably upgraded where these systems were being utilised fully within the context of the diagnosis and treatment of patients in such a fashion that errors in the information system, or indeed, the lack of access to such an information system for a period, might lead to unsatisfactory care and in the extreme case might damage or contribute to the premature death of a patient [4].

Although there were no specifically data protection and security projects in the first phase of the AIM programme, the European Parliament has expressed a definite interest in these issues and the AIM secretariat were able to participate with the relevant working group of the European Federation for Medical Informatics (EFMI WG2) in order to establish a very useful working conference during 1990 [5]. This conference was a landmark event in that the prestige of the European Commission enabled the conference to secure the participation of lawyers and data protection commissioners from a number of European States and information technology security specialists as well as the more regular participants from the medical informatics community. Tenders for projects in the second phase of the AIM programme, which was budgeted at a higher figure of 97 MECU, were invited during 1991. The projects that were supported are outlined in the AIM reports and these included the AIM.SEISMED (Secure Environment for Information Systems in MEDicine) project. It arose from the amalgamation of two proposals which built upon the different strengths of each other’s partners. The work was concerned with the security of Health Care Establishments (HCEs) although this was set within the general context of security measures for information systems [6].

The Guidelines developed on these various areas of security have been validated by the SEISMED project’s reference centres to a large extent. The project presented major parts of its results to the scientific and standards community at the working conference “Caring for health information” of the International Medical Informatics Association (IMIA) Working Group 4 [9]. In order to achieve a broader discussion and awareness, SEISMED organized in July 1994 a European workshop on “Towards Security in Medical Telematics: Legal and Technical Aspects” [10], which attracted about 90 legal, medical, and IT-experts. In September 1994 SEISMED hosted a training course on the key security issues for Health Care Establishments. The comments and critique from all these events was fed back into the validation of the guidelines. On the occasion of the AIM conference “Health in the New Communications Age” at Lisbon, SEISMED presented the prototype SECURE Talk to a wider audience.

Acknowledgements

The authors wish to acknowledge the support of the European Commission's secretariat for Advanced Informatics in Medicine (AIM) which awarded a contract to the SEISMED consortium (A2033) to carry out this work.

References

[1] van Goor JN, Christensen JP (eds.): Advances in Medical Informatics: Results of the AIM Exploratory Action; IOS Press, Amsterdam 1992.

[2] Roger-France FH, Santucci G: Perspectives of Information Processing in Medical Applications: Strategic Issues, Requirements and Options for the European Community; Springer Verlag, Berlin 1991.

[3] Barber B et al.: The Six Safety First Principles of Health Information Systems: A Programme of Implementation - Part 1 Safety and Security; O.A.Jensen et al: Part 2 Convenience and Legal Issues, pp 608 - 619; in O'Moore et al (eds): Medical Informatics Europe 90, Lecture Notes in Medical Informatics No 40, Springer Verlag, Berlin 1990.

[4] Barber B, Vincent R, Scholes M: Worst Case Scenarios: The Legal and Ethical Imperative; in Richards B et al (eds): HC92 Current Perspectives in Healthcare Computing, 1992, British Journal of Healthcare Computing, pp 282 - 288.

[5] European Commission, DG XIII/F AIM (ed): Data Protection and Confidentiality in Health Informatics: Handling Health Data in Europe in the Future, Research and Technology Development on Telematic Systems in Health Care; IOS Press, Amsterdam 1991.

[6] AIM SEISMED, A Secure Environment for Information Systems in Medicine Reference - Project Outline, SCOLL, 2 Ashley Ave, Epsom, UK.

[7] Barber B, Davey J: The Use of the CCTA Risk Analysis and Management Methodology (CRAMM) in Health Information Systems; in Lun KC, Degoulet P, Piemme TE, Rienhoff O (eds.), MEDINFO 92, North Holland, Amsterdam, 1992, pp 1589 - 1593.

[8] NHS Information Management Centre: Basic Information Systems Security, Security and Data Protection Programme, 15 Frederick Road, Birmingham, B15 1JD, UK.

[9] International Journal of Bio-Medical Computing 35 (Suppl. 1) (1994). Also published in Barber B, Bakker AR, Bengtsson S (ed.): Caring for Health Information: Safety, Security and Secrecy; Proceedings of the IMIA Working Conference at Heemskerk, Elsevier Science, Amsterdam 1994.

[10] Barber B, Bleumer G, Louwerse C, Treacher A (eds.): Towards Security in Medical Telematics: Legal and Technical Aspects (preliminary title), The SEISMED Workshop 11th July 1994; IOS Press, Amsterdam 1995 (to appear).

[11] Neumann PG: Computer Related Risks; ACM Press, Addison Wesley, Reading Massachusetts 1995.

[12] Roger-France FH, Gaunt N: The Need for Security — A Clinical View; in [9] 189-194.

[13] Department of Defense Standard: Department of Defense Trusted Computer System Evaluation Criteria; December 1985, DOD 5200.28-STD, Supersedes CSC-STD-001-83, dtd 15 Aug 83, Library No. S225,711.

[14] Canadian System Security Centre; Communications Security Establishment; Government of Canada: The Canadian Trusted Computer Product Evaluation Criteria; April 1992, Version 3.0e.

[15] European Communities - Commission: ITSEC: Information Technology Security Evaluation Criteria; (Provisional Harmonised Criteria, Version 1.2, 28 June 1991) Office for Official Publications of the European Communities, Luxembourg 1991 (ISBN 92-826-3004-8).

[16] Bundesamt für Sicherheit in der Informationstechnik: Common Criteria for Information Technology Security Evaluation; Preliminary Draft, Version 0.9, BSI 6010 CD, 11/1994.

[17] Biskup J, Bleumer G: Reflections on Security of Database and Datatransfer Systems in Health Care; Klaus Brunnstein, Eckart Raubold: Technology and Foundations; IFIP 13th World Computer Congress 94, Volume 2, Elsevier Science, Amsterdam 1994, 549-556.

[18] Bleumer G: Security for Decentralized Health Information Systems; in [9] 139-145.

[19] Council of Europe, Project Group on Data Protection: Draft recommendation on the protection of medical data and draft explanatory memorandom; Strasbourg, 13.10.1994, CJ-PD 894) Misc. 17.

[20] Katsikas S, Gritzalis D: The Need for a Security Policy in Health Care Institutions; in [9] 73-80

[21] AIM SEISMED: Callens S: Health Informatics Deontology Code, Deliverable 28, SP10; ©Katholieke Universiteit Leuven, Belgium, 1994.

[22] AIM SEISMED: Katsikas S: High Level Security Policy for Health Care Establishments, Deliverable 14, SP04; ©University of the Aegean, Greece, 1994.

[23] AIM SEISMED: Callens S: Recommendations for European Health Data Protection Legislation, Deliverable 37, SP10; ©Katholieke Universiteit Leuven, Belgium, 1995.

[24] AIM SEISMED: Davey J: Guideline on IT-Security Risk Analysis —Health Care Management—, Deliverable 25, SP05; ©HEIMDALL Ltd., England, 1995.

[25] AIM SEISMED: Davey J: Guideline on IT-Security Risk Analysis —IT-System End-Users—, Deliverable 25, SP05; ©HEIMDALL Ltd., England, 1995.

[26] AIM SEISMED: Davey J: Guideline on IT-Security Risk Analysis —IT and Security Personnel—, Deliverable 25, SP05; ©HEIMDALL Ltd., England, 1995.

[27] AIM SEISMED: van Dorp H, Dubbeldam J: Guidelines for System Procurement and Development —Health Care Management—, Deliverable 23, 24, SP06; ©BAZIS, The Netherlands, 1995.

[28] AIM SEISMED: van Dorp H, Dubbeldam J: Guidelines for System Development and Design —IT and Security Personnel—, Deliverable 23, 24, SP06; ©BAZIS, The Netherlands, 1995.

[29] AIM SEISMED: van Veenen G: Guidelines on Secure Implementation —Health Care Management—, Deliverable 24, SP06; ©BAZIS, The Netherlands, 1995.

[30] AIM SEISMED: van Veenen G: Guidelines on Secure Implementation —IT and Security Personnel—, Deliverable 24, SP06; ©BAZIS, The Netherlands, 1995.

[31] AIM SEISMED: Pangalos G: Security of Medical Database Systems —Health Care Management—, Deliverable 31, SP07; ©University of Thessaloniki, Greece, 1995.

[32] AIM SEISMED: Pangalos G: Security of Medical Database Systems —IT-System End-Users—, Deliverable 31, SP07; ©University of Thessaloniki, Greece, 1995.

[33] AIM SEISMED: Pangalos G: Security of Medical Database Systems —IT and Security Personnel—, Deliverable 31, SP07; ©University of Thessaloniki, Greece, 1995.

[34] AIM SEISMED: Sanders P: Baseline Security Guidelines for Existing Systems —Health Care Management—, Deliverable 26, SP07; ©University of Plymouth, England, 1994.

[35] AIM SEISMED: Sanders P: Baseline Security Guidelines for Existing Systems —IT-System End-Users—, Deliverable 26, SP07; ©University of Plymouth, England, 1994.

[36] AIM SEISMED: Sanders P: Baseline Security Guidelines for Existing Systems —IT and Security Personnel—, Deliverable 26, SP07; ©University of Plymouth, England, 1994.

[37] AIM SEISMED: Patel A: Guidelines of the Possible Implementation of the Security Menchanisms and Protocols by the Reference Centres —Health Care Management—, Deliverable 27, SP09; ©University College Dublin, Ireland, 1994.

[38] AIM SEISMED: Patel A: Guidelines of the Possible Implementation of the Security Menchanisms and Protocols by the Reference Centres —IT and Security Personnel—, Deliverable 27, SP09; ©University College Dublin, Ireland, 1994.

[39] AIM SEISMED: Bleumer G: Guideline for Cryptographic Mechanisms —Health Care Management—, Deliverable 29, SP08; ©Universität Hildesheim, Germany, 1994.

[40] AIM SEISMED: Bleumer G: Guideline for Cryptographic Mechanisms —IT-System End-Users—, Deliverable 29, SP08; ©Universität Hildesheim, Germany, 1994.

[41] AIM SEISMED: Bleumer G: Technical Recommendations for Cryptographic Mechanisms —IT and Security Personnel—, Deliverable 29, SP08; ©Universität Hildesheim, Germany, 1994.

[42] AIM SEISMED: Louwerse C P, Flikkenschild E L A, Fowler J, Gaunt N: Implementation of RA Results and HLSP Recommendations in Reference Centres, Deliverable 19, SP11; ©AZL/CDIV, The Netherlands, 1995.

[43] AIM SEISMED: Flikkenschild ELA, van der Sluijs P, Fowler J: Reference Centre Report on Implementation of Operational Security, Deliverable 20, SP11; ©AZL/CDIV, The Netherlands, 1995.

[44] AIM SEISMED: Flikkenschild ELA, Louwerse C P, Fowler J: Reference Centre Report on Implemenation of Network Security, Deliverable 22, SP11; ©AZL/CDIV, The Netherlands, 1995.

[45] AIM SEISMED: Flikkenschild ELA, van den Sluijs P, Buis E, Verhage J: SIDERO — A Relational Database Application for Security Practitioners Supporting the Implementation of SEISMED Guidelines in Health Care Institutions; Deliverable 38a, SP14; ©AZL/CDIV, The Netherlands, 1995.

[46] AIM SEISMED: Flikkenschild ELA, Bleumer G: Validation Report Addendum: Getting Started with SEISMED Guidelines; Deliverable 38b, SP14; ©AZL/CDIV, The Netherlands, 1995.

[47] AIM SEISMED: Flikkenschild ELA, Bleumer G: Validation Report Addendum to the Network Security Guidelines; Deliverable 38c, SP14; ©AZL/CDIV, The Netherlands, 1995.

Glossary

SEISMED has approached security from several starting points, which naturally lead to sometimes incompatible use of terms. For example, the legal and the technical community use different speeches and even the technical communities on database security and on network security have not harmonized their language completely. Of course, SEISMED has not overcome all differences but proposes to use security terms according to CEN/TC251/WG6. Other standards to which these definitions comply are given in brackets.

Access Control: The prevention of unauthorised use of a resource, including the preventions of use of a resource in an unauthorised manner. (ISO 7498-2)

Accountability: The property that ensures that the actions of an entity may be traced uniquely to the entity. (ISO 7498-2)

Audit Trail: The historic data and information which are available for examination in order to prove the correctness and integrity with which the agreed security procedures related to a key or transaction(s) have been followed and which allows breaches in security to be detectable.(ISO 8732)

Authentication: Establish the validity of a claimed identity (ISO 7498-2). The authentication information can be transferred to third parties and proves the originator's identity to them.

Availability: The property of (data) being accessible and useable upon demand by an authorised entity. (ISO 7498-2)

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes. (ISO 7498-2)

Corporate Security Policy (→ Security Policy, System Security Policy): The set of laws, rules and practices that regulate how assets including sensitive information are managed, protected and distributed within a user organisation. (European ITSEC)

Cryptographic Key: A parameter used with an algor ithm to validate, authenticate, encrypt, or decrypt a message. (ISO 8732)

Cryptographic System, Cryptosystem: A collection of transformations from plain text into ciphertext and vice versa, the particular transformation(s) to be used being selected by keys. The transformations are normally defined by a mathematical algorithm. (ISO/IEC 9594-8 / CCITT X.509)

(Data) Integrity: The property that data has not been altered or destroyed in an unauthorised manner. (ISO 7498-2)

Digital Signature: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. (ISO 7498-2)

Identification: Establish the validity of a claimed identity. The identification information does not prove the originator's identity to third parties, since the receiver of identification information can have produced that information by himself.

Key Management: The generation, storage, distribution, deletion, archiving and application of (cryptographic) keys in accordance with a security policy. (ISO 7498-2)

Masquerade: The pretence by an entity to be a different entity. (ISO 7498-2)

Password: Confidential aut hentication information, usually composed of a string of characters. (ISO 7498-2)

Physical Security: The measures used to provide physical protection of resources against deliberate and accidental threats. (ISO 74980-2)

Privacy: The right of individuals to control or influence what information related to them may be collected and stored and by whom that information may be disclosed. (ISO 7498-2)

Quality: The totality of features and characteristics of a product, process or service that be ar on its ability to satisfy stated or intended needs. (ISO 9000)

Safety: The expectation that a system does not, under defined conditions, lead to a state in which human life, limb and health, or economics or environment are endangered. (IEC 65A/122)

Security: The combination of confidentiality, integrity and availability. (European ITSEC)

Security Audit: An independent review and examination of systems records and activities in order to test for adequacy of systems controls, to ens ure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures. (ISO 7498-2)

Security Policy (→ Corporate Security Policy, System Security Policy): The set of criteria for the provision of security services. (ISO 7498-2)

System Security Policy (→ Corporate Security Policy, Security Policy): The set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specific system. (European ITSEC)

Threat: A potential violation of security. (ISO 7498-2)