SLOVENSKI STANDARD
SIST-TP CR 14302:2003

01-oktober-2003

Zdravstvena informatika ï Okvirne doloį be o varnostnih zahtevah za naprave, ki niso priključį ene stalno

Health informatics - Framework for security requirements for intermittently connected devices

Ta slovenski standard je istoveten z: CR 14302:2002

ICS:

35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology

SIST-TP CR 14302:2003 **en**

CEN REPORT

RAPPORT CEN

CEN BERICHT

CR 14302

January 2002

ICS

English version

Health informatics - Framework for security requirements for intermittently connected devices

This CEN Report was approved by CEN on 14 December 2001. It has been drawn up by the Technical Committee CEN/TC 251.

CEN members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No. CR 14302:2002 E

CONTENTS

Foreword

This CEN Report was prepared by CEN/TC 251 Health Informatics, the secretariat of which is held by SIS – Swedish Standards Institute.

This work is based on several years of discussions on various documents in CEN/ TC 251/ WG 7 and WG 6 and CEN TC 224/WG 12 . In particular, the work of TC251/PT 7-009 that drafted the ENV 12018 ” Medical Informatics - Identification, Administrative, and common Clinical Data structure for Intermittently Connected Devices used in Health Care (including machine readable cards)” should be acknowledged. Many of the concepts explained in this report are in fact underlying the security objects defined in that standard.

This CEN Report is also based on work carried out within the following CEC projects:

CEC - AIM Eurocards Concerted Action on Extending the use of Patient Data Cards: The Security Report and Assessment of Health Care Professional Card.

CEC - INFOSEC '94 programme on Electronic Signature and Trusted Third Party Services: Trusted Health Information Systems: Part 1. Requirements on Electronic Signature Services and Part 2. Trusted Third Party Services, published by Spri, Swedish Institute for Health Services Development, Stockholm 1995.

CEC – Health Telematics project TrustHealth 1. Deliverable 2.1 Selection of Security Services and Interfaces.

Introduction

Intermittently connected devices such as patient cards may carry important clinical information as well as administrative data of importance to health care delivery. The information regarding an identifiable individual is always sensitive and with clinical data it is particularly important to provide appropriate means to ensure the protection of confidentiality. In addition several other security services must be ensured to protect the patient safety as well as accountability of the professionals responsible for recording data and reading data from intermittently connected devices.

Health care person devices, particularly microprocessor cards, carried by professionals and other persons working in the health care sector, may play an important role in the provision of security for all health information systems for the following core functions; to provide a secure user authentication, to provide a digital signature mechanism and as a means to carry cryptographic keys for confidentiality protection of stored and communicated health care information. The authentication function may serve as a key to protected data on a Patient data card.

1. Scope

This CEN Report is aimed at providing a basis for a planned European Standard on the same subject, work item Security Requirements for Intermittently Connected Devices. The reason for processing this document as a formal CEN Report is that it has been requested as immediate guidance to the current work of CEN TC224/WG12 in its preparation of standards specifying the mechanisms for implementing security requirements in systems using machine readable cards in health care. The scope of this report is also to serve as guidance, without being normative, to the many large projects using cards in health care for both patients, professionals and other persons working in the health care sector, presently under development in Europe.

This report defines a framework of security requirements in systems with intermittently connected devices and discusses requirements for the following security services for ICD-systems:

Data Integrity protection
Data Origin and Entity Authentication
Access Control
Confidentiality protection

The report defines security requirements on the ICD-interchange interface between an application system and an ICD-System. However, the overall security requirements can only be met if certain requirements on the devices themselves are also followed.

Requirements for establishment of secure sessions with various types of ICDs as well as object related security services are defined.

The report particularly defines how access to different types of data on intermittently connected devices could be restricted to different classes of health care persons (professionals and other types of personnel) or to the patients, especially when multinational access should be allowed. The rights to read, add, change and delete must be defined separately.

The security policies proposed should also guarantee the authenticity of identification, administrative and clinical information that may have important implications.

This report gives detailed security requirements for active devices such as microprocessor cards, which are the only possibilities to implement some of the proposed services. The report also gives important advice for passive devices such as magnetic stripe card systems or floppy disks. The major focus is on systems for handling sensitive medical information on devices (mainly cards) held by patients. However, some requirements on ICDs to be used by health care persons (professionals and others) are also given. Detailed protocols for interaction between such devices and general medical information systems for the purpose of secure user identification will be developed within a separate work item.

2. Normative references

This CEN report incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any one of these publications apply to this standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication applies.

ISO 7498-2:1989	Information processing systems - Open systems interconnection Basic reference model - Part 2: Security architecture.
ISO/IEC 9594-8:1990	Information technology - Open Systems interconnection: The Directory - Part 8: Authentication framework.
ISO/IEC 9798-1:1991	Information technology - Security techniques - Entity authentication mechanisms - Part 1: General model
ISO/IEC 9796: 1991	Information technology - Open systems interconnection - Digital signature scheme giving message recovery
ENV 12388: 1996	Medical Informatics – Algorithm for Digital Signature Services
ENV 12018: 1996	Medical Informatics - Identification, Administrative, and common Clinical Data structure for Intermittently Connected Devices used in Health Care (including machine readable cards)

3. Definitions

This CEN Report does not introduce any new normative definitions. Please refer to the Glossary in the end of this document for definitions of commonly used security terms.

4. The variety of systems for intermittently connected devices

Intermittently connected devices may be used for many different applications and the security issues will vary accordingly. Patient data cards and cards held by health care professionals and other types of personnel have attracted particular attention in recent years. For the purpose of this report we are pointing at some of the differences with regard to administrative and medical uses of patient data cards. However, it is frequently impracticable to draw a sharp line between these applications. This report is an analysis of the security issues that arise with patient data cards and possible solutions. With a few exceptions it does not give recommendations that apply to all patient card systems. The flexible introduction of standardised security countermeasures based on the needs of the specific application is emphasised. The combination of medical data with non health care related applications have been suggested but the security problems involved makes it very difficult to implement.

Aspect	Administrative use	Medical use
Overall objective	Facilitating administrative procedures	Improving the quality of care
Typical data	Identification data Insurance details	Essential medical facts: diagnoses, drug therapy, lab results, hypersensitivity, etc
Main security objective	Data Integrity, Securing Payment	Protection of Confidentiality and Data Integrity

The International use

The underlying vision is that patient cards issued in one country should be possible to use not only in all health care institutions within one country, but throughout Europe. Such usage requires a common view related to the ethical issues concerning the transfer of personal data between health care professionals both at a national and international level. It is also necessary to harmonise the technology used to protect the appropriate security objectives. The details of the technologies require standardization that is on its way through the European standardization committee, CEN.

It may be possible to some extent to have different authorisation rules in different areas within the same basic technical framework and yet provide some degree of interoperability. Whereas it should be possible to restrict the use to a country or even a limited group of users the goal for the patient is usually to provide maximum mobility of the information within the bounds of confidentiality principles to aid and improve on the health care delivery process.

A basic principle on the international use of the card is the following:

The card issuer in a country should always be able to decide what can be done with a particular card, wherever that card is used. In addition, the person that records data on a card should know whom and under what circumstances could somebody gain access to that data.

In case of a conflict with local laws and practices as may for instance occur when trying to access a patient card from a different nation, it should be ensured that the proscriptions of the issuing nation are enforced. This could mean that when a patient with a card from a country not allowing unconditional access to the data by the patient, comes to a country with different laws, direct access to such data by the patient is prevented. Another example may be when erasure of data is possible according to the rules of the issuing country, a health care provider in another country where this would not be allowed could decide not to enter any information to such a card.

5. The major actors involved and their interests

The Patient must be in the centre

It must be emphasised that a patient card system should be in the interest of the patient. A card with essential information for health care controlled by the patients may be an important factor to support the free movement of people in Europe.

This consideration is not only relevant when medical data is included in the card but also when a card system is used for administration only. This is partly based on the practical fact that a device like a card is likely to disappear if the carrying person does not feel that its presentation will be of benefit to him.

The perspective of the patient will be very important in this report and we will come back to this aspect many times. It is important to consider however, that the patient, the customer in market driven health care, is frequently in a very weak position. Patients are usually old, frequently very old, and the disease may make it even worse for the patient to fight for his/her interests in relation to information systems and patient cards.

Public interest bodies - governments

Because the patient is a weak actor in health care, the governments - national or regional - usually make a lot of effort to protect the patient in relation to other actors in the health care market. They do this through legislation but there are also a number of other regulatory instruments and control functions. It is natural that governments in many countries will take a deep interest in the use of patient data cards.

Paying bodies

On the other side we have the interests of the organisation that pays the bill for health care. In most European countries it is not the patient himself, who pays directly, but it is an insurance company or similar institution, private or as a part of a public health care system.

The Health Care Provider

A fourth party that may have interests to protect in a patient card system, is the health care provider, either as an individual or institution which may be a commercial or public service body who may have a commercial interest in the form of the value of the data contained in the medical record. Such an entity may wish to conceal or not communicate certain patient related information, both administrative and clinical from potential competitors. Another thing to consider is the necessity of a card system to provide sufficient information to allow justice to be made in case of malpractice litigation. In this paper, health care providers will have a wide definition including entities such as pharmacies, patient transport (ambulances) etc.

Health Care Persons

In addition to the interests of the health care provider *institution* the people who work there have interests to protect in relation to the security of a patient card system. These persons are in this document henceforth referred to as Health Care Persons. This term will include various more or less well defined professional groups, such as physicians, pharmacists etc. but also other types of personnel such as administrative clerks etc.

The Card Issuer

The issuer of a patient card may be of different types, a paying institution, a health care provider, perhaps a national body or an organisation that is primarily just a card issuer. The issuing process normally includes the setting of the rules that will determine the usage of the cards, memory allocation and security functions. This freedom may however be limited by legislation. The actual process of physical personalisation of the cards may well be carried out by another entity under a contract from the issuer.

6. Interacting with cards

Various entities that interact with patient cards may perform one of the following interactions:

Issuing of cards

This will include setting the rules for access including memory allocation. This will usually also include the addition of a basic data set at least identifying the cardholder. By issuer we mean the entity that is responsible for the card issuing, the actual physical personalisation process may be carried out by another entity under a contract of the issuer.

Reading data

This may include reading of data that was previously added by the same entity or the reading of information added by another provider.

Adding data

Three types may be identified:

a) Data added that is intended to be read at a later time by the same entity
b) Data directed towards a certain other, perhaps named entity -ies
c) Undirected data, available to many potential users of the information in the future.

Erasing

An important difference is if an entity will attempt to erase data that was added by another entity or if it is handling its "own" data. A special instance of this occurs when the data is in the form of a directed ”message” aimed at a given recipient and the data has no further use after having reached its destination. In this case it may be natural to allow erasure if the medium so permits.

Erasing may be done for three reasons that has different security requirements:

a) Erasing data that is no longer relevant to facilitate finding of relevant information.
b) Erasing data that the patient will no longer agree to have on the card for further spread.
c) Erasing data to free space for new information with a higher priority.

Please note that under some legislations, erasure of information on patient held data cards may not be allowed in any circumstance.

Modifying data

Modifying may technically be regarded as a three-stage process, reading, erasure and then adding of new information. It is technically possible that a card or external system may allow the information to be presented as changed without actually erasing the old data, thereby preserving an audit trail with respect to the information.

Allocating new space

This may with some types of cards be a separate task, which might limit the availability of memory for other applications or entities.

7. Ethical and legal considerations

7.1 Ethical statements

Dealing with health is one of the most sensitive matters where ethical principles established through centuries of professional care are very important. In fact, they date at least back to Hippocrate in the year of 400 BC The Hippocratic oath is still part of the basic principles of most medical professional societies in Europe. One of the most important principles also for patient card systems is the confidentiality statement in free translation:

> ***The health care professional must not reveal the health status or other patient related facts collected during the care process to others***

The way this is usually interpreted in modern health care, with a group of staff caring for one patient, is that it is important to take every precaution to avoid that information from health records are accidentally released to people who do not have a caring responsibility for the patient.

How the group of carers is defined and what information is needed to carry out the work is a difficult question and shows considerable variations in different situations and in different European countries. A particularly difficult problem is to define the circumstances under which information about a patient should be given to another health care provider institution. In many cases the consent of the patient is required for such transfer.

On the other hand:

> ***It is in the interest of the patient, in most cases, that medical facts from their health record can be made available promptly and efficiently to all health care providers that will treat him. Such a principle persists even if the patient is not able to actively give their informed consent.***

Without patient data cards or functional standardized data communication, this is rarely the case, resulting in bad quality of care.

Another basically ethical statement (but in some countries also legislated) is the notion that:

> ***The patient should have adequate information about his health condition in order to be able to participate in the decision process regarding his treatment plan.***

This may be interpreted in various ways but in most cases, this basic principle will be valid:

> ***The patient should be in some control of the <u>medical</u> information on the card.***

This means:

- The right to know what is on the card
- The right to exclude certain information from being entered into the card
- The right not to reveal all or any information from the card to a health care provider
- The right to have removed a specific data entry on the card

All of these elements have to be defined separately and are only included here to illustrate some of the issues. There may be exceptions to the above principles in the case of specific legislations. In some countries medical data on a card may be regarded as any medical record and as such it may not be