National Standards Authority of Ireland

IRISH STANDARD

I.S. CR 14302:2002

ICS 35.240.80

National Standards
Authority of Ireland
Dublin 9
Ireland

Tel (01) 807 3800
Tel: (01) 807 3838

HEALTH INFORMATICS - FRAMEWORK FOR SECURITY REQUIREMENTS FOR INTERMITTENTLY CONNECTED DEVICES

This Irish Standard was published under the authority of the National Standards Authority of Ireland and comes into effect on March 8. 2002

Price Code J

Údarás um Chaighdeáin Náisiúnta na hÉireann

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
EUROPAISCHES KOMITEE FUR 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.