Irish Standard
I.S. ENV 13608-2:2000

Health informatics - Security for healthcare communication - Part 2: Secure data objects

I.S. ENV 13608-2:2000

Incorporating amendments/corrigenda issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard – national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation - recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces:

This document is based on:
ENV 13608-2:2000

Published:
24 May, 2000

This document was published
under the authority of the NSAI
and comes into effect on:
22 September, 2011

ICS number:
35.040
35.240.80

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

I.S. ENV 13608-2:2000

EUROPEAN PRESTANDARD

PRÉNORME EUROPÉENNE

EUROPÄISCHE VORNORM

ENV 13608-2

May 2000

ICS 35.040; 35.240.80

English version

Health informatics - Security for healthcare communication - Part 2: Secure data objects

This European Prestandard (ENV) was approved by CEN on 29 July 1999 as a prospective standard for provisional application.

The period of validity of this ENV is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the ENV can be converted into a European Standard.

CEN members are required to announce the existence of this ENV in the same way as for an EN and to make the ENV available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the ENV) until the final decision about the possible conversion of the ENV into an EN is reached.

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

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

Central Secretariat: rue de Stassart, 36 B-1050 Brussels

Ref. No. ENV 13608-2:2000 E

Contents

Foreword

This European Prestandard has been prepared by Technical Committee CEN/TC 251 "Health informatics", the secretariat of which is held by SIS.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this European Prestandard: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

This multipart standard consists of the following parts, under the general title *Security for Healthcare Communication (SEC-COM):*

- Part 1: Concepts and Terminology
- Part 2: Secure Data Objects
- Part 3: Secure Data Channels

This standard is designed to meet the demands of the Technical Report CEN/TC251/N98-110 Health Informatics - *Framework for security protection of health care communication*.

This standard was drafted using the conventions of the ISO/IEC directive Part 3.

The draft standard prENV 13608-2 contained in normative annexes A and B copies of IETF drafts that have been approved as RFC 2633 and RFC 2630 respectively after the approval vote but before this prestandard is published. These are now normative references available through IETF and not included in this publication. The remaining annexes are all informative are renumbered accordingly.

Introduction

The use of data processing and telecommunications in health care must be accompanied by appropriate security measures to ensure data confidentiality and integrity in compliance with the legal framework, protecting patients as well as professional accountability and organizational assets. In addition, availability aspects are important to consider in many systems.

In that sense, the SEC-COM series of standards has the intention of explaining and detailing to the healthcare end user the different alternatives they have to cope with in terms of security measures that might be implemented to fulfil their security needs and obligations. Incorporated within this is the standardization of some elements related to the information communication process where they fall within the security domain.

In the continuity of the *Framework for security protection of health care communication* (CEN/TC251/N98-110), hereafter denoted *the Framework*, whose CEN Report aimed at promoting a better understanding of the security issues in relations to the healthcare IT-communication, this European Prestandard shall aid in producing systems to enable healthcare professionals and applications to communicate and interact securely and therefore safely, legitimately, lawfully and precisely.

The SEC-COM series of standards are key communication security standards that can be generically applied to a wide range of communication protocols and information system applications relevant to healthcare, though they are neither complete nor exhaustive in that respect. These standards must be defined within the context and scenarios defined by TC251 Work programme, in which the messaging paradigm for information system interaction is *one* of the essentials, as was reflected by the *Framework*.

This Part 2 of the European Prestandard on Security for Healthcare Communication describes how to secure arbitrary octet strings that may be used in European healthcare. An arbitrary octet string might for example be an EDIFACT message, a patient record, etc. Securing within the concepts contained within this European prestandard include the preservation of data integrity, the preservation of confidentiality and accountability in terms of authentication of both communicating parties.

This standard does not specify methods related to availability, storage or transportation of data, key certificates or other infra-structural issues, nor does it cover application security aspects such as user authentication.

NOTE This standard defines a methodology to secure the octet string to allow it to be transported securely over insecure networks, independent of the underlying transportation system, e.g. e-mail or EDI system. The standard encompasses mechanisms for encryption and digital signature, and will allow that these mechanisms are used independently.

Health informatics - Security for healthcare communication - Part 2: Secure data objects

1 Scope

This European Pre-standard defines a standard way of securing healthcare objects. The objects are secured in such a way that they can be transported over open, unsecured networks, or stored in open unsecured repositories. An application is able to decide whether to apply any combination of encryption and digital signature to an object.
In general this European Pre-standard does not consider the contents of the objects, but can be applied to any octet string.

This European Pre-standard is based on existing security standards.

This European Pre-standard does not consider how the actual security is applied to the objects. A security infrastructure is assumed, which is used for performing the actual security operations.

2 Normative references

ISO 8824	Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1) (Version 2 1991-04-24)
IETF RFC 2630	Internet Engineering Task Force: Cryptographic Message Syntax (CMS)
IETF RFC 2633	Internet Engineering Task Force: S/MIME version 3 Message Specification
ISO 8824-1:1995	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1) - Part 1: Specification of the base notation
PKCS#7	Cryptographic Message Syntax Version 1.5, RFC 2315
MIXER-BPT	Mapping between CCIT X.400 and RFC-822/MIME Message Bodies, RFC-2157
CCIT X.400	ITU Data Communication Networks: Message Handling Systems X.400

3 Terms and definitions

3.1
accountability

The property that ensures that the actions of an entity may be traced uniquely to the entity [ISO 7498-2]

3.2
asymmetric cryptographic algorithm

An algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ [ISO 10181-1]

3.3
authentication

Process of reliably identifying security subjects by securely associating an identifier and its authenticator.
See also data origin authentication and peer entity authentication [ISO 7498-2]

3.4
availability

Property of being accessible and useable upon demand by an authorised entity [ISO 7498-2]

3.5
certificate revocation

Act of removing any reliable link between a certificate and its related owner (or security subject owner), because the certificate is not trusted any more whereas it is unexpired