SLOVENSKI STANDARD
SIST ENV 13608-2:2003

01-oktober-2003

Zdravstvena informatika – Varnost pri komuniciranju v zdravstvenem varstvu – 2. del: Varni podatkovni objekti

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

Ta slovenski standard je istoveten z: **ENV 13608-2:2000**

ICS:

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

SIST ENV 13608-2:2003 **en**

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

3.6
certificate holder

An entity that is named as the subject of a valid certificate

3.7
certificate user

An entity that needs to know, with certainty, the public key of another entity [ISO 9594-8]

3.8
certificate verification

Verifying that a certificate is authentic

3.9
certification

Use of digital signature to make transferable statement about beliefs of identity, or statements about delegation of authority

3.10
certification authority

An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys [ISO 9594-8]

3.11
ciphertext

Data produced through the use of encipherment. The semantic content of the resulting data is not available [ISO 7498-2]

3.12
ciphersuite

An encoding for the set of bulk data cipher, message digest function, digital signature algorithm and key exchange algorithm used within the negotiation phase of TLS

3.13
communication protection profile
CPP

A statement of systematic translation form communication security needs to technological concepts

3.14
communication security

Security of security objects communicated between security subjects

3.15
confidentiality

The property that information is not made available or disclosed to unauthorised individuals, entities, or processes [ISO 7498-2]

3.16
cryptography

The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use [ISO 7498-2]

3.17
cryptographic algorithm
cipher
an algorithm used to transform data to hide its information content which is used in the process of encryption (see 3.22)

3.18
data integrity
The property that data has not been altered or destroyed in an unauthorised manner [ISO 7498-2]

3.19
data origin authentication
The corroboration that the source of data received is as claimed [ISO 7498-2]

3.20
decryption
decipherment
Process of making encrypted data reappear in its original unencrypted form. The reversal of a corresponding reversible encipherment

3.21
digital signature
Data appended to, or a cryptographic transformation (see cryptography) 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]

3.22
encryption
encipherment
The cryptographic transformation of data (see cryptography) to produce ciphertext [ISO 7498-2]

3.23
hash function
A (mathematical) function that maps values from a (possibly very) large set of values into a smaller range of values [ISO 10181-1]

3.24
integrity
The property of being unmodified by any kind of unauthorised security subject

3.25
key
A sequence of symbols that controls the operations of encipherment and decipherment [ISO 7498-2]

3.26
key distribution
Process of publishing, or transferring to other security subjects a cryptographic key

3.27
key exchange algorithm
An algorithm used to derive a shared secret over an open communications channel

3.28
key generation

Process of creating a cryptographic key

3.29
key management

The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy [ISO 7498-2]

3.30
message recovery

Process of a third party decrypting an encrypted message

3.31
one-way function

A (mathematical) function that is easy to compute but, when knowing a result, it is computationally infeasible to find any of the values that may have been supplied to obtain it [ISO 10181-1]

3.32
one-way hash function

A (mathematical) function that is both a one-way function and a hash function [ISO 10181-1]

3.33
peer entity authentication

The corroboration that a peer entity in an association is the one claimed [ISO 7498-2]

3.34
plaintext

Intelligible data, the semantic content of which is available

3.35
private key

A key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity) [ISO 10181-1]

3.36
public key

A key that is used with an asymmetric cryptographic algorithm and that can be made publicly available [ISO 10181-1]

3.37
secret key

Key which is kept secure and only disclosed to parties intended to have access to data protected by it

3.38
security

The combination of availability, confidentiality, integrity and accountability

NOTE From an end-user perspective this encompasses auditability thereby constituting a guarantee that data items and, more generally any kind of security object, has not been altered, modified, disclosed, or with held by any kind of security subject in an unauthorized manner with respect to the security policy.

3.39
security object
object

A passive entity that contains or receives information [ITSEC]

NOTE Access to an object potentially implies access to the information it contains.

EXAMPLE Typical objects in the healthcare domain are: medical records, or files containing medical data.

3.40
security policy

The set of laws, rules, and practices that regulate how an organisation manages, protects, and distributes sensitive information [TCSEC]

3.41
security protocol

A formal detailed specification describing the implementation of a set of security functions

3.42
security procedure

A specification for a protocol designed to implement a security policy

3.43
security service

A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers [ISO 7498-2]

3.44
security subject
subject

An active entity, generally in the form of a person, process or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair [TCSEC]

NOTE According to the Object-Oriented paradigm, a subject is usually called a principal.

3.45
user certificate
public key certificate
certificate

The public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it [ISO 9594-8]

Note such kinds of certificates might be dedicated, on the basis of public key certification techniques, to attributes (i.e., attribute certificate), or digital signatures (i.e., signature certificate).