SIST

SLOVENSKI STANDARD
SIST ENV 13608-3:2003

01-oktober-2003

Zdravstvena informatika – Varnost komuniciranja v zdravstvenem varstvu – 3. del: Varni podatkovni kanali

Health informatics - Security for healthcare communication - Part 3: Secure data channels

Ta slovenski standard je istoveten z: ENV 13608-3:2000

ICS:

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

SIST ENV 13608-3:2003 en

EUROPEAN PRESTANDARD

PRÉNORME EUROPÉENNE

EUROPÄISCHE VORNORM

ENV 13608-3

May 2000

ICS

English version

Health informatics - Security for healthcare communication - Part 3: Secure data channels

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 13608-3:2000 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.

All annexes are informative.

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 health 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 the TC251 work programme, in which the messaging paradigm for information system interaction is *one* of the essentials, as it was reflected by the *Framework (*Framework for security -protection of health care communication.)

Secure Data Channel

This part 3 of the European Prestandard on Security for Healthcare Communication describes how to securely communicate arbitrary octet streams by means of a secure data channel communication protocol.

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

A secure data channel is defined for the purposes of this standard as a reliable communication protocol that implements the following security services:

1. authentication of communicating entities prior to the communication of any other data preservation of data integrity
2. preservation of confidentiality of the communicated data.

A secure data channel protocol operates in two distinct phases which, however, may be repeated:

1. negotiation phase: authentication of communicating entities (e.g. exchange of certificates), negotiation of the cipher suite to be used, derivation of a shared secret using a key exchange algorithm
2. communication phase: transmission of user data encrypted according to the negotiated cipher suite.

In addition the secure data channel can be closed by either party when it is no longer required.

The concept of a secure data channel can be best understood by looking at it's properties, especially in comparison with the properties of a secure data object (prENV 13608-2, part 2 of this European Prestandard):

1. Interactivity: the negotiation phase allows the communicating entities to interactively agree upon a cipher suite that meets both parties' security policies for the communication scenario in question (e.g. national vs. international communication). If the cipher suite negotiation is unsuccessful, no communication session is established.
2. Transience: the secure data channel, being part of a layered communication protocol, receives and delivers unsecured user data from and back to the calling layer. The encrypted representation of the data is transient (e.g. available only during transmission) and unavailable to the calling layer (e.g. application).
3. Performance: after the establishment of the cipher suite and shared secret during the negotiation phase, there is no need to use the computationally resource intensive asymmetric cryptographic algorithms during the communication phase. On the other hand, because of the transience of the encrypted representation of the data, encryption must be performed during the communication process and cannot be pre-computed off-line.
4. Forward secrecy: can be easily implemented as part of the key exchange protocol.
5. Completeness: since the authentication of the communicating entities (e.g. certificate exchange) is part of the protocol, no additional out-of-band communication (e.g. look-up of certificates in a trusted directory) is required to use the secure data channel, except if certificate revocation lists are used.
6. Transparency: a secure data channel can be implemented such that it's upper service access point resembles it's lower service access point (e.g. TCP/IP socket interface). This allows the easy addition of security services to existing non-security-aware systems and protocols by integrating the secure data channel as an additional layer in the communication protocol stack. A well-known example for this approach is "Secure HTTP" (HTTP over SSL3).

The IETF Transport Layer Security (TLS) specification is a description of how to provide a secure data channel. Although TLS is an IETF specification, it is not limited to TCP/IP. TLS only requires the presence of a reliable transmission protocol. This means that "TLS over OSI" would be possible if desired. This European Prestandard defines a set of profiles used within TLS for use within healthcare communication over secure data channels.

Health informatics - Security for healthcare communication - Part 3: Secure data channels

1 Scope

This European Prestandard specifies services and methods for securing interactive communications used within healthcare.

Interactive communications are defined for the purposes of this standard as scenarios where both systems are online and in bi-directional communication simultaneously. Securing in this European Prestandard includes the preservation of data integrity, the preservation of confidentiality with respect to the data being communicated, and accountability in terms of authentication of one or both communicating parties.

NOTE NOTE Examples of interactive communication are the download of HTML content over the Internet, a DICOM communication, or remote login to a computer.

This European Prestandard does not specify methods related to availability of the interactive communication, certification and certificate management and key management. Neither does this European Prestandard specify a mechanism for concealing that a communication session is in progress. This European Prestandard does not specify the methods or services required to secure the communicating systems themselves.

2 Normative references

This European Prestandard 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 of these publications apply to this European Prestandard only when incorporated in it by amendment or revision. For undated references, the latest edition of the publication referred to applies.

ISO 7498-2	Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture
ISO 8824	Information technology - Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1) (Version 2 1991-04-24).
ISO 9594-8	Information technology – Open Systems Interconnection – The Directory: Authentication framework
ISO 10181-1	Information technology - Open Systems Interconnection – Security frameworks for open systems: Overview.
RFC 2246	Internet Engineering Task Force: The TLS (Transport Layer Security) Protocol, RFC 2246

3 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
forward secrecy

Technique of ensuring that the communicated data is only decipherable for a limited time span by the communicating parties.

NOTE After that time the communicating parties typically achieve forward secrecy by destroying cryptographic keys. This prevents an attacker from coercing the communicating parties into decrypting old ciphertext.

3.24
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]

3.25
integrity

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

3.26
key

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

3.27
key distribution

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

3.28
key exchange algorithm

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

3.29
key generation

Process of creating a cryptographic key

3.30
key management

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

3.31
message recovery

Process of a third party decrypting an encrypted message

3.32
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]

3.33
one-way hash function

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

3.34
peer entity authentication

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

3.35
plaintext

Intelligible data, the semantic content of which is available

3.36
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]

3.37
public key

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

3.38
secret key

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

3.39
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.

3.40
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.

3.41
security policy

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