National Standards Authority of Ireland

IRISH STANDARD

ENV 13608-3:2000

ICS 35.040
35 240 80

National Standards
Authority of Ireland
Dublin 9

Tel (01) 807 3800
T[illegible] (01) 807 38[illegible]

HEALTH INFORMATICS - SECURITY FOR HEALTHCARE COMMUNICATION - PART 3: SECURE DATA CHANNELS

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

Price Code H

Údarás um Chaighdeáin Náisiúnta na hÉireann

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
EUROPAISCHES KOMITEE FUR NORMUNG

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

Ref. No. ENV 13608-3:2000 E

Contents

Foreword

Thıs 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.