NSAI
Standards

Irish Standard
I.S. ENV 13608-1:2000

Health informatics - Security for healthcare communication - Part 1: Concepts and terminology

I.S. ENV 13608-1:2000

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 13608-1:2000

Published:
24 May, 2000

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

ICS number:
01.040.35
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

EUROPEAN PRESTANDARD

PRÉNORME EUROPÉENNE

EUROPÄISCHE VORNORM

ENV 13608-1

May 2000

ICS 01.040.35; 35.040; 35.240.80

English version

Health informatics - Security for healthcare communication - Part 1: Concepts and terminology

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 13608-1:2000 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

This SEC-COM standard series on Security for healthcare communication can be 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.

Part 1 – Concepts and Terminology – reflects a user-requirements driven approach that provides a methodology for the analysis of the relation between 1) user needs and 2) a technological solution. It begins with a standardised way of expressing user needs, continues through technology-oriented successive refinements of the corresponding required security solutions and ends with a standard-oriented map of the corresponding recommended security solutions. Such a method can be utilised in many ways, out of which two important usages are:

1. as a common tool for breaking down user needs into technological solutions, through a process/journey of close collaboration between users and security experts, and
2. through using this common method in the standardization process, establishing a link between a defined set of user needs and a technological standard, a link that carries an *a priori* assurance on the effectiveness of the technological standards in terms of complying with the user needs. Such an *a priori* assurance will be of special value for the user that do not want to exercise the method in detail on his own, but merely want to *benefit from an established link* between a set of user needs that he/she can recognise, and the existence of an implementation standard.

Readers without a background in communications security are referred to Annex L.

The methodology is organised by means of a matrix, and the path through this matrix from the user needs to a technological solution may be viewed as the standard for the specification of a Communication Protection Profile (CPP), according to CEN/TC251/N98-110.

It is of paramount importance for the understanding of this methodology to recognise that it comprises a journey from user needs to detailed technological specifications, and that several distinct perspectives and contexts are undertaken along this journey. In particular, it is important to recognise that commonly used (already existing, e.g. ISO) standards are comparable to only a subset of the total number of contexts defined by the method. E.g. it has been necessary to introduce the concept of *auditability* for the *user need context*, because the more commonly used notion of *accountability* is perceived to have a more *limited* and *technical constitution*.

Different user views will imply different patterns of use of the matrix. For standardization purposes (to constitute a valid CPP), the matrix must be filled out in detail (however only in those parts that are applicable for a selection of user needs). This process provides some level of *assurance* that the actual technological solution is an *effective* representation of the user needs defined in the actual CPP. The method itself does not specify in detail how each specific cell of the matrix shall appear. However, Annexes B-J provide examples that may be viewed as guidelines.

Part 1 offers a set of different *views* or *journeys* through the successive refinement from user need to technological solution. The security journey on the most detailed level is a *combination* of :

1. top-down approach, by allowing for a systematic translation from a common policy expression, down to technological choices and options;
2. bottom-up approach, by being focused on utilisation of existing, commercial technologies.

Hence, the CPP concept must not be understood as a forced (one-way) development *from* user needs *to* technological solution, but merely as a (standardised) statement that gives evidential indication that a specific technological standard, is an *effective and reasonable fulfilment* of a specific set of user needs.

Hence, the normative function of Part 1 can be summarised as:

1. standardising the way of expressing a communication security policy;
2. standardising the steps of successive refinements down to the technology level, in order to provide a minimum level of assurance[1].

The benefit for a end-user is that he can look for a CPP that matches his demand for:

a. a matching set of user needs;
b. a technological context (e.g. EDI);

and successively identifies:

c. a named implementation standard (e.g. Part 2 or 3 of this Prestandard).

The user will then be assured that the standardization «rubber stamp» implicitly gives him some assurance that a product meeting the implementation standard effectively meets his user needs. Alternatively, if such a standard is not found, he/she can use the method in cooperation with security experts, to constitute a basis from which can be identified the needs and their effective solutions[2].

Figure 1 below depicts how the matrix is used methodologically to constitute relations between user needs, technological contexts and implementation standards.

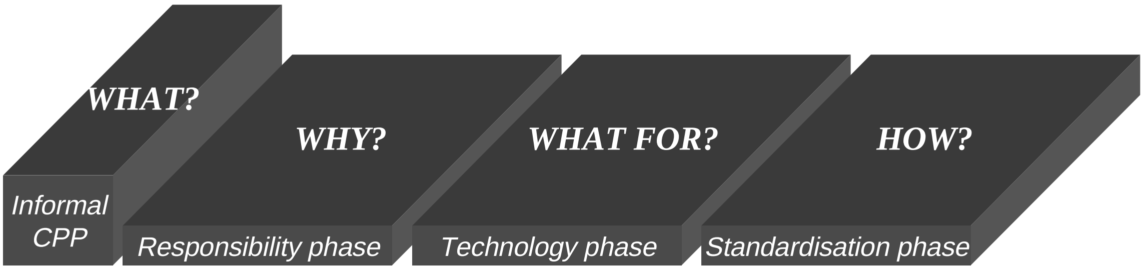

Figure 1 - The Security Policy Bridging phases

Parts 2 and 3 are examples of implementation standards that have a CPP counterpart, as they both are described in terms of Part 1 requirements (in Annex B and C). Both are based on rather simplistic technological contexts, however with a wide installed base in healthcare and with a large potential for future use. Both of them are based on commercial technologies with an existing product portfolio.

[1] The actual level of assurance achieved is not comparable to what can be achieved through a security evaluation process, cfr Annex K.

[2] ultimately with the potential of constituting a basis for bridging his/her communications security policy with those of communication counterparts.

The method prescribed by Part 1is however open in the sense that other pairs of CPP-standard can be developed in the future – e.g. based on other technological concepts such as middleware, WWW-based systems etc.

In order to provide external coherence:

- Annex A provides some examples and illustrations of the usage of this SEC-COM part 1 in terms of general security concepts, with a refined proposal for the auditability property,
- Annexes D to J indicate what a selection of *other* security standards actually can currently offer in regard of the SEC-COM method,
- In Annex K, the relation between the assurance gained through the method, and the assurance gained in a security evaluation based on Common Criteria, is discussed,
- Annex L gives some tutorial on the introduction to cryptography used for communication security.

The CPP approach based on Part 1 can however have wider implications than described so far. However without normative implications in this standard, it is emphasised that the CPP approach may also facilitate (end-system's) *security policy bridging*, which requires a "standardised" description of the embodiment of the site security policy. In the simplest case, the Part 1 way of expressing a (communication) security policy may be a (informal) basis for deciding whether to communicate or not. Moreover, the systematic refinement of a (communication) security policy down to a more technical level constitutes the basis for a more automatic and precise decision process (semiformal). Such a process thus consists of three different steps (also illustrated in the figure below):

i. The first step is the *Terminology Linking* one, ensuring that any communicating entity will be able to use and understand a *common* security policy language,

ii. The second step is the *Policy Matching* one, ensuring that any communicating entity will be able to compare and match his own communication security policy with any peer entity's communication security policy,

iii. The third step is the *Policy Negotiation* one, ensuring that any communicating entity will be able to adapt his own communication security policy in order to be able to adopt a common communication security policy (common in that it is shared by his communication peer entities).

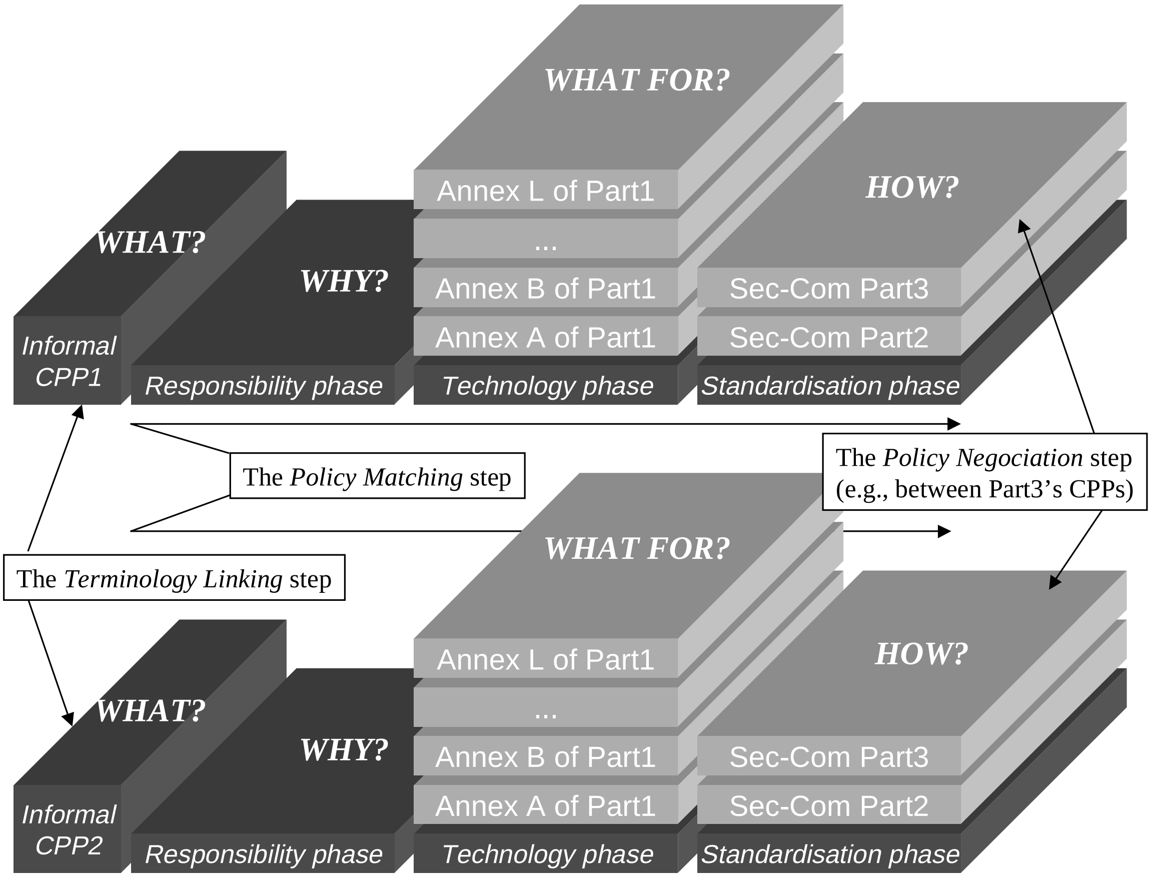

Figure 2 - The Security Policy Bridging steps

Health informatics - Security for healthcare communication - Part 1: Concepts and terminology

1 Scope

This European Prestandard specifies a methodology for defining, expressing and selecting a communication protection profile (CPP) specification, and thus provides:

1. a standard way of expressing healthcare user security needs in relation to communication
2. a standard method of successive refinement of policy statements, hereby helping to identify standardised security implementation specification that can be utilised to meet these security needs.

Security aspects contained within the communication protection profile include integrity, confidentiality, and availability, and also auditability.

This methodology shall thus serve the purpose of being a tool for:

A. the end-user in collaboration with security experts, while seeking effective solutions for relevant and powerful healthcare communication security needs;

B. the standardization process in which trustworthy links between 1) actual selections of such user needs and 2) technological standards, are established.

SAI GLOBAL