SLOVENSKI STANDARD
SIST-TP CR 14301:2003

01-oktober-2003

Zdravstvena informatika - Okvirne dolo ̣ be o zag ̣ l iti podatkov pri njihovi izmenjavi v zdravstvenem varstvu

Health informatics - Framework for security protection of healthcare communication

Ta slovenski standard je istoveten z: **CR 14301:2002**

ICS:

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

SIST-TP CR 14301:2003 **en**

CEN REPORT

RAPPORT CEN

CEN BERICHT

CR 14301

January 2002

ICS

English version

Health informatics - Framework for security protection of healthcare communication

This CEN Report was approved by CEN on 14 December 2001. It has been drawn up by the Technical Committee CEN/TC 251.

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

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

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No. CR 14301:2002 E

CONTENTS

Foreword

This informative CEN report was produced by CEN/TC 251, the secretariat of which is held by SIS, under work item 251 094. It covers the first step of work that will lead to a European Standard *entitled Health informatics - Security for health care communication.*

Introduction

The use of data processing and telecommunications in health care must be accompanied by appropriate security measures to ensure data accountability, confidentiality, integrity and availability in compliance with the legal framework, thus protecting patients as well as professional accountability and organisational assets.
Healthcare information technology (IT)-systems are no longer isolated systems. Although there still exist many technical obstacles to common practical solutions, data communication is used more and more for a variety of purposes within and between health care establishments. The electronic communication capabilities in current and emerging technologies requires that the concept of *healthcare communication security* embody not only the secure communication of data from A to B, but also supervision and guidance of the information flow, co-ordination of security policies, and the safe use of commercial, multi-purpose data networks. Not at least, the EU Directive on privacy enforces this.

1 Scope

This CEN Report aims at promoting a better understanding of the security issues in relation to health care (HC) IT-communication, to point at already existing applicable International and European standards.

The notion of a framework used in this report does *not* embody functional security models or specifications that constitute a basis for implementation of systems. This framework comprises identification and discussion of relevant issues, indicating other related standardisation work in this area, and indicating the need for specific healthcare standards in the field, to be followed up in this work item by the planned project team.

The framework can be used by the project team in order to prescribe security functionality in a set of communication scenarios, and also to establish appropriate (*effectiveness) assurances* as an integrated part of its standardisation work. This notion of (HC) effectiveness assurance shall be founded on existing and standardised terms and concepts, but shall be specifically aimed at providing a bridge between health care specific needs, and the utilisation of commercial, existing standards and technologies, preferably with an existing product portfolio.

The framework will pay attention to the currents *trends of user demands,* ranging from e.g. the classical EDI, to *shared care concepts*, but it will not mandate a total technological shift of focus that is deviating from the existing TC251 work plan. The basic assumption is that the shared care paradigm can be implemented not only with the most ambitious technologies, but *also* in conjunction with existing technologies, e.g EDI.

However, the framework is aimed to be relevant both in view of existing and upcoming technological concepts. An important requisite is hence that the framework captures the issue of coordination or “bridging” of security policies at the sending and receiving side.

In relation to the OSI model of communication, special emphasis will be put on the upper layers.

2 Informative references

This CEN Report incorporates by dated or undated reference, provisions from other publications. These 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 one of these publications apply to this standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication applies.

ISO 7498-2:1989 Information processing systems - Open systems interconnection Basic reference model - Part 2: Security architecture.

ISO/IEC 9594-6:1998 Information technology - Open Systems Interconnection : The Directory - Part 6: Selected attribute types

ISO/IEC 9594-8:1998 Information technology - Open Systems Interconnection : The Directory - Part 8: Authentication framework

ISO/IEC 9798-1:1991 Information technology - Security techniques - Entity authentication mechanisms - Part 1 : General model

ISO/IEC 9796:1991 Information technology - Open systems interconnection - Digital signature scheme giving message recovery

ISO/IEC 10181-1 Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview

ISO/IEC ISP 10611-1: 1997 Information technology -- International Standardized Profiles AMH1n -- Message Handling Systems -- Common Messaging -- Part 1: MHS Service Support

ITSEC Information Technology Security Evaluation Criteria. Published by the European Commission. 1993

EUD ”Directive 95/46/EC of the European Parliament and of the Council of Europe of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data", Official Journal of the European Communities, Number L281/31, 23 November 1995

Common Criteria Information technology -- Security techniques -- Evaluation criteria for IT security (ISO/IEC 15408-1-3:1999)

3 Terms and Definitions

For the purposes of this CEN Report the following definitions apply:

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]

availability: The property of being accessible and useable upon demand by an authorised entity. [ISO 7498-2]

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

binding of functionality: an aspect of the effectiveness of a secure system or product, namely the ability of its security enforcing functions and mechanisms to work together in a way which is mutually supportive and provides an effective and integrated whole (derived from ITSEC)

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]

certification path: An ordered sequence of certificates of objects in the Directory Information Tree which, together with the public key of the initial object in the path, can be processed to obtain the public key of the final object in the path. [ISO 9594-8]

common name: An attribute of the organisational person and thus also of the distinguished name. The common name is up to the issuer to define how to write. Usually it is first name and surname. [IS0 9594-6]

confidentiality: The prevention of unauthorised disclosure of information. [ITSEC]

cryptographic key: A parameter used with an algorithm to validate, authenticate, encrypt or decrypt a message. [ISO 8732]

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]

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

digital signature: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the that unit and protect against forgery e.g. by the recipient [ISO 7498-2]

effectiveness: an assurance property representing how well a secure system or product provides the security requested in the context of its actual or proposed operational use

electronic data interchange: The transfer of structured and coded data, by agreed message standards, from computer to computer, by electronic means.

electronic document: A defined set of digital information, text, pictures or other information with a designated person or organisation as the responsible issuer and where it is possible to ascertain that the contents originate from that entity.

encryption: A process of transforming plain text (readable) into cipher text (unreadable) for security or privacy. [ISO 7498-2].

entity authentication: The corroboration that an entity is the one claimed [ISO/IEC 9798-1].

integrity (data integrity, message content integrity): The property that data or a message's content has not been altered or destroyed in an unauthorised manner. [ISO 7498-2]

key pair: In a public key cryptosystem, the set of keys which consists of a public key and a private key that are associated with an entity. [ISO 9594-8]

non-repudiation (of origin, of submission, of delivery, of receipt): A security service providing an entity (individual or organisation) from falsely denying having performed a particular action related to some data, e.g. having participated in all or part of the creation of communication of that set of data.

organisational name: An object of the X.520 directory standard with attributes describing name, address, telephone numbers etc.

organisational person: An object of the X.520 directory standard describing a person in an organisation with attributes describing name, address, telephone numbers etc.

organisational unit: An object of the X.520 directory standard with an Organisational Unit Name attribute plus all the attributes of the "parent" organisational name.

origin authentication: (data origin authentication, message origin authentication): The process of corroborating that the source of data, a message or a document is as claimed. [ISO 7498-2]

security: The combination of confidentiality, integrity and availability. [ITSEC]

security policy (corporate security policy, system security policy): The set of laws, rules and practices that regulate how assets including sensitive information are managed, protected and distributed within a user organisation or a specific IT system. [ITSEC]

simple authentication : Authentication by means of simple password arrangements. [ISO 9594-8]

smart card: A machine readable card normally containing an integrated circuit chip which is capable of holding data and to perform computations. A microprocessor card.

strong authentication: Authentication by means of cryptographically derived credentials. [ISO 9594-8]

suitability of functionality: an aspect of the effectiveness of a secure system or product, namely the suitability of its security enforcing functions and mechanisms to in fact counter the actual and relevant threats to the security of the system or product, in relation to a specific context and risk. (derived from ITSEC)

trusted third party: An entity entrusted by a set of other entities to provide security services for a communication or authentication process.[1],[2]

4 Communication scenarios

4.1 The origins of HC user requirements

The purpose of this chapter is to illustrate some major types of communication scenarios in health care, where different security aspects will be relevant and different measures could be taken to ensure security. Please note that this classification does not purport to be comprehensive nor complete.

First of all, the HC community is faced with multiplicity of e.g. legal regulations, professional requirements and various sorts of demands and expectations. These are complex to map down to a set of technical and unambigious security specifications. This complexity escalates if there is concurrent demand to facilitate the adoption of solutions and products from other sectors, in a simple manner. Hence, there is a need for concepts, methods and tools that can establish a connection between the requirements of the HC user, and available technologies. This need applies to the perspective of the single communication party, but also to the need for coordination (bridging) between communicating parties.

On the other side, the HC sector has established some unnecessary complexities, e.g message security concepts that are linked to a variety of EDI formats and syntaxes, and to transportation protocols. This duality, the need to simplify and at the same time acknowledge an increasing complexity, raises special challenges for the standardisation process.
The specifics of communication scenarios in HC may be related to e.g the following (mainly non-technical) criteria:

- The purpose of communication, including the nature of the data shared through communication
- The organisational framework
- The type of networks to be utilised (e.g. Internet or a private network)
- The communication model (e.g. EDI), including the timing requirements

4.2 The purpose of communication

A description of a communication scenario is the key to a *risk analysis* leading to a set of security requirements. In HC, it is essential that a risk analysis does not take a direct technical approach, but follows a logical sequence :

1. The purpose of the intended information flow
2. The security properties to be cared for in that information flow
3. The risks introduced by the selected technology and the organisational context
4. The means and countermeasures (security functions)

[1] An important example of a trusted third party service is a certification authority issuing public key certificates.
[2] The use of the term trusted third party as an information provider, broker or storage is not intended by the concept used in this CR.

Some aspects to consider in this respect may be[3]:

1. Does the data concern identified individuals, patients or health care staff ?
2. What elapsed time is acceptable from sending to receipt of a message or data object".
3. Is the communication bi-directional ?
4. If so, is this because of a need to get a response to a specific question in a near future or is it just because there is a need to have the appropriate delivery of the message acknowledged ?
5. What is the likelihood of somebody interfering with the communication ? Is there a possible gain to be made for somebody ? Or is there a substantial possibility of sabotage?
6. What are the requirements for availability of the service ? What would be the consequences of the delay of the requested communication for a defined period of time ?

Examples:
The communication of invoices from a Health Care Establishment to a Payment body is clearly different from a real time transfer of an ECG from an ambulance to an emergency department in a hospital.
The annual supply of statistical data to central health care planning authorities, however not attributed to any identified person, is very different from a transfer of an urgent laboratory result to the intensive care unit.
The communication for searching published information from a bibliographic database is different from remote control of a CT-scanner.

4.3 Organisational view

The issue of purpose of communication requires an (inter- or intra-) organisational view. It is important to clarify whether the communication is going to take place within an organisation with sufficient control of the security policy to be utilised at both ends of the communication - as well as for the intermediary network (*intradomain* communication), or if the communication is going to cross organisational boundaries (*interdomain* communication).

Mutual support between communication parties in terms of consistent and mutually supportive security policies should be a requisite for a communication to legitimately take place. However, such a logical link between security policies is not automatically created as the result or function of a communication that has in fact happened[4]. However, at the technical level, a mechanism that is able to “calculate” the resulting security policy of a hypothetical communication, might be very useful in implementing such security policy “bridging”.
The key issues to consider are the security *policy* (which should be explicit) and the interactions between security *domains* associated with specific policies. The easiest task to handle is communication fully within a security domain. The more challenging alternative is to cross domains (with different persons having responsibilities for ensuring the policy), while maintaining the same basic security policy and fundamental security aspects.

In the latter context the following question arises: How can organisations "connect together" by the use of open (external, commercial) networks, in manners that are mutually supportive and consistent, in order to create a "logical" network enabling mutual trust between the participants[5]. Moreover, if interdomain communication is to be established over a common

[3] This list is not intended to be exhaustive

[4] It *could* however be, if there is an a priori agreement that the recipient will follow the instructions of the originator, e.g. in terms of Distribution Rules

[5] Which also requires some assurances that can justify the trust

network that also services *other domains that does not comply* with the policies and regulations of the sending and receiving domains, the more general issue of *Security Policy Bridging* arises. That is, in addition to authentication of identities, it also will be necessary to evaluate or recognise the policy of the other party as relevant to the communication task at hand.[6] In some situations this can be arranged off-line, but generally the inter-domain "handshaking" may have to include the negotiation or recognition of a coded (known) security policy, as well as an automatic decision on a common procedure on how to protect information in transit between the two cooperating domains, and when this should be allowed.

There are several possible strategies to establish a solution to the bridging problem, e.g :

1. The promotion of common security policies and networking principles through Codes of Connection[7] that stimulate uniform network security practices and solutions
2. The combination of "classical" EDI messaging combined with accepted standards and joint compliance with *Distribution Rules* (ENV 13608-3 Health informatics – Electronic healthcare record communication – part 3: Distribution rules)
3. Temporary communication channels in which the security policies are negotiated and technical measures are agreed, before actual communication of data
4. Middleware solutions providing automatic policy bridging and negotiation services between principals at different levels (e.g users, systems, programs)

The communication between A and B may have to pass several domains before reaching the destination domain. In many cases all the intermediate steps are important to consider and preferably in some sense control, at least by motivation of the availability issue. However, this is often impossible, e.g. when using the Internet.

4.3.1 The implications of the EU Data Protection Directive (EUD)

The EUD emphasises that information flow should be strictly purpose-oriented, and puts substantial limitations on the "reuse" of information shared for a certain purpose. The need for Security Policy Bridging – as introduced above - may hence be derived from the EUD. Moreover, the Directive raises the issue on how *individuals* (both healthcare professionals and other personnel) can function within an organisational agreement and framework, pursuing their *individual responsibilities*. The promotion of common security policies incorporating *Codes of Conduct* guiding the individual user with respect to various responsibilities and obligations, is an important part of this. Such Codes of Conduct must reflect legal, ethical and professional norms and standards of the healthcare community.
One particular aspect of policy differences may occur when national borders are crossed, meaning that different legislations are in effect. For some of the aspects with regard to the protection of the privacy of persons, European legislation is emerging (the EU data protection directive approved by the Council of Ministers, October, 1995 is now available and should be adopted by all EU-states before 24 July 1998) [EUD]. Many aspects of international communication have, however, not yet been appropriately solved.

The Directive encourages the establishment of Codes of Conduct as a means for ensuring proper implementations of national laws and provisions, pursuant to the Directive. This demands a comment: in view of some specific issues raised by the use of networks and

[6] I.e, that the security policies of the sender and the recipient are mutually consistent and supportive in order to ensure continuity with respect to the protection of the information asset contained in the actual message).
[7] E.g., as being used by NHS in the UK