SLOVENSKI STANDARD
SIST ENV 13606-3:2003

01-oktober-2003

Zdravstvena informatika –Komuniciranje z elektronskimi zapiski v zdravstvenem varstvu – 3. del: Pravila za razdeljevanje

Health informatics - Electronic healthcare record communication - Part 3: Distribution rules

Ta slovenski standard je istoveten z: ENV 13606-3:2000

ICS:

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

SIST ENV 13606-3:2003 **en**

EUROPEAN PRESTANDARD
PRÉNORME EUROPÉENNE
EUROPÄISCHE VORNORM

ENV 13606-3

May 2000

ICS 35.240.80

English version

Health informatics - Electronic healthcare record communication - Part 3: Distribution rules

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 13606-3:2000 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 is Part 3 of a multipart standard on *Electronic Healthcare Record Communication*.

The multipart standard consists of the following parts:

- Part 1: Extended Architecture
- Part 2: Domain Term List
- Part 3: Distribution Rules
- Part 4: Messages for the Exchange of information

This Prestandard was drafted using the conventions of the ISO/IEC directive part 3.

All annexes are informative.

Introduction

The need to distribute electronic healthcare records in whole or in part, whilst at the same time preserving security principles, has been the prime motivation behind the writing of this part European prestandard. However, the need for the opportunity for the subject of care to take a central role in their electronic healthcare record or its components being distributed both within and outside an information system to potential data users has taken priority over all other issues. The EU Data Protection Directive [95/46/EC] and the Council of Europe Recommendation on the Protection of Medical Data R(97)5 have also been central to the development of these distribution rules.

Serious consideration has been given to handling problems of access, not only to read from an electronic healthcare record but also to add information from within the same care team and document correctly. The problems are closely related since in many cases there are two systems interacting: one sending and the other receiving information.

This part European prestandard does not define the rules themselves (e.g. who should have access to what), these needing to be determined by local users, national guidelines and legislation. However it does define some of the requirements in relation to the architecture of the information system and in particular architectural component as described in part one of this four part European prestandard. It also places certain requirements on the functioning of information systems complying with this architecture and this part European prestandard in particular. These requirements when fulfilled enable compliance with the distribution rules defined by the data controller of the electronic healthcare record.

Distribution rules are a controlling mechanism, enabling access to and/or further distribution of the components to which they are attributed. Under the provisions and requirements of this European prestandard if a distribution rule is present then the data cannot be accessed or distributed unless the provisions of the rule are complied with. As a consequence it is possible to implement the distribution rules principles in such a fashion that the data may become unavailable thereafter. For both legal and healthcare reasons this should be prevented by the application of "fall back" rules with a "super user" type of access that will grant access to all data stored within the information system.

In order to provide the necessary flexibility required by the user community and avoid simple hierarchical constructs it is intended that where multiple distribution rules are present, they are processed individually and not as a combination. This method will provide for interoperability across country borders without weakening the rights of the subject of care. As a safeguard an access log has been included to ensure that if, for auditing or legal purposes, information is required on the distribution of data under the provision of distribution rules then this can be recreated in full. This access log and its entries are not intended to be communicated outside the information system to which it relates other than rendered in human viewable format.

If, for example, a data user be granted the privilege of having data distributed to them under the terms of a distribution rule that grants the right to modify or add to the architectural component covered by the rule then a

new version of those components is created. This new version may have further distribution rules added to it to provide for the new information needs. Version control within the architecture, as defined in part one of this four part European prestandard, provides for full recreation of the audit trail when used in conjunction with the relevant access log entry.

In clause 5, a set of data objects are shown that can be used to define rules that when implemented are interactive with other components and functions in an information system to control the distribution of data. Vendors are free to implement the distribution rules as they find best suited for their system, but they will have to follow the specifications in this document, including the data type definitions, when a distribution rule is distributed outside the originating electronic healthcare record system.

Annex A (Informative) shows the data structures when rendered into human viewable format for legal recreation and audit purposes outside the automated components of an information system.

Throughout this document Unified Modeling Language (UML) has been used. Reference is made to this technique in the Bibliography annex.

When national profiles are created using this European prestandard, then whilst the mandatory elements prescribed within the data objects will need to be included, the presence of optional elements within the national profile are left to national discretion.

If transnational interoperability is required, then all attributes are necessary and this European prestandard will need to be implemented in its entirety.

Health informatics - Electronic healthcare record communication - Part 3: Distribution rules

1 Scope

This European prestandard specifies data objects for describing rules for distribution or sharing of electronic healthcare records in whole or in part.

This European prestandard establishes general principles for the interaction of these data objects with other components and mechanisms within an electronic healthcare record application, thereby controlling the distribution of electronic healthcare records in whole or in part.

This European prestandard establishes ways of creating information with associated security attributes.

This European prestandard defines a methodology for constructing rules built from defined data objects, capable of being implemented using a range of techniques, to effect the control of sharing of electronic healthcare record data.

This European prestandard establishes principles that allow security policies to be implemented and incorporated in order to ensure the safe use of the data.

This European prestandard specifies a method for constructing an Access Log, that can be rendered human viewable, that records distribution of the data to which a Distribution Rule is attached.

This European prestandard does not specify the mechanisms and functions that take part within the negotiation procedure and therefore fully automate the data distribution process.

This European prestandard does not specify the mechanisms and functions that will allow some systems to continuously re-authenticate the data communication session and monitor its integrity.

This European prestandard allows the sharing of records distributed in space, time or responsibility.

This European prestandard does not specify the data objects and packages represented in an Information System.

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	639	1988	Codes for the representation of names of languages
ISO	1087	1990	Vocabulary of terminology
ISO	7498-2		Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture
ISO	8824-1	1995	Information Technology - Open Systems Interconnection Specification of Abstract Syntax Notation One (ASN.1). - Part 1: Specification of the basic notation
ISO	7498-4	1997	Open systems interconnection - The directory - authentication framework
EN	23166	1994	Codes for the representation of countries
ENV	12265	1996	Medical Informatics - Electronic Healthcare Record Architecture
IETF	RFC2315	1998	PKCS#7 Cryptographic Message Syntax Version 1-5. B.
ITU-T	[X.509]	1997	Recommendation X.509, The Directory: Authentication Framework

3 Terms and definitions

For the purposes of this European prestandard, the terms and definitions following apply

3.1
access right

privilege granted to a data user with respect to access to data contained within an information system

3.2
access rule

rule that describe and govern the access right

3.3
architectural component

part of an electronic healthcare record that is identifiable for the purposes of referencing and revision

3.4
availability

property of being accessible and useable upon demand by an authorized entity. [ISO 7498-2]

3.5
care team

logical grouping of carers and healthcare professionals involved in the ongoing medical care of a subject of care or a defined group of subjects of care

3.6
data elements

data entities that have an existence of their own without incorporating other data entities into a compound construct

3.7
data integrity

property that data has not been altered or destroyed in an unauthorized manner. [ISO 7498-2]

3.8
data provider

entity which provides data to other user

3.9
data provision

act of making data available to a data user from within an information system

3.10
data object

defined group of data

3.11
data user

user of a data object which has been provided to them

3.12
distribute

give out, hand out, make available, or deliver

3.13
distribution

act of distributing

3.14
distribution rule

logical concept or rule intended to convey and govern distribution of data

3.15
episode of care

identifiable grouping of healthcare related activity characterized by the entity relationship between the subject of care and a healthcare provider, such grouping determined by the healthcare provider

3.16
healthcare agent

system, organization, person or other entity responsible for, or involved in, the direct or indirect provision of healthcare services to an individual or involved in the provision of healthcare related services

NOTE 1 healthcare agent can include the patient themselves, in that patients can themselves administer their own healthcare services

NOTE 2 healthcare agent can be used to represent any other entity authorized to have access to healthcare information

3.17
healthcare party

organization or person responsible for the direct or indirect provision of healthcare services to an individual or involved in the provision of healthcare related services

3.18
healthcare person

person entrusted with the direct or indirect provision of healthcare services to a subject or population of subjects

3.19
healthcare information system architecture

structure of, and interrelationships with, as well as relationship to the organization and business context to be supported by a healthcare information system

3.20
object

part of the perceivable or conceivable universe. [ISO1087]

4 Symbols and abbreviations

AC	Architectural Component
ASN.1	Abstract Syntax Notation Version 1
DR	Distribution Rule
EHCR	Electronic Healthcare Record
HCR	Healthcare Record
HCP	Healthcare Party
ID	Identification
PKCS#7	Public Key Cryptography Standard 7
UID	Unique Identifier
UML	Unified Modeling Language
UTC	Universal Coordinated Time

5 Distribution rule and access log

5.1 Overview

A distribution rule is a logical concept or rule intended to convey intent for and govern distribution of a data object. This European prestandard defines a conceptual model and content of data objects and the services that interact with these data objects to provide the functions necessary to convey and govern the distribution of a data object.

The distribution rule shall be applicable at the level of the architectural component as described in part one of this four part European prestandard. Conformance with this European prestandard at a mandatory level will deliver a base functionality that offers a simple but secure implementation. However this will also in some senses offer the strongest control of information distribution as it is the addition of optional elements within multiple distribution rules that will allow access to the data in other circumstances.

The process of distribution of data is always an active process. It can itself be initiated by an active process, as is seen as the result of a directed query or request for information from an information system. In any of these cases there is always a data provider and a data user. This process is shown in figure 1

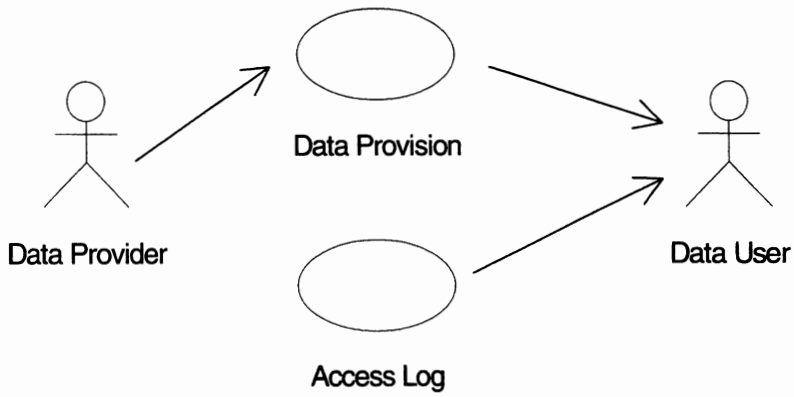


Figure 1 — Act of data provision

The UML use case diagram in figure 1 is the representation of a data provider making information available. The data provider may conceptually be a person taking an active intent on providing data to a third party or may be an information system acting as a repository from which a data user extracts information. The act of sending a message or data provision may result in the automated creation of an access log Item entry maintained in some part of an information system maintained by the data provider. The data user can either be someone requesting access to the architectural component, message recipient or an auditor carrying out the function of accessing the data access log item entry. The data provider with the originating information system maintains the access log item entries.

All of these types of data access with the exception of auditing the access log items themselves result in the generation of an access log item entry, if one is present, according to the constructs defined in this European prestandard. The access log is only retrieved for auditing or legal purposes and then shall only be in full and its data rendered into human viewable format according to the data definitions contained in annex A. In figure 2 the diagram makes the following assumptions in relation to data provision and data access:

a) data user can be any user authorized to access data and can encompass healthcare agent in context;

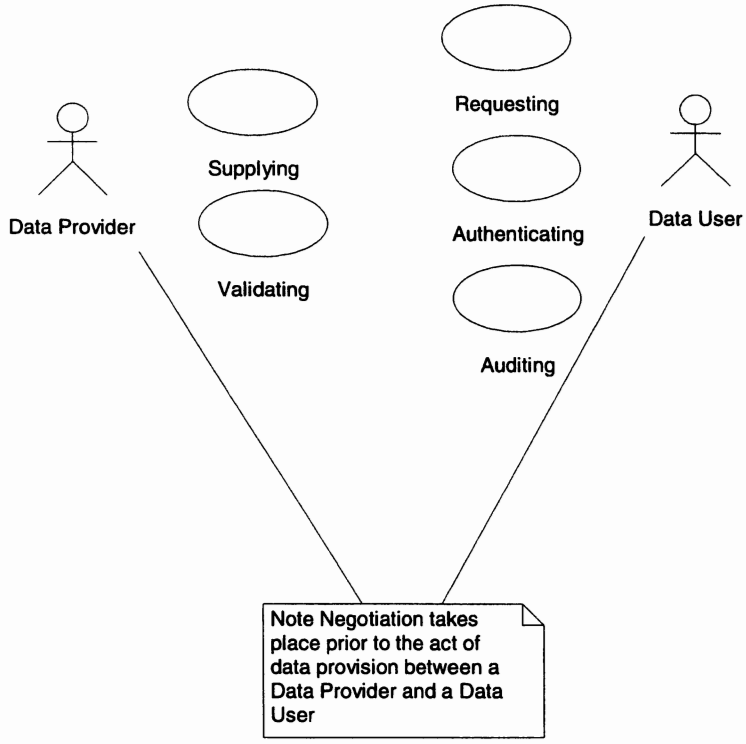
b) healthcare agent, healthcare party, auditor and subject of care;

c) data provider is any information system which may be distributed in space;

d) access log entry is maintained concurrent with the data to which it relates;

e) access log entry is created by the process of successful data acquisition.

During the process of data provision, from a data provider complying with this European prestandard to a data user, a negotiation procedure takes place between the data user and the data provider as illustrated in figure 2.



NOTE A phase of negotiation takes place prior to the act of data provision between a data provider and a data user.

Figure 2 — The Negotiation procedure 1

This process may be fully automated but it is outside the scope of this European Prestandard to specify the mechanisms and functions that shall take part within this negotiation procedure as shown in figure 3

NOTE The act of data provision may create an entry in an access log, if present.

Figure 3 — The Negotiation procedure 2

An expanded view of the data objects and functions required to deliver this process of negotiation is shown in figure 5.

The process of information provision can be regarded as a two way process involving both request and reply. During this process the request may be implicit as envisioned in the case of a directed message, or explicit as in the request for information. For the process to take place and the phase of negotiation to be established both the data user and the data provider need to be authenticated. This process can be initiated from either end assuming a validated communication session can be established. Once the session is established the process of information request and negotiation can take place. Some systems will continuously re-authenticate the session and monitor its integrity but the functioning of this is outside the scope of this European prestandard.

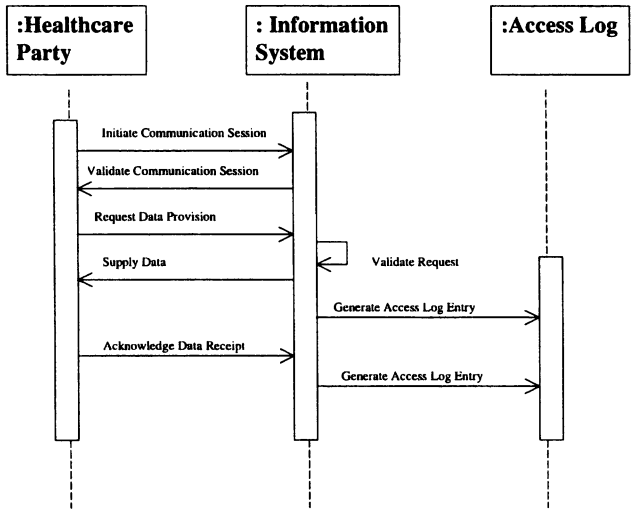


Figure 4 — The communication session

Figure 4 shows a session of communication during the process of data provision. For the process of negotiation to take place information about the data user is checked by systems within the providing application against the data within the distribution rule, in order to determine that the rules for distribution of the data object are satisfied. In the case of directed messaging some of these systems may require to be non-automated. The formal data components interacting in this process are shown in figure 5.

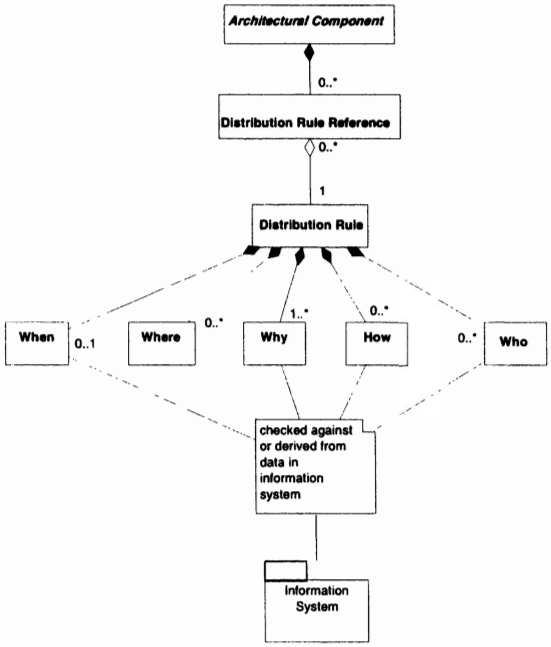


Figure 5 — Data elements utilized in the negotiation process

NOTE 1 The package represented in figure 5 as information system, falls outside the scope of this European prestandard.

NOTE 2 Sharing covers all the methods by which electronic healthcare records are made available to healthcare professionals. It includes accessing a physical healthcare record archive such as database interrogation, access to Architectural Components (see ENV 13606-1, part one of this four part European Prestandard), creating a virtual healthcare record by enabling access to data from several different sources (distributed database interrogation) and communicating healthcare records in whole or in part from system to system, such as messaging (see ENV 13606-4, part four of this four part European Prestandard).

NOTE 3 If a data user is granted the privilege of having data distributed to them under the terms of a distribution rule that grants the right to modify or add to the Architectural Component covered by the rule, then a new version of those components shall be created. This new version shall have the potential for further distribution rules to be added to it to provide for the new information needs.

NOTE 4 Version control within the architecture, as defined in ENV 13606-1, provides for full recreation of the audit trail when used in conjunction with the relevant access log entry.

NOTE 5 Architectural Component, Healthcare Agent in Context, Healthcare Agent and Healthcare party are defined in ENV 13606 part one: Extended architecture, of this four part European prestandard.

5.2 Overview to distribution rules and access log items

Figure 6 gives a diagrammatic representation of the linkage between an architectural component and a distribution rule and its associated access log item entries and their sub-components. These objects and their attributes are further defined below.

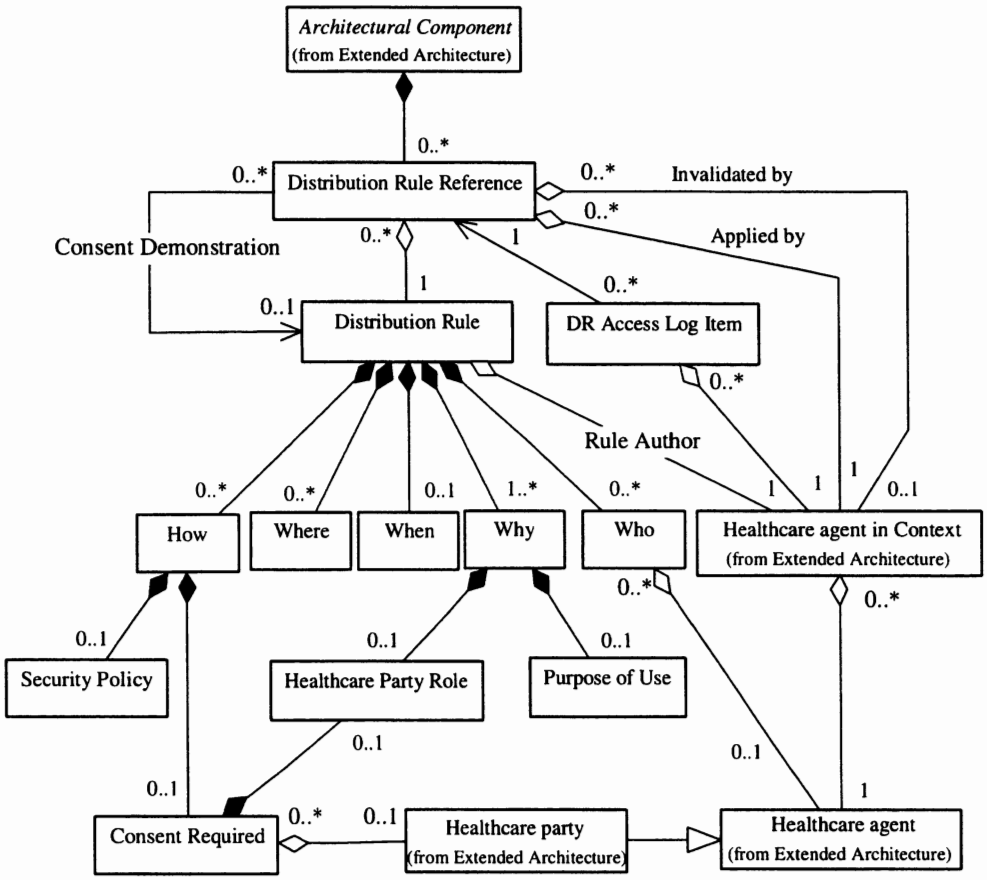


Figure 6 — - Architectural Component linkage

Throughout this document the healthcare agent in context, or one of its specializations, is shown as a reference. When an access log is recreated for the purposes of audit the data contained within these classes shall be rendered into human viewable format along with the rest of the data contained in the access log.

5.3 Distribution rule reference

5.3.1 Scope of distribution rule reference

The distribution rule reference shall contain all the data necessary to apply specific distribution rules to specific architectural components.

5.3.2 Structure of distribution rule reference

A conceptual diagram of distribution rule reference is shown in figure 7.