SLOVENSKI STANDARD

SIST EN 12251:2005

01-januar-2005

Nadomeġļ a:

SIST ENV 12251:2003

Zdravstvena informatika – Varna identifikacija uporabnikov v zdravstvenem varstvu – Upravljanje in varnost avtentikacije z gesli

Health informatics - Secure User Identification for Health Care - Management and Security of Authentication by Passwords

Medizinische Informatik - Sichere Nutzeridentifikation im Gesundheitswesen - Management und Sicherheit für die Authentifizierung durch Passwörter

Informatique de santé - Sécurité de l'identification de l'utilisateur des soins de santé - Gestion et sécurité de l'authentification des mots de passe

Ta slovenski standard je istoveten z: EN 12251:2004

ICS:

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

SIST EN 12251:2005 en

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 12251

August 2004

ICS 35.240.80

English version

Health informatics - Secure User Identification for Health Care - Management and Security of Authentication by Passwords

Informatique de santé - Sécurité de l'identification de l'utilisateur des soins de santé - Gestion et sécurité de l'authentification des mots de passe

Medizinische Informatik - Sichere Nutzeridentifikation im Gesundheitswesen - Management und Sicherheit für die Authentifizierung durch Passwörter

This European Standard was approved by CEN on 21 June 2004.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the Central Secretariat has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, 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. EN 12251:2004: E

Contents

page

Foreword

This document (EN 12251:2004) has been prepared by Technical Committee CEN/TC 251 “Health informatics”, the secretariat of which is held by SIS.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2005, and conflicting national standards shall be withdrawn at the latest by February 2005.

This document supersedes ENV 12251:2000.

This document is designed to improve the authentication of individual users of health care IT system, by strengthening the automatic software procedures associated with the management of user identifiers and passwords, without resorting to additional hardware facilities.

Although the use of passwords, and the need for improved security in this respect, is by no means specific for the Health Care field, it is felt strongly that the way in which systems are being used in this field, often in direct support of patient care and handling very sensitive information, urgently call for a good solution in this area. However, the methods specified in this document can possibly be applied in other sectors as well at the discretion of users.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

Introduction

Information Technology (IT) systems in the health care environment are being used in increasingly sensitive and critical circumstances. To facilitate secure access control to an IT system and within an IT system, it is essential to uniquely establish the identity of all users seeking access. Further, to have confidence that a user really is who he or she claims to be, there is a need for secure means of verifying the claimed identity. The use of passwords, being confidential to each user, and constructed in such a way that others cannot compromise this confidential authentication information easily, is the most common means of authentication in current computer systems, and will be so for some time to come. This document can facilitate the wider process of Security Management.

Conventional passwords have several disadvantages. Some of these are:

— They can easily be shared among several users

— The use of unprotected network technology makes them easy targets for eavesdropping

— They can be hard to remember if chosen as to be secure

Other technologies such as chip cards and biometrics, which provide more secure means of authentication, have been introduced and will eventually phase out the use of passwords. However, in the meantime it is important to facilitate the most secure use of passwords in health care IT systems. This is the main objective of this document.

1 Scope

This document is designed to improve the authentication of individual users of health care IT systems, by strengthening the automatic software procedures associated with the management of user identifiers and passwords, without resorting to additional hardware facilities.

This document applies to all information systems (hereafter called systems) within the health care environment that handle or store sensitive person identifiable health information, using passwords as the only means of authenticating the entered user identifier, i.e., verifying the claimed identity of a user. Systems that fall within the scope of this document include for example electronic patient record systems, patient administrative systems and laboratory systems, containing personal health information.

This document does not apply to systems outside the health care environment. Neither does it apply to systems within the health care environment that use other means of identification and authentication, such as smart cards, biometric methods or other technical facilities.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 7498-2, *Information processing systems – Open systems interconnection – Basic reference model – Part 2: Security architecture*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
access control
prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner

3.2
authentication
process of verifying a claimed user identity, in this document on the basis of an entered user identifier and password

3.3
authentication information
information used to establish the validity of a claimed identity [ISO 7498-2]

3.4
authorised user
person who is given access rights to the system, i.e., person who is given a unique user identifier and an initial password, and by this is given the right to log-on to the system, in order to perform the functions or access to the data the user is entitled to

3.5
default password
initial password, provided by the system on installation, to enable initial use

3.6
identification
process that enables recognition of an authorised user described to the system, by the use of a unique user identifier

3.7
password
confidential authentication information composed of a string of characters [ISO 7498-2]

3.8
security administration
act of controlling and administering all relevant security issues in the system. It can be performed by one or more specially authorised users through the assignment of security relevant access rights

NOTE These users are called security administrators.

3.9
site-specifiable
site-modifiable
specifiable (or modifiable) by the local security administrators after purchase of the system

3.10
system
combination of computer hardware and software, used in this document as the system as it is perceived by the user

3.11
user identifier
information, composed of a string of characters, uniquely identifying an authorised user of the information system

4 Requirements

4.1 Unique identification and authentication

The system shall use user identifiers to uniquely identify and authenticate users.

4.2 Identification and authentication prior to all other interactions

Identification and authentication shall take place prior to all other interactions between the system and the user, apart from the system provided log-on message (see 4.5). Other interactions shall only be possible after successful identification and authentication, i.e., identification and authentication leading to system access, of an authorised user.

4.3 Associating unique identity with users

The system shall provide a mechanism which allows site-defined attributes, e.g. name and affiliation, to be associated with each user identifier, for the purpose of uniquely identifying the person.

4.4 Maintaining the identity of active users

The system shall maintain the identity of all users currently logged on.

4.5 Log-on message

Prior to initiating the log-on procedure, the system shall provide a message regarding unauthorised use and the possible consequences of failure to meet those requirements. This message shall be site-specifiable by the security administrators, and shall be visible to the user during the log-on procedure.

NOTE This message should point out the need to comply with confidentiality requirements, and indicate possible legal action after misuse.

4.6 Number of log-on trials

The log-on procedure shall exit if the user authentication procedure is unsuccessfully performed, i.e., not leading to system access, a site-specifiable number of times within a log-on session.

NOTE The recommended number of times is three times.

When the site-specifiable number is exceeded, the system shall generate an alarm to the security administrators within the shortest possible time, and actions designed to limit possible misuse shall be initiated.

When the site-specifiable number is exceeded, a site-specifiable period of time shall elapse before the log-on process can be restarted on that input device, provided it can be securely identified (It shall be possible to specify this period of time to be zero for specific input devices, e.g., for input devices in intensive care or emergency units).

An alternative is to reject log-on from the user identifier for a site-specified time.

4.7 Incorrectly performed log-on procedure

The system shall appear to perform the entire user authentication, irrespective of errors detected in any of the data entered during the log-on procedure.

Error feedback shall not contain any information regarding which part of the authentication information was incorrect, or in what respect the information was incorrect.

4.8 Display of log-on statistics

Upon successful access to the system, the system shall display:

a) The date and time of the user's last successful access.

b) The number of unsuccessful attempts to access the system by that user identifier since the last successful system access.

4.9 Password sharing

The system shall not provide any means to facilitate explicit sharing of passwords by multiple users.

The system shall allow a user to choose a password that is already associated with another user.

The system shall not provide any indication that a password is already associated with another user.

4.10 Password storage

The system shall store passwords in a one-way encrypted form.

No users shall be able to have, or give themselves, read access to files containing encrypted passwords.