

Health informatics — Secure user identification for health care — Management and security of authentication by passwords

ICS 35.240.80

National foreword

This Draft for Development is the English language version of ENV 12251:2001.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature due to the limited duration of the European Prestandard. It should be applied on this provisional basis, so that information and experience of its practical application may be obtained.

Comments arising from the use if this Draft for Development are requested so that UK experience can be reported to the European organization responsible for its conversion into a European Standard. A review of this publication will be initiated 2 years after its publication by the European organization so that a decision can be taken on its status at the end of its three-year life. The commencement of the review period will be notified by an announcement in *Update Standards*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into a European Standard, to extend the life of the prestandard or to withdraw it. Comments should be sent in writing to the Secretary of BSI Technical Committee IST/35, Health Informatics, at 389 Chiswick High Road, London W4 4AL, giving the document reference and clause number and proposing, where possible, an appropriate revision of the text.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

This Draft for Development, having been prepared under the direction of the DISC board, was published under the authority of the Standards Policy and Strategy Committee on 19 October 2001

Summary of pages

This document comprises a front cover, an inside front cover, the ENV title page, pages 2 to 16, an inside back cover and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

© BSI 19 October 2001

ISBN 0 580 38595 7

English version

Health informatics - Secure user identification for health care - Management and security of authentication by passwords

This European Prestandard (ENV) was approved by CEN on 7 January 2000 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

Contents

1. Scope 6

2. Normative references 7

3. Definitions 8

3.1 access control.....8

3.2 authentication information 8

3.3 authorised user 8

3.4 default password 8

3.5 identification 8

4. Requirements.....9

4.1 Unique identification and authentication 9

4.2 Identification and authentication prior to all other interactions 9

4.3 Associating unique identity with users 9

4.4 Maintaining the identity of active users 9

4.5 Log-on message 9

4.6 Number of log-on trials 9

4.7 Incorrectly performed log-on procedure 9

4.8 Display of log-on statistics 10

4.9 Password sharing.....10

4.10 Password storage.....10

4.11 Logging of passwords 10

4.12 Password display suppression 10

4.13 User-changeability of passwords 10

4.14 Default passwords.....10

4.15 Initialised passwords 11

4.16 Temporary passwords 11

4.17 Password expiration.....11

4.18 Password expiration notification 11

4.19 Password reuse 11

4.20 Password complexity 12

Annex A (informative) Potential password complexity requirements 13

Annex B (informative) User responsibilities 14

Annex C (informative) Password communication 15

Annex D (informative). Bibliography.....16

Foreword

This European Prestandard has been prepared by Technical Committee CEN/TC 251 "Health informatics", the secretariat of which is held by SIS.

This European Prestandard 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 prestandard 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 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.