SLOVENSKI STANDARD
SIST ENV 13729:2003

01-oktober-2003

Zdravstvena informatika ï Varna identifikacija uporabnikov ï Moļ na avtentikacija z mikroprocesorskimi karticami

Health informatics - Secure user identification - Strong authentication using microprocessor cards

Ta slovenski standard je istoveten z: ENV 13729:2000

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices
35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology

SIST ENV 13729:2003 **en**

EUROPEAN PRESTANDARD

PRÉNORME EUROPÉENNE

EUROPÄISCHE VORNORM

ENV 13729

July 2000

ICS 35.240.15; 35.240.80

English version

Health informatics - Secure user identification - Strong authentication using microprocessor cards

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

Ref. No. ENV 13729:2000 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.

This European prestandard was developed under mandate M/255 issued by the European Commission and EFTA.

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.

Introduction

There is a requirement that patient data must be protected with special care. A key element for any data confidentiality protection mechanism to be effective is to have a secure means of user identification, which will additionally form the basis for the provision of accountability services including the authentication of data origin.

In general, access control systems and access rights will be determined locally. Identification, however, and the method to authenticate the claimed identity, is a key element for security standardization since it will be used in communication between systems. When used for inter-organizational communication it depends on Trusted Third Parties (TTP) that provide certification services (also referable as Certification Service Providers), which is another reason for the importance of standard methods. Standard solutions are also needed to ensure a user-friendly environment where the users can identify themselves with one method for possible access to a variety of different healthcare systems.

A European Prestandard for the use of passwords for user authentication was drafted by CEN/TC 251, (prENV 12251 "Health Informatics -Secure User Identification for Health Care - Management and Security of Authentication by Passwords - Health Care Oriented IT Security Functionality Class") aimed at improving the widely used password systems used today, which may be sufficient if only base level protection is required. However, for many healthcare systems a higher level of protection is required, in particular if unsecured networks are used, in which case the use of strong authentication with a cryptographic challenge-response method is required.

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;
- the considerable problems of managing passwords, especially in large complex organisations.

The use of strong authentication using microprocessor (smart) cards, offers distinct advantages:

- ease of administration in the complex healthcare environment also allowing secure user identification across organisations and potentially cross-borders;
- mobility of the users;
- solutions based on standardized protocols and products;
- a much better security protection level important for confidentiality and legal value.

The importance of using microprocessor cards and strong authentication as a key mechanism for the Global Information Infrastructure has also been recognised outside of Europe, and the G7-collaboration has emphasised the topic of Health Professional Cards (HPCs) as a priority work item.

Microprocessor-cards containing microprocessor-based integrated circuits (ICs) with cryptographic functions often realised by cryptographic co-processors can be used for secure identification of users of information systems. Furthermore they may be used for other core security services related to the user's identity such as accountability and non-repudiation services provided by digital signatures and confidentiality services. In several European countries cards used by health professionals and in other sectors, are combining these services with a core identity authentication as defined in this European Prestandard. It has not been considered feasible to standardize these services at this time.
The most important linkage of the card to a user is in the fact that the user shall keep this personal token in his secure custody. In addition most card systems, and as specified in this European Prestandard, use PIN-codes, the verification of which within the IC Card provides further security.

However, the user's properties (e.g. biometrics) may also be stored on the IC card (ICC) verifying the card user as the legitimate card user. However, since neither do base standards for the use of such methods currently exist, nor is it deemed necessary and feasible for the healthcare sector at this point to

employ them, no attempt has been made to provide detailed support for such user properties in this specification.

Although the need for improved security in user identification is by no means specific for the healthcare 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 European solution in this area to support implementations nationally as well as cross-border healthcare applications. However, the methods specified in this prestandard can be applied in other sectors as well at the discretion of users. During the development of this European Prestandard, several national solutions for this problem have been identified in e.g. Germany, France, Sweden and Finland. These have been taken as the basis for this specification and in many aspects they are all already compliant with this European solution. As a guide to possible implementation of such solutions three examples of card specifications compliant with the normative requirements of this prestandard are included as recommendations in a note within the body of this prestandard.

This European Prestandard aims to facilitate interoperability between different types of remote health information systems and users of local systems. In a local, regional or national context it may also be important that the cardholder can use his/her card in any healthcare local system. In view of the aim to achieve the highest level of openness and provide real guidance for such interoperability, additional normative specification may be required; this prestandard focuses firmly on the use of a Public Key Infrastructure (PKI) with asymmetric cryptography, and provides appropriate functional requirements together with detailed certificate specification based on the ISO/IEC 9594-8 standard (ITU-T's X.509). This does not exclude the validity of symmetric (i.e. more restricted) solutions to be justifiable particularly for access to patient data cards. However, a European solution on this basis is not practicable.

This Prestandard is intended primarily for use by healthcare system designers and implementers, but can also provide guidance for system procurers.

In addition to the normative parts focusing on interoperability between local users and remote systems, and a normative annex providing further requirements for cardholder verification, this document also contains informative elements in other annexes, including tutorial material and healthcare professional data.

1 SCOPE

This European Prestandard defines a method for strong authentication of the identity of a user of a health information system where the user is equipped with a microprocessor card. By system is meant primarily a general purpose computer system with hardware ranging from a personal computer (PC) to a mainframe. Dedicated embedded systems with special operating systems are not considered, nor is access control to data on a smart card such as a patient data card. However this European Prestandard does not preclude the addition of this functionality to a user card.

The main focus of consideration is on users who are the healthcare persons, registered professionals and other staff using health information. In situations when patients are allowed to use healthcare information systems directly to access their personal data, and secure user identification is needed, this European Prestandard may also be used.

This European Prestandard defines a cryptographic authentication procedure using microprocessor cards with digital signature capabilities. This procedure is designed to be usable both within a local system and by a remote system across an unprotected network.

This European Prestandard specifies the cryptographic algorithm to be employed and which must be available in the microprocessor card as well as in any authenticating system, remote or local, in the implementation of the defined strong authentication method.

This European Prestandard defines the minimum set of physical, electrical and protocol standards that microprocessor cards shall support in order to conform to this standard; it does not define the internal structure of systems that support the use of these cards.

This ENV identifies a number of IETF standards that support remote authentication in a way that is compatible with the use of this standard.

The method for strong authentication defined in this European Prestandard requires Certification services. While these are outlined in the authentication reference model and some functional requirements on the TTP services are included, the detailed specification of these are outside the scope of this prestandard.

The requirements on procedures for the process of the card authenticating the user are also defined, focusing on PIN-code handling, where the PIN verification is only performed within the IC Card.

This involves the comparison of the user supplied PIN against the reference PIN held within the card. Provision has been made for the possible future addition of biometric techniques.

The identity authenticated by the method in this European Prestandard is held in a set of data provided in a public key certificate specification based on the ISO/IEC 9594-8 (X.509) standard. This European Prestandard includes some additional requirements on such data for cross border use. A national or local implementation profile will frequently be needed for additional specification.

This authentication method may also be used to authenticate the role/registered professional class using the same basic technology. This status information may be used for authorisation, access control, accountability (including non-repudiation, data origin authentication, integrity) etc., but such additional functions as these are outside the scope of this European Prestandard. One example of a data structure for use in certificates is given in informative annex B.

While the technology of asymmetric encryption used for strong authentication can also be used to provide a mechanism for digital signature creation and confidentiality services, these possible services of the same card are outside the scope of this European Prestandard.

This prestandard defines a mechanism that can be used in provision of the general aspects of security for healthcare communication as described in ENV 13608-1.

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.

ENV 13608	Health informatics - Security for healthcare communication - Part 1: Concepts and terminology Part 2: Secure data objects Part 3: Secure data channels
IETF/RFC 2246	Transport Layer Security (TLS) Protocol, Version 1.0 Note: for client authentication using Transport layer security over TCP/IP
IETF/RFC 2459	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
IETF/RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices ('PKIX framework ')
ISO/IEC 2382	Information technology – Vocabulary Part 8: Security
ISO 3166	Country codes Part 1: Country codes
ISO 7498-2	Information processing systems - Open Systems Interconnection, Basic Reference Model – Part 2: Security Architecture. Note: ISO 7498-2 is superseded by ISO/IEC 10745 (ITU-T X.803), ISO/IEC 13594 - IT-Lower layers security (ITU-T X.802) and ISO/IEC 10181-1 (ITU-T X.810).
ISO/IEC 7816	Information technology - Identification cards, Integrated circuit(s) cards with contacts – Part 1 – Physical characteristics Part 2 – Dimensions and location of contacts Part 3 – Electronic signals and transmission protocols Part 4 - Interindustry commands for interchange Part 8 - Security architecture and related interindustry commands NOTE Part 8 includes security functions for public key procedures and extended PIN functions
ISO 9564-1	Banking – Personal Identification Number management and security – Part 1: PIN protection principles and techniques
ISO/IEC 9594-8	Information technology - Open Systems Interconnection - The Directory – Part 8: Authentication framework [Note: equiv. to ITU-T/X.509]

ISO/IEC 9798	ISO/IEC: Information technology – Security techniques – Entity authentication Part 1: General Part 2: Mechanisms using symmetric encipherment algorithms Part 3: Mechanisms using digital signature techniques Part 4: Mechanisms using a cryptographic check function Part 5: Mechanisms using zero knowledge techniques
ISO/IEC 9979	ISO/IEC: Information technology – Security techniques – Procedures for the registration of cryptographic algorithms
ISO/IEC 10118	Information technology - Security techniques - Hash-functions – Part 1: General Part 2: Hash-functions using an n-bit block cipher algorithm Part 3: Dedicated hash-functions Part 4: Hash-functions using modular arithmetic
ISO/IEC 10181	Information technology - Open Systems Interconnection - Security frameworks for open systems – Part 1: Overview [equivalent to ITU-T Rec. X.810] Part 2: Authentication framework
ISO/IEC 10745	ISO/IEC: Information technology – Open Systems Interconnection -- Upper layers security model
ISO 10202	Financial transaction cards -Security architecture of financial transaction systems using integrated circuit cards - Part 6: Cardholder verification Part 8: General principles and overview
ISO/IEC 10736	Telecommunications and information exchange between systems - Transport layer security protocol.
ISO/IEC 13594	Information technology - Lower layers security.
ISO/IEC 13888	ISO/IEC: Information technology – Security techniques – Non-repudiation Part 1: General
ISO/IEC PDTR 14516	Information technology - Security techniques - Guidelines on the use and management of TTP services
ITU-T/X.509	see ISO/IEC 9594-8
IETF/ SSLv3	Secure Sockets Layer, version 3
NCSC TG-004	National Computer Security Center - Glossary of Computer Security Terms, Version 1, October 1988 ['the Aqua Book']
ANSI/SIA 3	American National Standard Institute - Glossary of biometric terms [draft standard from US Security Industry Association, 1993]
NCSC/TCSEC	National Computer Security Center - Trusted Computer System Evaluation Criteria, ['the Orange Book']

3 Definitions

For the purposes of this European Prestandard the following definitions apply (followed by their sources).

access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

[ISO/IEC 2382-8]

accountability
the property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2]

asymmetric cryptographic algorithm
asymmetric encryption algorithm
algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ

[ISO 10181-1]

authentication
process of reliably identifying security subjects by securely associating an identifier and its authenticator

[ISO 7498-2]

NOTE See also data origin authentication and peer entity authentication.

authenticator
means used to confirm the identity or to verify the eligibility of a station, originator, or individual

[NCSC TG-004]

biometric
measurable, unique physical characteristic or personal trait used to recognise the identity, or verify the claimed identity, of an enrolee

[ANSI/SIA 3]

card accepting device
CAD
device used to interface with the ICC during a session

[ISO 10202-8]

cardholder
the person to whom the card has been issued

cardholder verification method (CVM) capability
the indication of all the methods supported by the terminal for verifying the identity of the cardholder at the terminal

[EMV '96]

certificate management
procedures relating to certificates: certificate generation, certificate distribution, and certificate archiving

certificate revocation
revocation of certificates
act of removing any reliable link between a certificate and its related owner (or security subject owner), because the certificate is not trusted any more although it is unexpired

certification
use of digital signature to make transferable statement about beliefs of identity, or statements about delegation of authority

certification authority
authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys

[ISO 9594-8]

cryptographic algorithm
algorithm which transforms data in order to hide or reveal its information content and which uses at least one secret parameter. (In the case of an asymmetric algorithm the data is hidden using a public parameter and revealed using a secret parameter)

[ISO/IEC 9979: 1991]

data origin authentication
the corroboration that the source of data received is as claimed

[ISO 7498-2]

digital signature
data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[ISO 7498-2]

hashing algorithm
an algorithm used to perform a (mathematical) function that maps values from a (possibly very) large set of values into a smaller range of values

[based on ISO 10181-1]

health professional card
HPC
a card issued to a person working professionally in the provision of health services which is used as a security device to provide secure user authentication and possibly other security services

identification
Identification - Process that enables recognition of an entity by an IT product.

[Federal Criteria for Information Security v.1]

identifier
piece of information used to distinguish an object including a computer systems user from other objects of the same class

integrated circuit card
IC Card
ICC

ID-1 card type (as specified in ISO 7810, ISO 7811 parts 1 to 5, ISO 7812, and ISO 7813) into which has been inserted one or more integrated circuits (ICs)

[ISO 7816-1]

key
sequence of symbols that controls the operations of encipherment and decipherment

[ISO 7498-2]

key certification
digitally signing a cryptographic key to indicate to third parties the identity or other attribute of the key owner

[prENV 13608-1]

microprocessor card
integrated circuit card in which one or more of its contained integrated circuits is/are microprocessors

peer entity authentication
the corroboration that a peer entity in an association is the one claimed

[ISO 7498-2]