SLOVENSKI STANDARD
SIST ENV 12388:2003

01-oktober-2003

Medicinska informatika – Algoritem za storitve digitalnega podpisa v zdravstvenem varstvu

Medical Informatics - Algorithm for Digital Signature Services in Health Care

Medizinische Informatik - Algorithmen für digitale Unterschriftsdienste im Gesundheitswesen

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Informatique de santé - Algorithme pour les services de signature numérique dans le domaine de la santé

SIST ENV 12388:2003
https://standards.iteh.ai/catalog/standards/sist/bda74dbf-cdf5-4a39-9ce7-a2021f23a1fa/sist-env-12388-2003

Ta slovenski standard je istoveten z: **ENV 12388:1996**

ICS:

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

SIST ENV 12388:2003 **en**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST ENV 12388:2003

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST ENV 12388:2003
https://standards.iteh.ai/catalog/standards/sist/bda74dbf-cdf5-4a39-9ce7-a2021f23a1fa/sist-env-12388-2003

SIST ENV 12388:2003

EUROPEAN PRESTANDARD **ENV 12388**

PRÉNORME EUROPÉENNE

EUROPÄISCHE VORNORM September 1996

ICS 11.020; 35.240.60

Descriptors: data processing, information interchange, data transmission, medicine, signature, numeric representation, algorithms

English version

Medical Informatics - Algorithm for Digital Signature Services in Health Care

Informatique de santé - Algorithme pour les services de signature numérique dans le domaine de la santé

Medizinische Informatik - Algorithmen für digitale Unterschriftsdienste im Gesundheitswesen

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ENV 12388:2003
https://standards.iteh.ai/catalog/standards/sist/bda74dbf-cdf5-4a39-9ce7-a2021f23a1fa/sist-env-12388-2003

This European Prestandard (ENV) was approved by CEN on 1996-08-29 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 an European Standard (EN).

CEN members are required to announce the existance 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, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CEN

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

Central Secretariat: rue de Stassart,36 B-1050 Brussels

© 1996 Copyright reserved to CEN members

Ref. No. ENV 12388:1996 E

SIST ENV 12388:2003

CONTENTS

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ENV 12388:2003
https://standards.iteh.ai/catalog/standards/sist/bda74dbf-cdf5-4a39-9ce7-a2021f23a1fa/sist-env-12388-2003

SIST ENV 12388:2003

Foreword

This European Prestandard has been prepared by Technical Committee CEN/TC 251 "Medical Informatics", the secretariat of which is held by IBN.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the folloxing countries are bound to announce this European Prestandard: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

Introduction

The use of data processing and telecommunications in health care must be accompanied by appropriate security measures to ensure data confidentiality and integrity in compliance with the legal framework. This is aimed at protecting patient privacy as well as professional accountability.

Digital signature techniques are essential parts of several security services of great importance for the health care sector. Examples of these are:

Authentication of computer users, organisations and systems
Authentication of document originators
To protect document integrity and ensure that contents and signature are bound together.

iTeh STANDARD PREVIEW

Additional derived security services that can be implemented with the digital signatures are:

(standards.iteh.ai)

Non repudiation of origin and receipt of messages
Time-stamping
Proof of general authorisation as a registered professional and other qualifications

SIST ENV 12388:2003
https://standards.iteh.ai/catalog/standards/sist/...
a2021f23a1fa/sist-env-12388-2003

As automated interchange of information in healthcare increases, it is essential to provide appropriate information interchange standards. Several aspects of these security services are standardized at an international level mainly through ISO/IEC JTC1/SC27 work on protocols. However, no inter-sector standard exists at the time of writing that defines the precise algorithm to be used for the digital signature. In European health care with the need for open secure communications between all parties involved regionally and increasingly also transborder, it is essential that at least one standard algorithm can be used for all services depending on digital signature techniques.

The protocols referring to a digital signature algorithm should therefore identify the selected algorithm to allow possible changes in the future. The algorithm defined in this standard was selected because at the time of writing it fulfilled the following criteria:

- If used with appropriate key length, it provides very good protection against attacks
- It has been in the public domain for a very long time and has been very thoroughly examined for possible flaws or hidden trap-doors
- It can be calculated with modern hardware at appropriate speed
- It can be used in Europe free of patent restrictions
- There is in Europe a wide experience of its use in several sectors and a multitude of industrial products with the algorithm available

SIST ENV 12388:2003

1 Scope

This European Prestandard specifies a digital signature algorithm for use in European Health Care should such an algorithm be required.

The full functionality of the use of this core algorithm for various applications, requires additional specifications of protocol elements related to the application requirements. These may be user agreements and/or may be parts of future standards for e.g. security of health care communication or health care records.

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 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 9594-8:1990	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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ENV 12388:2003
https://standards.iteh.ai/catalog/standards/sist/bda74dbf-c1f5-4a39-9ce7-a2021f23a1fa/sist-env-12388-2003

3 Definitions

For the purposes of this European Prestandard the following definitions apply.

3.1 DATA ORIGIN AUTHENTICATION: corroboration that the source of data is as claimed [ISO 7498-2].

3.2 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 that unit and protect against forgery e.g. by the recipient [ISO 7498-2].

3.3 ENTITY AUTHENTICATION: corroboration that an entity is the one claimed [ISO/IEC 9798-1].

SIST ENV 12388:2003

4 Digital signature algorithm

The algorithm defined by normative annex A shall be used as a digital signature algorithm for health care.

The public key exponent *v* shall have a value of 3.

NOTE 1: Normative annex A is identical to the *informative* annex A of ISO/IEC 9796:1991.

NOTE 2: Informative annex B and C of ISO/IEC 9796:1991 may be referred to for calculation examples using this algorithm.

NOTE 3: The same algorithm is also described in ISO/IEC 9594-8 (corresponding to CCITT rek. X.509) informative annex C, although with another text, and is frequently used for signed certificates and directory services.

NOTE 4: This algorithm is frequently referred to as RSA derived from the authors of the first description, Rivest, Shamir and Adleman (Rivest, R.L., Shamir, A. and Adleman, L. (February 1978) - A method for Obtaining Digital Signatures and Public-key Cryptosystems, Communications of the ACM, 21, 1, 120-126.)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

NOTE 5: The application of the algorithm for specific services requires additional protocol specifications, eg. for digital signatures of documents a message digest (also called hash) function is usually required. The selection of this is outside the scope of this standard.

SIST ENV 12388:2003
https://standards.iteh.ai/catalog/standards/sist/e0da7-4b39-9ce7-a2021f23a1fa/sist-env-12388-2003

SIST ENV 12388:2003

Annex A (normative)

A.1 Definitions

Modulus: Integer constructed as the product of two primes.

Public verification key: Modulus and verification exponent.

Secret signature key: Signature exponent.

Signature: string of bits resulting from the signature process

A.2 Symbols and abbreviations

RR	Representative element
IR	Intermediate integer
IR'	Recovered intermediate integer
Σ	Signature
k_s	Length of the signature in bits
IS	Resulting integer
n	Modulus
k	Length of modulus in bits
p,q	Prime factors of the modulus
v	Verification exponent
s	Signature exponent
lcm(*a*, *b*)	Least common multiple of integers a and b
(*a*|*n*)	Jacobi symbol of a with respect to n
Sign	Signature function under the control of the secret signature key
Verif	Verification function under control of the public verification key

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ENV 12388:2003
https://standards.iteh.ai/catalog/standards/sist/bda74dbf-cdf5-4a39-9ce7-a2021f25a1fa/sist-env-12388-2003

NOTE: Let *p* be an odd prime, and let *a* be a positive integer. The Legendre symbol of integer *a* with respect to prime *p* is defined by the following formula:

$$(a|p)=a^{(p-1)/2} \bmod p$$

When integer *a* is not a multiple of *p*, then the Legendre symbol of integer *a* with respect to prime *p* is valued either +1 or -1 depending on whether integer *a* is or is not a square modulo *p*.

The Legendre symbol of multiples of *p* with respect to prime *p* is null.
Let *n* be an odd positive integer, and let *a* be a positive integer. The Jacobi symbol of integer *a* with respect to integer *n* is the product of the Legendre symbols of integer *a* with respect to the prime factors of *n*.

Therefore if $n=p\,q$, then $(a|n) = (a|p)\,(a|q)$.

The Jacobi symbol of any integer *a* with respect to any integer *n* may be efficiently computed without the prime factors of *n*.

SIST ENV 12388:2003

A.3 Key production

A.3.1 Public verification exponent

Each signing entity shall select a positive integer v as its public verification exponent.

The public verification exponent may be standardized in specific applications.

NOTE: Values 2 and 3 may have practical advantages.

A.3.2 Secret prime factors and public modulus

Each signing entity shall secretly and randomly select two distinct odd primes p and q subject to the following conditions.

— if v is odd, then p-1 and q-1 shall be coprime to v.
— if v is even, then $(p-1)/2$ and $(q-1)/2$ shall be coprime to v.
Moreover, p and q shall not be congruent to each other mod 8.

The public modulus n is the product of the secret prime factors p and q.

$$n = p\,q$$

The length of the modulus is k. Number k shall equal $k_s + 1$.

NOTE 1: Some additional conditions on the choice of primes may well be taken into account in order to deter factorization of the modulus.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

NOTE 2: Some forms of the modulus simplify the modulo reduction and need less storage. These forms are

SIST ENV 12388:2003
https://standards.iteh.ai/catalog/standards/sist/bda74dbf-cdf5-4a39-9ce7-a2021f23a1fa/sist-env-12388-2003

$F_{x,y,-}$: $n = 2^{64x} - c$ of length: $k = 64x$ bits,

$F_{x,y,+}$: $n = 2^{64x} + c$ of length: $k = 64x + 1$ bits,

where : $1 \le y \le 2x$ and $c < 2^{64x - 8y} < 2c$.

In the negative forms, all the bits of the y most significant bytes are valued to one, up to a quarter of the length of the modulus.

In the positive forms, after a single most significant bit valued to one, all the bits of the y most significant bytes are valued to zero, up to a quarter of the length of the modulus.

A.3.3 Secret signature exponent

The secret signature exponent is the least positive integer s such that sv-1 is a multiple of

- lcm(p-1, q-1) if v is odd;
- ½ lcm(p-1, q-1) if v is even.