SLOVENSKI STANDARD
SIST ENV 13608-1:2003

01-oktober-2003

Zdravstvena informatika – Varnost komuniciranja v zdravstvenem varstvu - 1. del: Koncepti in izrazje

Health informatics - Security for healthcare communication - Part 1: Concepts and terminology

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: ENV 13608-1:2000

SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/ccff4c9-aff5-4d54-b9ca-0d59fe2d186c/sist-env-13608-1-2003

ICS:

01.040.35	Informacijska tehnologija. Pisarniški stroji (Slovarji)	Information technology. Office machines (Vocabularies)
35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology

SIST ENV 13608-1:2003 **en**

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

SIST ENV 13608-1:2003

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/ccff14c9-aff5-4d54-b9ca-0d59fe2d186c/sist-env-13608-1-2003

SIST ENV 13608-1:2003

EUROPEAN PRESTANDARD

PRÉNORME EUROPÉENNE

EUROPÄISCHE VORNORM

ENV 13608-1

May 2000

ICS 01.040.35; 35.040; 35.240.80

English version

Health informatics - Security for healthcare communication - Part 1: Concepts and terminology

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/ccff14c9-aff5-4d54-b9ca-0d59fe2d186c/sist-env-13608-1-2003

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

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

© 2000 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

SIST ENV 13608-1:2003

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/ccff14c9-aff5-4d54-b9ca-0d59b2d186c/sist-env-13608-1-2003

SIST ENV 13608-1:2003

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 multipart standard consists of the following parts, under the general title *Security for Healthcare Communication (SEC-COM):*

- Part 1: Concepts and Terminology
- Part 2: Secure Data Objects
- Part 3: Secure Data Channels

This standard is designed to meet the demands of the Technical Report CEN/TC251/N98-110 Health Informatics - *Framework for security protection of health care communication.*

This standard was drafted using the conventions of the ISO/IEC directive Part 3.

All annexes are informative.

Introduction

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/ccff14c9-af15-4d54-b9ca-0d59fe2d186c/sist-env-13608-1-2003

This SEC-COM standard series on Security for healthcare communication can be applied to a wide range of communication protocols and information system applications relevant to healthcare, though they are neither complete nor exhaustive in that respect.

Part 1 – Concepts and Terminology – reflects a user-requirements driven approach that provides a methodology for the analysis of the relation between 1) user needs and 2) a technological solution. It begins with a standardised way of expressing user needs, continues through technology-oriented successive refinements of the corresponding required security solutions and ends with a standard-oriented map of the corresponding recommended security solutions. Such a method can be utilised in many ways, out of which two important usages are:

1. as a common tool for breaking down user needs into technological solutions, through a process/journey of close collaboration between users and security experts, and
2. through using this common method in the standardization process, establishing a link between a defined set of user needs and a technological standard, a link that carries an *a priori* assurance on the effectiveness of the technological standards in terms of complying with the user needs. Such an *a priori* assurance will be of special value for the user that do not want to exercise the method in detail on his own, but merely want to *benefit from an established link* between a set of user needs that he/she can recognise, and the existence of an implementation standard.

Readers without a background in communications security are referred to Annex L.

The methodology is organised by means of a matrix, and the path through this matrix from the user needs to a technological solution may be viewed as the standard for the specification of a Communication Protection Profile (CPP), according to CEN/TC251/N98-110.

It is of paramount importance for the understanding of this methodology to recognise that it comprises a journey from user needs to detailed technological specifications, and that several distinct perspectives and contexts are undertaken along this journey. In particular, it is important to recognise that commonly used (already existing, e.g. ISO) standards are comparable to only a subset of the total number of contexts defined by the method. E.g. it has been necessary to introduce the concept of *auditability* for the *user need context*, because the more commonly used notion of *accountability* is perceived to have a more *limited* and *technical constitution.*

Different user views will imply different patterns of use of the matrix. For standardization purposes (to constitute a valid CPP), the matrix must be filled out in detail (however only in those parts that are applicable for a selection of

SIST ENV 13608-1:2003

user needs). This process provides some level of *assurance* that the actual technological solution is an *effective* representation of the user needs defined in the actual CPP. The method itself does not specify in detail how each specific cell of the matrix shall appear. However, Annexes B-J provide examples that may be viewed as guidelines.

Part 1 offers a set of different *views* or *journeys* through the successive refinement from user need to technological solution. The security journey on the most detailed level is a *combination* of :

1. top-down approach, by allowing for a systematic translation from a common policy expression, down to technological choices and options;
2. bottom-up approach, by being focused on utilisation of existing, commercial technologies.

Hence, the CPP concept must not be understood as a forced (one-way) development *from* user needs *to* technological solution, but merely as a (standardised) statement that gives evidential indication that a specific technological standard, is an *effective and reasonable fulfilment* of a specific set of user needs.

Hence, the normative function of Part 1 can be summarised as:

1. standardising the way of expressing a communication security policy;
2. standardising the steps of successive refinements down to the technology level, in order to provide a minimum level of assurance[1].

The benefit for a end-user is that he can look for a CPP that matches his demand for:

a. a matching set of user needs;
b. a technological context (e.g. EDI);
and successively identifies:
c. a named implementation standard (e.g. Part 2 or 3 of this Prestandard).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The user will then be assured that the standardization «rubber stamp» implicitly gives him some assurance that a product meeting the implementation standard effectively meets his user needs. Alternatively, if such a standard is not found, he/she can use the method in cooperation with security experts, to constitute a basis from which can be identified the needs and their effective solutions[2].

ENV 13608-1:2000
https://standards.iteh.ai/catalog/standards/sist/ccff14c9-aff5-4d54-b9ca-0d59fe2d186c/sist-env-13608-1-2003

Figure 1 below depicts how the matrix is used methodologically to constitute relations between user needs, technological contexts and implementation standards.

Figure 1 - The Security Policy Bridging phases

Parts 2 and 3 are examples of implementation standards that have a CPP counterpart, as they both are described in terms of Part 1 requirements (in Annex B and C). Both are based on rather simplistic technological contexts, however with a wide installed base in healthcare and with a large potential for future use. Both of them are based on commercial technologies with an existing product portfolio.

---

[1] The actual level of assurance achieved is not comparable to what can be achieved through a security evaluation process, cfr Annex K.

[2] ultimately with the potential of constituting a basis for bridging his/her communications security policy with those of communication counterparts.

SIST ENV 13608-1:2003

The method prescribed by Part 1is however open in the sense that other pairs of CPP-standard can be developed in the future – e.g. based on other technological concepts such as middleware, WWW-based systems etc.

In order to provide external coherence:

- Annex A provides some examples and illustrations of the usage of this SEC-COM part 1 in terms of general security concepts, with a refined proposal for the auditability property,
- Annexes D to J indicate what a selection of *other* security standards actually can currently offer in regard of the SEC-COM method,
- In Annex K, the relation between the assurance gained through the method, and the assurance gained in a security evaluation based on Common Criteria, is discussed,
- Annex L gives some tutorial on the introduction to cryptography used for communication security.

The CPP approach based on Part 1 can however have wider implications than described so far. However without normative implications in this standard, it is emphasised that the CPP approach may also facilitate (end-system's) *security policy bridging*, which requires a "standardised" description of the embodiment of the site security policy. In the simplest case, the Part 1 way of expressing a (communication) security policy may be a (informal) basis for deciding whether to communicate or not. Moreover, the systematic refinement of a (communication) security policy down to a more technical level constitutes the basis for a more automatic and precise decision process (semiformal). Such a process thus consists of three different steps (also illustrated in the figure below):

i. The first step is the *Terminology Linking* one, ensuring that any communicating entity will be able to use and understand a *common* security policy language,

ii. The second step is the *Policy Matching* one, ensuring that any communicating entity will be able to compare and match his own communication security policy with any peer entity's communication security policy,

iii. The third step is the *Policy Negotiation* one, ensuring that any communicating entity will be able to adapt his own communication security policy in order to be able to adopt a common communication security policy (common in that it is shared by his communication peer entities).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/ccff14c9-a0f5-4b4d-b9ca-0d59fe2d186c/sist-env-13608-1-2003

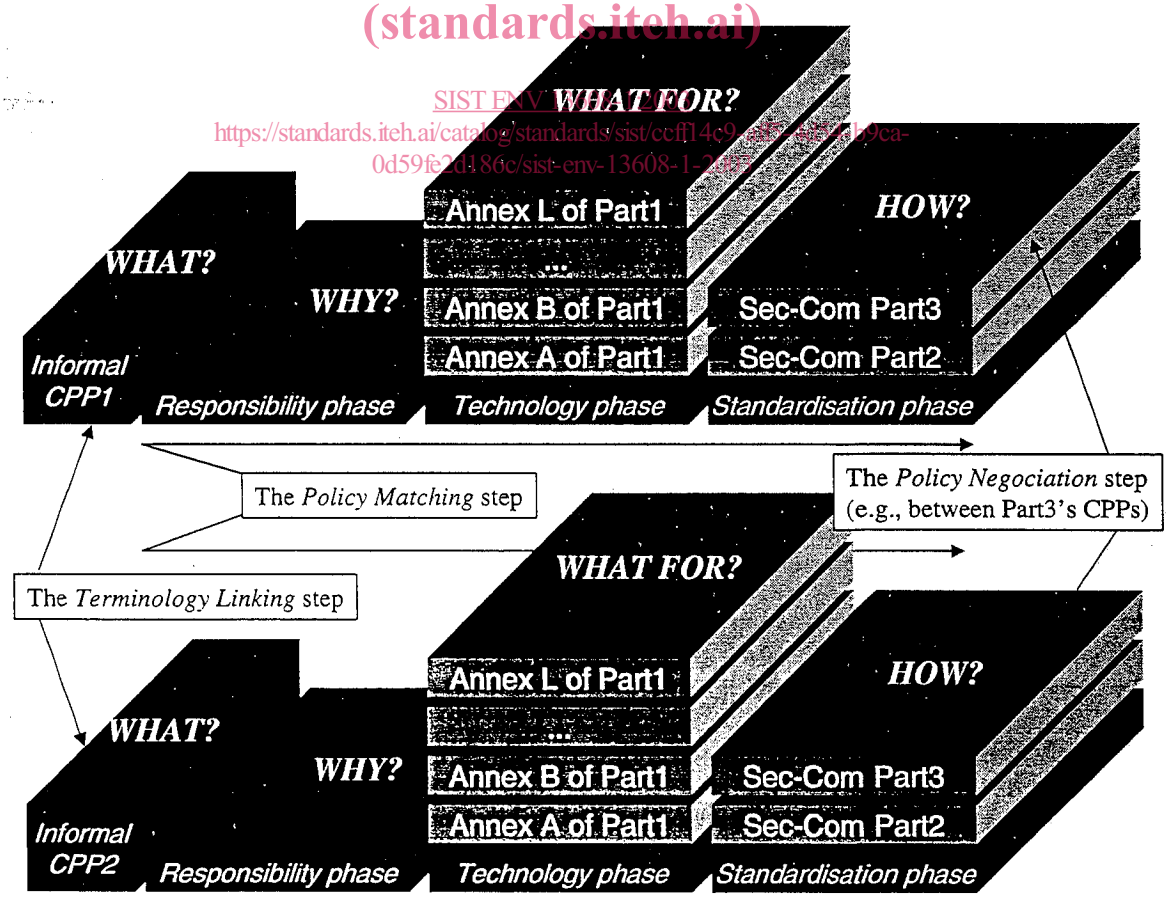

Figure 2 - The Security Policy Bridging steps

SIST ENV 13608-1:2003

Health informatics - Security for healthcare communication - Part 1: Concepts and terminology

1 Scope

This European Prestandard specifies a methodology for defining, expressing and selecting a communication protection profile (CPP) specification, and thus provides:

1. a standard way of expressing healthcare user security needs in relation to communication
2. a standard method of successive refinement of policy statements, hereby helping to identify standardised security implementation specification that can be utilised to meet these security needs.

Security aspects contained within the communication protection profile include integrity, confidentiality, and availability, and also auditability.

This methodology shall thus serve the purpose of being a tool for:

A. the end-user in collaboration with security experts, while seeking effective solutions for relevant and powerful healthcare communication security needs;
B. the standardization process in which trustworthy links between 1) actual selections of such user needs and 2) technological standards, are established.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/ccff14c9-aff5-4d54-b9ca-0d59fe2d186c/sist-env-13608-1-2003

SIST ENV 13608-1:2003

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/IEC 2382-8	Information technology – Vocabulary -- Part 8: Security (1998)
ISO 7498-2	Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture
ISO 9594-8	Information technology – Open Systems Interconnection – The Directory: Authentication framework
ISO 10181-1	Information technology - Open Systems Interconnection – Security frameworks for open systems: Overview
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 9735-4	Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules Part 4 Syntax and service report message for batch EDI (Message type – CONTRL)
ISO 9735-5	Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules Part 5 Security rules for batch EDI (Authenticity; integrity and non-repudiation of the origin)
ISO 9735-6	Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules Part 6 Secure authentication and acknowledgement message (Message type – AUTACK)
ISO 9735-7	Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules Part 7 Security rules for batch EDI (confidentiality)
ITU/CCITT X.435	Message Handling Systems: Electronic Data Interchange Messaging System (X.435 Recommendation)
ITU/CCITT F.435	Message Handling Services: Electronic Data Interchange Messaging Services (F.435 Recommendation)
PKCS#7	Cryptographic Message Syntax Version 1.5, RFC 2315
Common Criteria V2	Common Criteria for Information Technology Security Evaluation V2.0 – July 1998
ECMA TR/46	European Computer Manufacturers Association – Security in Open Systems: A Security Framework
ITSEC	Information Technology Security Evaluation Criteria – June 1991
Federal Criteria	US Federal Criteria for Information Technology Security – December 1992
TCSEC	US Department of Defence – Trusted Computer System Evaluation Criteria – Dec. 1985

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/ccff14c9-aff5-4d54-b9ca-0d59fe2d186c/sist-env-13608-1-2003

SIST ENV 13608-1:2003

3 Definitions

3.1
abstract security mechanisms

Security mechanism described in a generalised fashion, without specific choices made for algorithms

3.2
access control

A 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]]

3.3
accountability

The property that ensures that the actions of an entity may be traced uniquely to the entity [ISO 7498-2]

3.4
asymmetric cryptographic algorithm

An algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ [ISO 10181-1]

3.5
auditability

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The property that ensures that any action of any security subject on any security object may be examined in order to establish the real operational responsibilities

NOTE In the SEC-COM series the *auditability* property, considered as encompassing several sub-properties contributing to the transfer of responsibility in the message transport system and also proving authorship, is not defined as synonymous with the classical *accountability* property, but as encompassing it as indicated by its refinement in the informative annex A.

3.6
authentication

Process of reliably identifying security subjects by securely associating an identifier and its authenticator.
See also data origin authentication and peer entity authentication [ISO 7498-2]

3.7
authenticator

Piece of information that confirms a claimed identity by transforming a successful identification into a successful authentication

3.8
authorization

The granting of rights, which includes the granting of access based on access rights [ISO 7498-2]

3.9
availability

Property of being accessible and useable upon demand by an authorised entity [ISO 7498-2]

3.10
certificate distribution

Act of publishing certificates and transferring certificates to security subjects

SIST ENV 13608-1:2003

3.11
certificate generation
Act of creating certificates

3.12
certificate management
Procedures relating to certificates: certificate generation, certificate distribution, certificate archiving

3.13
certificate revocation
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 whereas it is unexpired

3.14
certificate holder
An entity that is named as the subject of a valid certificate

3.15
certificate user
An entity that needs to know, with certainty, the public key of another entity [ISO 9594-8]

3.16
certificate verification
Verifying that a certificate is authentic

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.17
certification
Use of digital signature to make transferable statement about beliefs of identity, or statements about delegation of authority

SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/cc1f4c9-af5-4d54-b9ea-0d59fe2d186c/sist-env-13608-1-2003

3.18
certification authority
An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys [ISO 9594-8]

3.19
ciphertext
Data produced through the use of encipherment. The semantic content of the resulting data is not available [ISO 7498-2]

3.20
ciphersuite
An encoding for the set of bulk data cipher, message digest function, digital signature algorithm and key exchange algorithm used within the negotiation phase of TLS

3.21
communication destination
destination
A security subject involved in a communication in the general sense that it is the address to which the sensitive information is sent by other security subject

SIST ENV 13608-1:2003

3.22
communication originator
originator

A security subject involved in a communication in the generic sense that it is the origin from where the sensitive information is sent to other security subjects

3.23
communication transporter
transporter

A security subject involved in a communication which is contractually responsible for transporting sensitive information from communicating senders to communicating receivers

3.24
communication protection profile
CPP

A statement of systematic translation form communication security needs to technological concepts

3.25
communicating sender
sender

A security subject involved in a communication which is legally responsible for sending sensitive information to other security subjects

NOTE *Sender* is a special case for *Originator*, in the restricted sense of active communication entity.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.26
communicating receiver
receiver

SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/ccff14c9-aff5-4d54-b9ca-0d59fe2d186c/sist-env-13608-1-2003

A security subject involved in a communication which is legally responsible for receiving sensitive information from other security subjects

NOTE *Receiver* is a special case of *Destination* in the restricted sense of an active communication entity.

3.27
communicating carrier
carrier

A security subject involved in a communication which is legally responsible for transporting sensitive information from communicating senders to communicating receivers

NOTE *Receiver* is a special case of *Transporter* in the restricted sense of an active communication entity.

3.28
communication third party
repository

A security subject optionally involved in a communication which is legally responsible for notarisation of information to provide an independent attestation of a security property where a conflict of interests potentially exists between the communicating parties

NOTE a *Repository*, in the sense of an active communication entity for which legally notarisation responsibility has been recognised by all the communicating parties, is a case of third party for the communication context.

SIST ENV 13608-1:2003

3.29
communication security
Security of security objects communicated between security subjects

3.30
confidentiality
The property that information is not made available or disclosed to unauthorised individuals, entities, or processes [ISO 7498-2]

3.31
cryptography
The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use [ISO 7498-2]

3.32
cryptographic algorithm
cipher
an algorithm used to transform data to hide its information content which is used in the process of encryption (see 3.37)

3.33
data integrity
The property that data has not been altered or destroyed in an unauthorised manner [ISO 7498-2]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.34
data origin authentication
The corroboration that the source of data received is as claimed [ISO 7498-2]

SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/ccff14c9-aff5-4d54-b9ca-0d59fe2d186c/sist-env-13608-1-2003

3.35
decryption
decipherment
Process of making encrypted data reappear in its original unencrypted form. The reversal of a corresponding reversible encipherment

3.36
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]

3.37
encryption
encipherment
The cryptographic transformation of data (see cryptography) to produce ciphertext [ISO 7498-2]

3.38
end-user's security needs
Security requirements from the end user's domain specific viewpoint

NOTE 1 They are typically informally expressed since the end-user will express them in terms of his application domain and it's native terminology.

SIST ENV 13608-1:2003

NOTE 2 The primary objective of the security policy, from the end-user's point of view, is for the end users security needs to be satisfied.

3.39
forward secrecy

Technique of ensuring that the communicated data are only decipherable for a limited time span by the communicating parties. After that time the communicating parties typically achieve forward secrecy by destroying cryptographic keys. This prevents an attacker from coercing the communicating parties into decrypting old ciphertext.

3.40
generic security functionalities

Set of semi-formal security functionalities

NOTE A semi-formal security specification is in between an informal formulation of security requirements and a formal implementation of security mechanisms.

3.41
hash function

A (mathematical) function that maps values from a (possibly very) large set of values into a smaller range of values [ISO 10181-1]

3.42
human-intrinsic risks

Security threats arising from human involvement in the system

iTeh STANDARD PREVIEW
(standards.iteh.ai)

NOTE 1 They are intrinsically human-dependent since they come from required human involvement in the system.

SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/cdff4c9-ad5-4d54-b9ea-0d59fe2d186c/sist-env-13608-1-2003

NOTE 2 The first objective of any security policy is to minimise the threats posed by human intrinsic activity.

3.43
identification

Process of identifying the security subjects attributes, such as name, address, or other subject attributes

3.44
identifier

Piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

3.45
integrity

The property of being unmodified by any kind of unauthorised security subject

3.46
key

A sequence of symbols that controls the operations of encipherment and decipherment [ISO 7498-2]

3.47
key certification

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

SIST ENV 13608-1:2003

3.48
key distribution
Process of publishing, or transferring to other security subjects a cryptographic key

3.49
key exchange algorithm
An algorithm used to derive a shared secret over an open communications channel

3.50
key generation
Process of creating a cryptographic key

3.51
key management
The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy [ISO 7498-2]

3.52
message recovery
Process of a third party decrypting an encrypted message

3.53
one-way function
A (mathematical) function that is easy to compute but, when knowing a result, it is computationally infeasible to find any of the values that may have been supplied to obtain it [ISO 10181-1]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.54
one-way hash function
A (mathematical) function that is both a one-way function and a hash function [ISO 10181-1]

SIST ENV 13608-1:2003
https://standards.iteh.ai/catalog/standards/sist/ccff14c9-aff5-4d54-b9ca-0d59fe2d186c/sist-env-13608-1-2003

3.55
peer entity authentication
The corroboration that a peer entity in an association is the one claimed [ISO 7498-2]

3.56
plaintext
Intelligible data, the semantic content of which is available

3.57
pragmatic security protocols
Set of formal security features or characteristics when expressed in a non-ambiguous language with the detailed description of implementation options and parameter usage

3.58
private key
A key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity) [ISO 10181-1]

3.59
public key
A key that is used with an asymmetric cryptographic algorithm and that can be made publicly available [ISO 10181-1]