SLOVENSKI STANDARD
SIST EN 17646:2022

01-oktober-2022

Varnostne shranjevalne enote - Klasifikacija visoko varnostnih ključavnic po odpornosti proti nepooblaščenemu odpiranju - Porazdeljeni sistemi

Secure storage units - Classification for high security locks according to their resistance to unauthorized opening - Distributed systems

Wertbehältnisse - Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen - Verteilte Systeme

Unités de stockage en lieu sûr - Classification des serrures haute sécurité en fonction de leur résistance à l'effraction - Systèmes répartis

Ta slovenski standard je istoveten z: **EN 17646:2022**

ICS:

13.310	Varstvo pred kriminalom	Protection against crime

SIST EN 17646:2022 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 17646

August 2022

ICS 13.310

English Version

Secure storage units - Classification for high security locks according to their resistance to unauthorized opening - Distributed systems

Unités de stockage en lieu sûr - Classification des serrures haute sécurité en fonction de leur résistance à l'effraction - Systèmes répartis

Wertbehältnisse - Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen - Verteilte Systeme

This European Standard was approved by CEN on 27 June 2022.

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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

This document (EN 17646:2022) has been prepared by Technical Committee CEN/TC 263 “Secure storage of cash, valuables and data media”, the secretariat of which is held by BSI.

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 2023, and conflicting national standards shall be withdrawn at the latest by February 2023.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

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

1 Scope

This document is applicable to Distributed Systems (DS), i.e. high security locks with components which have a wired or wireless connection via a transmission system in order to execute fixed operating conditions using different individually fixed access possibilities.

Products which are to be tested on the basis of this document comply with the generally recognized state of the art at the time of testing. Due to the short innovation cycles in the field of electronic and, in particular, information technology applications, the technical possibilities available at the time of product development should also be taken into account during implementation.

Distributed systems can be used, for example, to operate high security locks of secure storage units (safes and strongrooms).

High security locks (HSL) are used in DS as locking unit.

This document does not apply for stand-alone HSL, which are not part of a distributed system. For these stand-alone HSL EN 1300 is applicable only.

The document will be revised with a frequency of 3 years as the research in the area of cryptography and relevant attacks evolve with high speed as well as the referenced standards.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

EN 1300, *Secure storage units - Classification for high security locks according to their resistance to unauthorized opening*

EN 1143-1, *Secure storage units - Requirements, classification and methods of test for resistance to burglary - Part 1: Safes, ATM safes, strongroom doors and strongrooms*

EN 1143-2, *Secure storage units - Requirements, classification and methods of tests for resistance to burglary - Part 2: Deposit systems*

EN ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 1300 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
remote input unit
rIU
additional component which allows information to be entered from a remote location and is intended for exclusive use in a distributed system

Note 1 to entry: Input units (IU) are defined in EN 1300.

3.2
condition as supplied
status of a DS or a component of a DS before the first customer-specific modification has been carried out except for software/firmware updates, which can remain in effect

3.3
authenticity
quality that ensures, for example, that a communication partner is who they claim to be; for authentic information it is ensured that it was created by the specified source

3.4
authentication factor
category of credential (knowledge factors (e.g. a password), possession factors (e.g. a card) or inherence factors (e.g. biometric characteristics)) that is intended to verify that an entity requesting an access is who they are declared to be

3.5
authorized user
person who is identified by input of the required information as being authorized for a certain action

3.6
independent component
component of a DS that has an active influence on the data processing as well as the security state of the DS and that is absolutely necessary for the intended use of the DS

3.7
extraneous component
EC
component of a DS which is not manufactured especially for the DS but is used in the DS as a functional unit

Note 1 to entry: For example, public components of a transmission path or office computers may be used as extraneous components.

3.8
data processing unit
DPU
system for processing, managing and/or storing of information

Note 1 to entry: In order to minimize the risk of unauthorized access to security relevant information by third parties, it is strongly recommended that a DPU is used exclusively within the direct sphere of influence of the operator.

3.9
communication path
CP
transmission path for the exchange of information between the remote input unit and the processing unit including the intermediary stored data processing units

3.10
authentication of components
coupling of two communication partners by using unique identification features

3.11
security-relevant information
codes (e. g. opening, recognized, duress, parallel codes, cryptographic keys), authentication information (e. g. passwords), data on software/firmware updates

3.12
locking device
LD
component which directly or indirectly allows the physical lock (locking) of further components, e. g. a door or a boltwork

3.13
monitoring entry
stored information on a defined event within the DS with the indication of:

— causing event;

— time/date of event;

— triggering operator/triggering component

3.14
distributed system
DS
components operating as a unit, locally separated and aimed at the systematic implementation of a common aim

Note 1 to entry: The exchange of information between the components can be wired or wireless.

3.15
deliberate action
conscious action of a person to confirm a status change

Note 1 to entry: A deliberate action may be, for example, the pushing of an operating button, the input of a (confirmation) code or the turning of a handle.

3.16
access-secured area
area of a secure storage unit which, due to the physical properties, is not accessible when the product is closed and not accessible trace-free in the open state

Note 1 to entry: For example, this can be the inside of a safe door that has a mechanical cover even when the door is open.

3.17
two factor authentication
method for authenticating a user, service or component by means of two different authentication factor types

Note 1 to entry: Examples of authentication factors can be found in the corresponding definition.

4 Symbols and abbreviations

For the purposes of this document, the following symbols and abbreviations apply.

ANSSI:	Agence nationale de la sécurité des systèmes d'information (National Cybersecurity Agency of France)
BSI (DE):	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CP:	communication path
DPU:	data processing unit
DS:	distributed system
EC:	extraneous component
ENISA:	European Union Agency for Network and Information Security
HSL:	high security lock
IU:	input unit
LD:	locking device
NIST:	National Institute of Standards and Technology
PU:	processing unit
rIU:	remote input unit

5 Classification

Distributed systems are divided into four classes A (DS), B (DS), C (DS) and D (DS). For DS of class A (DS) the lowest requirements are applicable, for those of class D (DS) the highest requirements are applicable.

For an approved distributed system, the component with the lowest classification relating to LD, PU, IU and rIU determines the class of the entire distributed system.

6 Requirements

6.1 General

6.1.1 General

For HSL operated in distributed systems according to this document, the requirements of EN 1300 apply in principle. The classification level achieved by an HSL according to EN 1300 determines the maximum possible class for this document (see Table 1). For the components inside of the secure storage unit Annex A is applicable.

Table 1 — Connection between EN 1300 and this document

Classes of this document	The requirements of the following classes of EN 1300 shall be fulfilled
A (DS)	A, B, C or D
B (DS)	B, C or D
C (DS)	C or D
D (DS)	D

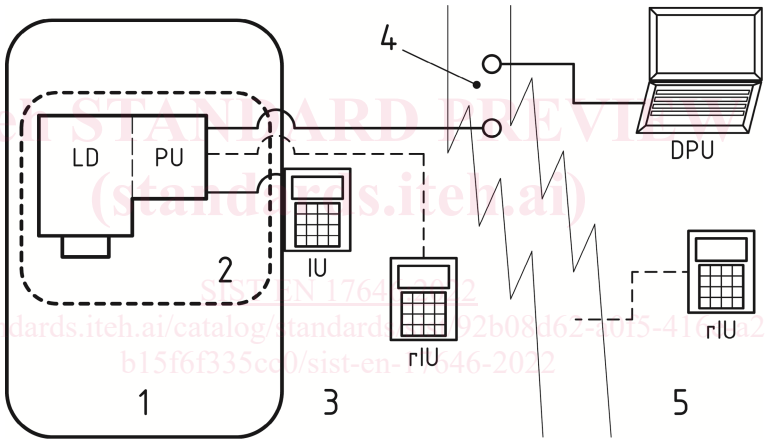
In case of conflicting requirements between EN 1300 and this document, this document prevails. Where possible and applicable, reference is made to the corresponding clauses of EN 1300.

This document specifies requirements for independent components (see 6.2 to 6.4) and extraneous components (see 6.5).

This document refers to the term state of the art. The state of the art shall be based on recommendations of relevant publications of accepted organizations like European Union Agency for Network and Information Security (ENISA), the German Federal Office for Information Security (BSI), the French National Agency for Information Systems Security (ANSSI) or the National Institute of Standards and Technology (NIST).

6.1.2 Construction

DS have a basic structure consisting of a processing unit (PU), a locking device (LD), an input unit (IU) as well as the communication paths (CP) which could be public or local networks and, if applicable, a data processing unit (DPU) or a remote input unit (rIU) or both. It is possible that these components exist more than once in the system. The structure is not predefined in detail, but is based on the representation in Figure 1.



Key

1 secure storage unit
2 access-secured area
3 local area
4 network
5 remote area

Figure 1 — Principle of a distributed system

Independent components with the exception of the IU, the rIU and the DPU, shall be located in the access secured area of the DS.

The arrangement of the components shall be such that unauthorized access to these components can be detected (e.g. by breaking a seal) even when the safe-storage space is properly opened.

6.2 System administration

6.2.1 Administrative procedures

Configuration and service activities around the DS such as:

— initialization;

— configuration (e.g. integration of new components);

— setting up a time slot;

— setting the opening delay;

— administration of users;

— administration of user rights;

— back-up (and if applicable restoring);

— reset of hardware, if applicable;

shall be performed exclusively by authorized users (according to 6.2.7).

If an HSL also provides product-specific functions through which data can be accessed at any location of the DS, these functions may also only be performed by authorized users (according to 6.2.7).

All configuration and service activities mentioned above as well as any additional product-specific functions shall generate a monitoring entry in accordance with the requirements of 6.2.9.

System-wide, the entry of codes is only permitted via specially designed and protected components (IU or rIU according to 6.2.11).

6.2.2 Confirmation of remotely initiated security relevant operating procedures

The following security-relevant operating procedures shall (if remotely initiated) be confirmed by means of a deliberate action from an authorized user at the IU:

— authentication of components;

— unlocking the HSL;

— configuring hardware during initial commissioning;

— modifying hardware after initial commissioning;

— resetting the system to the condition as supplied.

For the following security-relevant operations it is sufficient if the deliberate action from an authorized user within the DS is performed on one lock for this lock as well as for further locks of the same or a lower class:

— changing the user code;

— activating new users.

The deliberate action shall generate an event entry according to 6.2.9.