SLOVENSKI STANDARD

oSIST prEN 1300:2017

01-marec-2017

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

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

Wertbehältnisse - Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen

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

Ta slovenski standard je istoveten z: prEN 1300

ICS:

13.310	Varstvo pred kriminalom	Protection against crime

oSIST prEN 1300:2017 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 1300

February 2017

ICS 13.310

Will supersede EN 1300:2013

English Version

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

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

Wertbehältnisse - Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 263.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

European foreword 4
Introduction 6
1 Scope 7
2 Normative references 7
3 Terms and definitions 8
4 Classification 13
5 Requirements 13
5.1 General requirements 13
5.1.1 Requirements for all classes 13
5.1.2 Class D HSL 14
5.1.3 Mechanical Key Operated HSL 14
5.1.4 Lift heights for mechanical key locks 14
5.1.5 Electronic HSL 15
5.1.6 Electronic tokens 15
5.1.7 Requirements for cryptography in distributed security systems 17
5.1.8 Firmware updates 18
5.2 Security requirements 19
5.2.1 Usable codes 19
5.2.2 HSL having over ride feature 19
5.2.3 Manipulation resistance 19
5.2.4 Destructive burglary resistance 19
5.2.5 Spying resistance 19
5.2.6 Electrical and electromagnetic resistance 20
5.2.7 Physical environmental resistance 20
5.2.8 Temperature resistance 20
5.3 Reliability requirements 22
6 Technical documentation 23
7 Test specimens 24
8 Test methods 24
8.1 General 24
8.1.1 General 24
8.1.2 Evaluation by inspection 24
8.1.3 Test procedure 25
8.2 Security tests 26
8.2.1 Usable codes 26
8.2.2 Manipulation resistance 26
8.2.3 Destructive burglary resistance 29
8.2.4 Spying resistance 29
8.2.5 Electrical and electromagnetic resistance 30
8.2.6 Physical environmental resistance 31

8.2.7 Temperature Resistance 32
8.3 Reliability testing 33
8.3.1 Cycling 33
8.3.2 Code changes 33
8.3.3 Dynamic code input of mechanical combination HSL 34
9 Test report 34
10 Marking 35
Annex A (normative) Parameters for installation and operating instructions 36
A.1 Installation instructions 36
A.2 Operating instructions 37
Annex B (normative) Determination of manipulation resistance due to the design requirement 38
B.1 General 38
B.2 Key locks 38
B.2.1 General 38
B.2.2 Gate clearance 38
B.2.3 Bolt stump 42
B.2.4 False notches 42
B.2.5 Additional design requirements 43
B.3 Mechanical combination locks 43
B.3.1 General 43
B.3.2 Fence 44
B.3.3 Wear test 45
Annex C (normative) Manufacturer’s Declaration 46
Annex D (informative) Typical locking device dimensions 48
Annex E (normative) Determination of burglary resistance due to design requirements 49
E.1 General 49
E.2 Electronic HSL with separate processing unit not included in the lock case 49
E.2.1 Scope of design requirement 49
E.2.2 Design requirement 49
Annex F (normative) Firmware declaration 50
Annex G (informative) A-deviations 51
Bibliography 54

European foreword

This document (prEN 1300:2017) 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 document is currently submitted to the CEN Enquiry.

This document will supersede EN 1300:2013.

In comparison with EN 1300:2013, the following changes have been made:

General changes:

— references have been updated in Clause 2;

— definitions in Clause 3 have been added (locking element, unsecured condition, firmware and application software). Other definitions have been defined more precisely;

— Clarifications in 5.1.1.4, 5.1.4.1, 5.1.4.3, 5.1.5.8, 5.1.7.2.1, 5.2.6.3, Clause 6, 8.2.5.8, 8.2.6.1, Clause 10 and Figure 1, Annex D.

Technical changes for any type of lock:

— the requirements for HSL with more than one mode of authentication have been added in 5.2.1

— the shock test has changed (see 8.2.6.2);

— the immersion test is changed and now done with salt water (see 8.2.6.3);

— Cycling test has been updated (see 8.3.1.1);

— The manipulation test has been renewed. A third basic value has been added (see 8.2.2.5) and the power supply test is now required for electronic locks (5.1.5.9 and 8.2.5);

— The manufacturers declaration in Annex C has been updated.

Technical changes for mechanical key operated locks:

— The requirements for the production of mechanical key operated HSL have been raised (see 5.1.3.1.

Technical changes for electronic locks:

— New requirements for electronic HSL have been added for instance in 5.1.5.1, 5.1.5.2, 5.1.5.9, 5.2.6.1, 5.2.6.3, Table 2. 8.2.5.5, 8.2.5.6, 8.2.6.4, 8.2.6.5 and Annex A. This includes a new EMC test with higher frequency.

— Requirements for one-time-code locks have been added in 5.1.5.10 and Annex A

— The requirements of class A locks of the type “electronic token” and “distributed system” have been raised to the requirements of class B (see 5.1.6.4, 5.1.7.1.6, 5.1.7.1.8, 5.1.7.1.9.1 and 5.1.7.2.2)

— Requirements for the viewing protection of distributed systems have been added.

- Requirements for firmware and firmware updates have been added in 5.1.8, Table 1 and in Annex F ("firmware declaration").

- Design requirements for a certain type of electronic lock have been added in new Annex E.

This document reflects the market demand to include requirements for distributed systems and electronic locks and responds to the state of the art requirements when it was written down.

This European Standard has been prepared by the Working Group 3 of CEN/TC 263 as one of a series of standards for secure storage of cash valuable and data media. Other standards in the series are, among others:

- EN 1047-1, *Secure storage units — Classification and methods of test for resistance to fire — Part 1: Data cabinets and diskette inserts*

- EN 1047-2, *Secure storage units — Classification and methods of test for resistance to fire — Part 2: Data rooms and data container*

- 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 test for resistance to burglary — Part 2: Deposit systems*

- EN 14450, *Secure storage units — Requirements, classification and methods of test for resistance to burglary — Secure safe cabinets*

Introduction

This European Standard also specifies requirements for high security electronic locks (HSL) which are controlled remotely. Regarding distributed systems, this standard responds to the state of the art requirements when it was written down. It is mandatory that the standard has to 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.

1 Scope

This European Standard specifies requirements for high security locks (HSL) for reliability, resistance to burglary and unauthorized opening with methods of testing. It also provides a scheme for classifying HSL in accordance with their assessed resistance to burglary and unauthorized opening.

It applies to mechanical and electronic HSL. The following features may be included as optional subjects but they are not mandatory:

a) recognized code for preventing code altering and/or enabling/disabling parallel codes;

b) recognized code for disabling time set up;

c) integration of alarm components or functions;

d) remote control duties;

e) resistance to attacks with acids;

f) resistance to X-rays;

g) resistance to explosives;

h) time functions.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 1143-1:2012, *Secure storage units - Requirements, classification and methods of test for resistance to burglary - Part 1: Safes, ATM safes, strongroom doors and strongrooms*

EN 60068-2-1, *Environmental testing - Part 2-1: Tests - Test A: Cold (IEC 60068-2-1)*

EN 60068-2-2, *Environmental testing - Part 2-2: Tests - Test B: Dry heat (IEC 60068-2-2)*

EN 60068-2-6, *Environmental testing - Part 2-6: Tests - Test Fc: Vibration (sinusoidal) (IEC 60068-2-6)*

EN 61000-4-2, *Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test (IEC 61000-4-2)*

EN 61000-4-3, *Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test (IEC 61000-4-3)*

EN 61000-4-5, *Electromagnetic compatibility (EMC) — Part 4-5: Testing and measurement techniques — Surge immunity test (IEC 61000-4-5)*

EN ISO 6988, *Metallic and other non-organic coatings - Sulfur dioxide test with general condensation of moisture (ISO 6988)*

ISO/IEC 9798-1:2010, *Information technology — Security techniques — Entity authentication — Part 1: General*

ISO/IEC 9798-2, *Information technology — Security techniques — Entity authentication — Part 2: Mechanisms using symmetric encipherment algorithms*

ISO/IEC 9798-4, *Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
High Security Lock
HSL
independent assembly normally fitted to doors of secure storage units

Note 1 to entry: Codes can be entered into an HSL for comparison with memorized codes (processing unit). A correct match of an opening code allows movement of a blocking feature.

3.2
code
identification information required which can be entered into a HSL and which, if correct, enables the security status of the HSL to be changed

3.2.1
opening code
identification information which allows the HSL to be opened

3.2.2
recognized code
identification information which allows access to the processing unit and which may also be an opening code

Note 1 to entry: Master codes, manager codes, authorization codes and services codes may fall under recognized codes

3.2.3
duress code
parallel code which initiates some additional function

3.2.4
parallel code
opening code which has identical function to that of an existing opening code but constructed of different figures

3.3
coding means
method by which the code is held

3.3.1
material code
code defined by the physical features or other properties of a token

3.3.2
mnemonic code
remembered code consisting of numeric and/or alphabetic information

3.3.3
biometric code
code comprising human characteristics

3.3.4
one time code
code changing after each use generated by use of an algorithm

3.4
input unit
part of an HSL which communicates codes to a processing unit

3.5
processing unit
part of an HSL which evaluates whether the input code is correct and enables or prevents movement of a locking device

3.6
locking device
mechanical unit as part of the HSL that contains the blocking feature

Note 1 to entry: An example of a locking device is shown in Annex D.

3.7
token
object whose physical form or properties defines a recognized code, e.g. a key

Note 1 to entry: An electronic token incorporates an integrated circuit containing volatile and non-volatile memory, associated firmware/software and in many cases a microcontroller which communicates with an input unit by contact or contactless means.

3.8
mechanical HSL
HSL which is secured by means of mechanical elements only

3.9
electronic HSL
HSL which is secured partly or fully by electrical or electronic elements

3.10
blocking feature
part of a HSL which, after inputting the correct opening code moves, or can be moved, typically this is a bolt

Note 1 to entry: A blocking feature either secures a door or prevents movement of a boltwork. The bolt of a mechanical lock is an example of a blocking feature.

3.11
locking element
part of the HSL which enables the blocking feature to be moved

EXAMPLES Levers, spindles, wheels, motors, solenoids

3.12
destructive burglary
attack which damages the HSL in such a manner that it is irreversible and cannot be hidden from the authorized user

3.13
reliability
ability to function and achieve the security requirements of this standard after a large number of duty cycles

3.14
manipulation
method of attack aimed at removing the blocking function without causing damage obvious to the user

Note 1 to entry: A HSL may function after manipulation although its security could be permanently degraded.

3.15
spying
attempt to obtain unauthorized information

3.16
usable codes
codes or tokens permitted by the manufacturer and conforming to the requirements of this standard

Note 1 to entry: For mechanical HSL the number of usable codes is much less than the total number of codes to which the HSL can be set.

3.17
scrambled condition
coding elements are not in the configuration necessary for the HSL to be opened without entering the complete correct code or proper token

3.18
locking sequence
series of actions which start with an open door and are complete when the door is closed, bolted, locked and secure

3.19
open door
door is not in its frame

3.20
closed door
door is within its frame ready for throwing its bolt(s)

3.21
bolted door
bolts are thrown

3.22
locked door
boltwork cannot be withdrawn because of the HSL

3.23
secured door
door is closed, bolted and locked with an HSL in the secured HSL condition

3.24
secured HSL condition
blocking feature is thrown and can only be withdrawn after entering the opening code(s)

3.25
unsecured HSL condition
HSL not being in secure HSL condition

3.26
normal condition
after testing, the HSL specimen is in the secured HSL condition, and all design functions are operating

3.27
operating condition
after testing, the HSL specimen is in the secured HSL condition and can be unlocked with the opening code(s), but not all design functions are operable

3.28
fail secure
after testing, the HSL specimen is in the secured HSL condition, but not all design functions are operable therefore it cannot be unlocked with the opening code(s)

3.29
resistance unit
RU
value for burglary and manipulation resistance

Note 1 to entry: It shows a calculated result from using a tool with a certain value over a period of time.

3.30
penalty time
time delay because of time exceeding the limit of trials

3.31
authentication
method to prevent fraud by ensuring that communication with components of a distributed system can only be established after the identity of the components have been properly confirmed

3.32
cryptographic algorithm
mathematical method for the transformation of data that includes the definition of parameters (e.g. key length and number of iterations or rounds)

3.32.1
asymmetric cryptographic algorithm
cryptographic algorithm that uses two related keys, a public key and a private key, which have the property that deriving the private key from the public key is computationally infeasible

3.32.2
symmetric cryptographic algorithm
cryptographic algorithm that uses a single secret key for both encryption and decryption

3.33
cryptographic key
parameter used in conjunction with a cryptographic algorithm which is used to control a cryptographic process such as encryption, decryption or authentication

Note 1 to entry: Knowledge of an appropriate key allows correct en- and/or decryption or validation of a message.

3.34
cryptographic module
set of hardware and firmware/software that implements security functions for distributed systems and electronic tokens including cryptographic algorithms

3.35
distributed system
system with components connected by a transmission system, wired or wireless

Note 1 to entry: It is assumed that the transmitted information can be accessed by a third party. A high security lock with components in separate locations is defined as distributed system. A lock system with two input units, one on the safe and the other remote (= distributed input unit) is an example of a distributed system). An electronic lock with a non-accessible transmission system in the sense of 5.1.5.3 of this standard or with a temporary on-site wired connection to a mobile device (e.g. Personal Computer) supervised by an authorized person is not considered as a distributed system.

3.36
encryption
procedure that renders the contents of a message or file unintelligible to anyone not authorized to read it

Note 1 to entry: During the encryption procedure, a cryptographic algorithm using the cryptographic key is used to transform plaintext into cipher text. This procedure is composed of:

— the mode of operation, describing the way to process data with the algorithm;

— the padding scheme, describing the way to fill up data strings to a defined length.

3.37
transmission system
communication system between the elements of a distributed system

Note 1 to entry: Dedicated lines, wired and wireless public switched networks may be used as the transmission path.