SLOVENSKI STANDARD
oSIST prEN 1300:2022

01-februar-2022

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 1300:2022 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT prEN 1300

December 2021

ICS 13.310 | Will supersede EN 1300:2018

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, 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.

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: Rue de la Science 23, B-1040 Brussels

Ref. No. prEN 1300:2021 E

Contents

page

European foreword

This document (prEN 1300:2021) 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 1300:2018.

In comparison with EN 1300:2018, the following changes have been made:

General changes:

— references have been updated in Clause 2;

— definitions in Clause 3 have been added (opening event, opening related event, relevant audit information, non relevant audit information). Other definitions have been updated (secured HSL condition, fail secure, authentication, firmware);

— editorial changes for clarification in 5.1.5.1, 5.1.5.3, 5.1.6.6, 5.2.1, 5.2.6.4, 8.2.4.3.2, B.2.4 and Table 2.

Technical changes for any type of lock:

— updating requirement for indication of blocking status (5.1.2.5 and Annex A);

— changing test requirement from “normal condition” to “operating condition” in several clauses (see 5.2.8.1, 5.2.8.2, 8.2.5.1, 8.2.5.2, 5.3.1, 5.3.3, 8.2.6.1, 8.2.6.3.2, 8.2.6.3.3, 8.2.7.1, 8.2.7.2, 8.3.1.1, 8.3.2.1 and 8.3.3.1);

— number of test specimens changed from four to seven (see 7.1).

Technical changes for electronic locks:

— removal of requirements regarding distributed systems into the European Standard prEN 17646 (see Clause 1, 5.2.5.2, 5.2.5.4, Annex A, Annex F);

— raising encryption requirements for contactless electronic tokens for class B (from 64 bits to 128 bits, see 5.1.7.2.3) and for all classes, if the range is more than 15 cm (shall be tested according to prEN 17646, see 5.1.7.2.1);

— Clause 5.1.7.2.4 is now also applicable for contacted electronic tokens (5.1.7.3);

— new minimum requirements for recording events (see 5.1.6.2);

— updating requirements for local firmware updates (see 5.1.8);

— adding tolerance for usable codes for electronic locks (see Table 1);

— including new requirements for the manipulation of electronic locks and mechanical locks with electronic components 5.2.5.4, 8.2.2.1, Table 4 and Annex B;

— minor updates in 5.1.6.7.

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 document 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 document 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 document 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. For electronic locks used in a distributed system, see prEN 17646 for further information.

The following features can 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 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 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*

prEN 17646, *Secure storage units — Classification for high security locks according to their resistance to unauthorized opening — distributed systems*

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

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

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

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

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

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

EN ISO 6988, *Metallic and other non-organic coatings - Sulfur dioxide test with general condensation of moisture (ISO 6988:1985)*

ISO/IEC 9798-2, *IT Security techniques — Entity authentication — Part 2: Mechanisms using authenticated encryption*

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

NIST/SP 800-57, *Recommendation for Key Management — Part 1: General*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
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 inside of the secure storage unit that contains the blocking feature, the lock case, the lock cover and other mechanical and/or electronic parts

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

EXAMPLE: 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 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 which is not in its frame

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

3.21
bolted door
closed door where the bolts of the boltwork are thrown, but the HSL may still be open

3.22
locked door
bolted door where the boltwork cannot be withdrawn because of the HSL locking device being thrown

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

3.24
secured HSL condition
the blocking feature is thrown and the HSL has been locked and scrambled

3.25
unsecured HSL condition
HSL not being in secure HSL condition

3.26
operating condition
HSL specimen is in the secured HSL condition and can be unlocked with the opening code(s), but not all design functions are operable

3.27
fail secure
HSL specimen is in the secured HSL condition, but not all design functions are operable therefore it might not be unlocked with the opening code(s)

3.28
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.

3.29
penalty time
time delay because of time exceeding the limit of trials

3.30
authentication
method to prevent fraud by ensuring that communication can only be established after the identity of the components have been properly confirmed

3.31
cryptographic algorithm
mathematical method for the transformation of data that includes the definition of parameters

EXAMPLE Key length and number of iterations or rounds.

3.31.1
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

3.31.2
symmetric cryptographic algorithm
cryptographic algorithm that uses a single secret key for both encryption and decryption

3.32
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.

3.33
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 5.1.6.3 of this standard or with a temporary on-site wired connection to a trusted device (e.g. trusted Personal Computer) supervised by an authorized person is not considered as a distributed system.

3.34
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

3.35
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.

3.36
security relevant information
codes according to 3.2, authentications, any code or key transmissions and changes as well as firmware updates of input and processing units

3.37
firmware
software code that operates the processing or input units of the HSL

3.38
trusted device
wire-connected device, on which no unauthorised person will have access to security-relevant information

3.39
opening event
entry of an authorized code with the aim to change the HSL to unsecured HSL condition

Note 1 to entry: The entry of an authorized code with the intention to change settings or for other purposes than changing to unsecured HSL condition is not an opening event (for instance changing the time, adding users etc).

3.40
opening related event
recorded event, which is directly connected to an opening

EXAMPLES Entering an opening code, entering a partial opening code (dual code function), presenting a token (for single or two factor authentication), activating the blocking unit after entering opening code, opening the blocking device, changing HSL to secured condition, remote blocking status change

Note 1 to entry: It is not mandatory to store these events, but if they are stored the requirements in Clause 5.1.6.2 are relevant.

3.41
relevant audit information
recorded event, which is directly connected to the HSL and which is neither an opening event nor an opening related event

EXAMPLES Activation of penalty time, adding new user, deleting user, tamper switch activation, time delay change, time change, incorrect code entered, connection to a programming or auditing device related to the HSL, low battery indication, change of user profiles, change of lock profiles, security and communication error messages, lock reset

Note 1 to entry: It is not mandatory to store these events, but if they are stored the requirements in Clause 5.1.6.2 are relevant.

3.42
non relevant audit information
recorded event, which is not directly connected to the HSL

EXAMPLES Temperature, humidity, pressure, vibration, door opened, door closed, boltwork opened, boltwork closed, connected to alarm systems (excluding duress alarm code as opening code), regular battery status

Note 1 to entry: It is not mandatory to store these events, but if they are stored the requirements in Clause 5.1.6.2 are relevant.

4 Classification

HSL are classified to an HSL class (A, B, C or D) according to Table 1, Table 2 and Table 3 by their security requirements. General requirements (see 5.1 and 5.2, 5.3) security and reliability requirements shall be met.

NOTE HSL class A has the lowest requirements and HSL class D has the highest requirements.

5 Requirements

5.1 General requirements

5.1.1 General

All requirements shall be tested according to 8.1.2.