



BSI Standards Publication

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

National foreword

This British Standard is the UK implementation of EN 1300:2023. It supersedes BS EN 1300:2018, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee GW/2, Secure storage of cash, valuables and data media.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 16973 7

ICS 13.310

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2023.

Amendments/corrigenda issued since publication

Date	Text affected

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 European Standard was approved by CEN on 16 July 2023.

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, Türkiye 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.....	4
1 Scope	6
2 Normative references	6
3 Terms and definitions.....	7
4 Classification	13
5 Requirements	13
5.1 General requirements	13
5.1.1 General	13
5.1.2 Requirements for all classes	13
5.1.3 Class D HSL	13
5.1.4 Mechanical key operated HSL	14
5.1.5 Lift heights for mechanical key locks	14
5.1.6 Electronic HSL	14
5.1.7 Electronic tokens	16
5.1.8 Firmware updates	17
5.2 Security requirements	17
5.2.1 Usable codes	17
5.2.2 HSL having over ride feature	17
5.2.3 Manipulation resistance	17
5.2.4 Destructive burglary resistance	18
5.2.5 Spying resistance	18
5.2.6 Electrical and electromagnetic resistance	18
5.2.7 Physical environmental resistance	19
5.2.8 Temperature resistance	19
5.3 Reliability requirements	21
6 Technical documentation	22
7 Test specimens	22
8 Test methods	23
8.1 General	23
8.1.1 General	23
8.1.2 Evaluation by inspection	23
8.1.3 Test procedure	23
8.2 Security tests	25
8.2.1 Usable codes	25
8.2.2 Manipulation resistance	25
8.2.3 Destructive burglary resistance	28
8.2.4 Spying resistance	28
8.2.5 Electrical and electromagnetic resistance	29
8.2.6 Physical environmental resistance	30
8.2.7 Temperature resistance	32
8.3 Reliability testing	32
8.3.1 Cycling	32
8.3.2 Code changes	33
8.3.3 Dynamic code input of mechanical combination HSL	33

9	Test report	34
10	Marking.....	34
	Annex A (normative) Parameters for installation and operation instructions	35
	Annex B (normative) Determination of manipulation resistance due to the design requirement	37
B.4.2	Sniffing the code via the data cable connection	44
B.4.3	Sniffing the code via key logger.....	45
B.4.4	Replay attack via the cable connection	46
B.4.5	Brute force attack.....	47
B.4.6	Side channel attacks.....	48
B.4.7	Lock spiking.....	49
B.4.8	Mechanical bypassing.....	49
B.4.9	Optical code spying.....	49
	Annex C (informative) Example of manufacturer's declaration.....	50
	Annex D (informative) Typical locking device dimensions	52
	Annex E (normative) Determination of burglary resistance due to the design requirement	53
	Annex F (informative) Example of firmware declaration.....	54
	Annex G (informative) A-deviations.....	55

European foreword

This document (EN 1300:2023) 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 March 2024 and conflicting national standards shall be withdrawn at the latest by March 2024.

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.

This document supersedes EN 1300:2018.

EN 1300:2023 includes the following significant technical changes with respect to EN 1300:2018:

General changes:

- editorial changes in the Scope;
- 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, character). Other definitions have been updated (one time code, locked door, secured HSL condition, fail secure, penalty time, authentication, firmware);
- requirements have been added for the used clocks (see 8.2.2.2.1 and 8.2.3.2.1);
- requirements have been added that the test report shall include any deviations from the procedure and unusual features observed (see Clause 9);
- Annex C and Annex F have been changed from normative to informative;
- editorial changes for clarification in 5.1.4.5, 5.1.5.1, 5.1.5.3, 5.2.1, 5.2.6.5, 5.2.3.1, 5.2.7, 8.1.3, 8.2.1.4, 8.2.2.1, 8.2.2.3, 8.2.2.5, 8.2.4.3.2, 8.2.6.2.5, 8.2.6.3.1, 8.2.6.3.2, 8.2.6.3.3, 10, A.2b), B.2.2, B.2.4, Annex G, Figure 1, Table 1 and Table 2.

Technical changes for any type of lock:

- requirement for indication of blocking status (5.1.2.5 and Annex A) has been updated;
- test requirement has been changed 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, 8.3.1.4, 8.3.2.1, 8.3.2.3 and 8.3.3.1);
- number of test specimens has changed from four to seven (see 7.1);
- the manipulation tool “personal computer” has now been classified with 0 basic units (with standard software) and with 25 basic units (with lock specific manipulation software), see Table 4.

Changes for mechanical combination locks:

- a dynamic code entry requirement was added (see 5.3.4) that corresponds to the already existing test requirement in 8.3.3.

Technical changes for electronic locks:

- removal of requirements regarding distributed systems into the European Standard EN 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 EN 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;
- updating of power supply tests: raising current from 220 V to an effective value of 230 V (AC) and changing it to 60 V (DC), re-structuring of the clauses for better reading, changing checking time from 12 h to 24 h, adding test requirements for electronic HSL with separate processing unit not included in the locking device used in secure cabinets (see 5.1.6.8, 5.2.6.1, 5.2.6.2, 8.2.5.3, 8.2.5.4 and Annex E);
- updates in 5.1.6.6 and 5.1.6.7.

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*

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 organizations 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, Türkiye and the United Kingdom.

1 Scope

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

It is applicable to mechanical and electronic HSL. For electronic locks used in a distributed system, see EN 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) resistance to attacks with acids;
- e) resistance to X-rays;
- f) resistance to explosives;
- g) 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*

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

EN 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 (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 IEC 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 22479, *Corrosion of metals and alloys - Sulfur dioxide test in a humid atmosphere (fixed gas method) (ISO 22479)*

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 terminology 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 an 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 characters

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

temporary code that expires after a single use

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 specifies 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 an 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: An 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 it is blocked by the HSL

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

period of time during which the HSL cannot be operated to prevent the limit of incorrect code entries being exceeded

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 specified 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 unauthorized person will have access to security-relevant information

3.39

opening event

entry of a recognized code with the aim to change the HSL to unsecured HSL condition

Note 1 to entry: The entry of a recognized 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 locking element after entering opening code, opening the blocking feature, changing HSL to secured condition

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

3.43

character

letter, digit, or other symbol having at least ten distinguishable variants used to represent parts of a mnemonic code

EXAMPLES One of the characters 0 to 9 in a decimal numeration system.

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.

5.1.2 Requirements for all classes

5.1.2.1 HSL shall only be opened by valid opening codes. The opening code(s) shall be retained as the only valid opening code(s) until deliberately reset. Overlaying or undocumented code(s) are not permitted.

5.1.2.2 Where mnemonic codes are used with an HSL these shall be able to be changed.

5.1.2.3 Any supplementary device (e.g. micro switch) which is fitted by the HSL manufacturer shall not be capable of being used to obtain information about the code.

5.1.2.4 An input unit is a necessary part of a mnemonic and electronic HSL although one input unit may operate more than one processing unit.

All HSL shall have a processing unit to validate the correct code. Each HSL shall also incorporate a blocking feature or be capable of causing movement of a blocking feature. If this feature shall be activated before first use a note to this effect is to be included in the instructions for the use of the lock

5.1.2.5 If the blocking feature is not moved manually there shall be a means of indicating whether the HSL is in secured HSL condition. If the HSL does not fulfil the requirement by itself automatically and the secure and locked condition can solely be checked by trying to turn the handle of the boltwork of the secure storage unit, then specific requirements shall be included in the installation instructions as well as in the operating instructions (according to Annex A).

5.1.2.6 An opening code shall not be capable of being altered or being changed other than by a recognized code.

5.1.3 Class D HSL

5.1.3.1 Means shall be provided by which the locking status, locked or unlocked, is made obvious.

5.1.3.2 A mechanical combination HSL shall be in a scrambled condition after locking.

5.1.3.3 A class D HSL shall contain a device which indicates the scrambled condition.

5.1.4 Mechanical key operated HSL

5.1.4.1 For all mechanical key operated HSL (see Clause 4), the same codes for the key sets shall not be repeated until 100 % of the usable codes have been used. If a manufacturer has more than one manufacturing plant the requirement is to be applied per plant. No synchronization between the plants is needed. However multiple manufacturing plants shall not start at the same code at the same time.

5.1.4.2 Codes (and sets of code tokens) shall be chosen at random.

5.1.4.3 There shall be no number or marking on either token or HSL which identifies the code. Also, no legitimization card shall be issued.

5.1.4.4 It shall not be possible to remove the key from an HSL whilst that HSL is in the open position except for code changing. This requirement is applicable to all classes. Note that it is acceptable for this feature to be activated immediately prior to the first use of the HSL.

5.1.4.5 The key shall not break under the applied maximum torque of $(2,5 \pm 0,1)$ Nm and the tested key shall still be usable to open the HSL. The test shall be conducted according to 8.2.1.4.

5.1.4.6 In addition to the foregoing requirements the manufacturer is also to complete the declaration set out in Annex C.

5.1.5 Lift heights for mechanical key locks

5.1.5.1 The maximum allowed number of coding elements (levers) of the same lift height shall be calculated by taking 40 % of the coding elements. Round the result according to the example below.

EXAMPLE If the result would be 0,405 the rounded result is 41 %. If the result would be 0,404 the rounded result is 40 %.

5.1.5.2 Usable codes shall not have more than two neighbouring elements, e.g. two levers next to each other, with the same lift height.

5.1.5.3 In usable codes, the difference between the highest and lowest lift height shall be equal or more than 60 % of the maximum lift height difference of the HSL. Calculation shall be rounded according to the example in 5.1.5.1.

5.1.6 Electronic HSL

5.1.6.1 Electronic HSL shall not require the use of electric power to stay in secured condition.

5.1.6.2 Electronic HSL as of class B and with more than 2 opening codes and all HSL of class C and D shall fulfil the following:

The HSL shall retain the records of the opening events and shall have the means to retain the record for at least 1 year, even in the event of a power failure.

The record shall not contain any security relevant information.

The minimum number of stored events shall fulfil one of the following:

- a) have a minimum size of 2 000 entries; or
- b) store opening events (see 3.39) and audit entries relating to firmware updates in such a way that the minimum requirements of Table 1 are always fulfilled; or
- c) shall have a minimum size according to the following formula. If non-relevant audit entries are used, these shall be stored in a separate memory:

$$R_{min} = T + (T \times \sum OR) + (5 \times T \times RE) + F$$

where

R_{min}	is the minimum total number of retained events;
T	is the minimum number of retained records of opening events (see column 2 of Table 1).
OR	is the number of different opening related events (see 3.40). The opening event itself is not counted as OR;
RE	is either 0 in case no other relevant audit information is recorded or 1 in case other relevant audit information is recorded;
F	is the minimum number of recorded firmware update events including version and date of the relevant HSL class according to Table 1 (not relevant, if the HSL does not have a firmware update function).

EXAMPLE 1 A HSL of class B only records opening events without any opening related events or other events. The minimum number of retained audit events is then $10 + (10 \times 0) + (5 \times 10 \times 0) + 0 = 10$.

EXAMPLE 2 A HSL of class C records the following event types: “user entering code to initiate opening of the HSL” (see 3.39), “HSL unlocked” (connected to opening event, see 3.40), “HSL locked” (connected to opening event, see 3.40), user code changed (connected to HSL, see 3.41), tamper switch activated (connected to HSL, see 3.41 and 5.1.6.4), penalty time activated (see 3.41 and 5.2.3.1) as well as “firmware update performed” (see Table 1). The minimum number of retained events is then $(50 + (50 \times 2) + (5 \times 50 \times 1) + 3 = 403$.

5.1.6.3 For non-distributed systems all component parts of the input unit shall be fixed to the secure storage unit. With the input unit being fixed to the secure storage unit the cabling from input unit to processing unit shall be non-accessible.

5.1.6.4 In class C and D any manipulation or replacement of the input unit shall generate an audit entry and automatically display information to the user at each use until it's neutralized by an authorized person.

5.1.6.5 If the Penalty Time is active there shall be a clear indication, in all classes of HSL, to the user.

5.1.6.6 For battery powered locks, where it is not possible to connect a power source from outside of the secure storage unit or a mechanical override does not exist, the following requirements shall be met: They shall be able to operate for at least 3 000 complete lock openings. The battery capacity shall be monitored. In the case of a low battery/low batteries an audible or visual signal shall occur during or immediately after an opening process. After the first low battery signal at least ten (10) complete opening and locking processes shall still be possible.

5.1.6.7 The processing unit evaluating and memorizing the code which is relevant for the opening of the HSL shall be located inside the secure storage unit.

5.1.6.8 All electronic HSL shall stay in secured condition when attacked with power supply according to 8.2.5.3 b) and as of class B and higher electronic HSL shall additionally be attacked with power supply according to 8.2.2.

For all electronic HSL constructed according to E.2.1 additionally Annex E is applicable.

5.1.6.9 Any application software generating one-time codes shall use authorization methods (e.g. password or dongle) to access and operate it and shall use data protection to store any kind of data. The manufacturer shall state which authorization methods and data protection is used for his system to the testing laboratory (see Annex C).

The manufacturer shall give a statement in his manuals that any application software generating one-time codes shall only be installed and operated in a secured environment.

5.1.7 Electronic tokens

5.1.7.1 General

The manufacturer shall give a statement in his manuals that electronic tokens shall be secured like mechanical keys.

5.1.7.2 Contactless electronic tokens

5.1.7.2.1 General

The following requirements for contactless electronic tokens are only applicable for near field communication devices, where a typical operation range is less than 15 cm, e.g. NFC or Mifare.

If the typical distance between electronic token and input unit for data transmission is more than 15 cm or the electronic token is used for a class D HSL, the requirements of EN 17646 shall be met.

NOTE Optical systems are considered to be distributed systems. An example for a contactless electronic token is RFID card.

5.1.7.2.2 Mutual authentication

Mutual authentication according to ISO/IEC 9798-2 or ISO/IEC 9798-4 shall be used. The time variant parameter such as time stamp, sequence numbers or random numbers to prevent valid authentication information from being accepted at a later time or more than once (see ISO/IEC 9798-1:2010, Annex B) shall have at least 32 bits. In addition to mutual authentication a valid opening code shall be used to open the HSL.

5.1.7.2.3 Cryptographic key

The cryptographic key for symmetric algorithms shall have a minimum length of 64 bits for class A and 128 bits for classes B, C and D and shall be intended only for the specific HSL model. Asymmetric algorithms shall have comparable key lengths with regard to the security level (NIST/SP 800-57). The cryptographic key for symmetric algorithms or the private key for asymmetric algorithms shall never be sent out of the token. It may be part of the transmitted communication data into the electronic token for initialising purposes. The initialization process shall be done by an authorized person in a secure environment. This shall be stated in the user instructions.

5.1.7.2.4 Identification number

Each electronic token shall have a unique identification number. The identification number shall have a length of at least 32 bits. Normally, the identification number is required for audit purposes only. If the serial number is also used as security relevant information, it shall not be visible on the token.

5.1.7.3 Contacted electronic tokens

Contacted electronic tokens for locks other than class D may not meet the same additional requirements as contactless electronic tokens of 5.1.7.2.1, 5.1.7.2.2 and 5.1.7.2.3. The manufacturer then shall give a statement in his manuals if any security relevant information is stored unencrypted.

Security relevant information should be stored secure in the token and there should be a secure authentication.

5.1.7.4 Multi-use

If the electronic token is designed to be used in applications other than the HSL system, the security relevant information shall not be accessible to the other applications.

If the electronic token is not protected against multi-use, the following statement shall be included in the manual: *Never use this electronic token in applications other than this HSL model.*

5.1.8 Firmware updates

If an HSL has a firmware update function the following shall be met:

Firmware updates shall be uploaded locally by a contacted connection (for instance by a wire) using at least an encryption of 64 bits for class A and B or 128 bits for class C and D to the processing unit and/or an input unit. Firmware updates shall be initiated by a recognized code. The number of firmware update attempts per hour shall follow Table 1 (column “Maximum No. of trials per hour for each type of coding means”). If the firmware updates change, add or delete opening codes, this shall be documented in the user instructions. Each firmware update shall be acknowledged at the HSL by an authorized person. It shall be possible to audit the firmware update according to Table 1.

The change log of the firmware, the procedure and the encryption shall be noted in a declaration (see Annex F).

All devices between input and processing unit shall not create and/or store any HSL related security relevant information. The manufacturer shall include this requirement into the operation instruction.

5.2 Security requirements

5.2.1 Usable codes

The minimum number of usable codes when tested in accordance with 8.2.1 for each class and type of HSL shall be as given in Table 1. The minimum number of 25 000 usable codes for mechanical key locks of class A shall be sufficient only if the required manipulation resistance as in Table 1 is ascertained by 8.2.2. As of 80 000 usable codes or more and by compliance with Annex B, class A HSL shall not be tested for resistance to manipulation.

HSL with parallel codes: the minimum number of usable codes shall be multiplied by the number of possible parallel codes.

HSL with variable opening code lengths: the smallest number of used characters which the HSL is able to accept for opening code input shall be used for the calculation of usable codes.

It shall not be possible to open mechanical key operated HSL with additional keys when tested in accordance with 8.2.1.3.

HSL having more than one mode of coding means (for instance mnemonic code and electronic token): at least one of the coding means shall fulfil the security requirements of this standard. If there is a secondary mode of coding means, which does not completely fulfil the security requirements of this standard, it shall only be used in addition to the mode which fulfils the requirements completely.

5.2.2 HSL having over ride feature

HSL with an override feature (e.g. an electronic HSL having a mechanical override) shall be classified by the least secure system used.

5.2.3 Manipulation resistance

5.2.3.1 Limit of trials

The maximum number of incorrect code entries in a row per hour which can be made shall be as shown in Table 1.

NOTE Mechanical token HSL are not included in Table 1 because the time taken for changing tokens sufficiently limits the rate of trials.