BS EN 1300:2013

BSI Standards Publication

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

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 1300:2013. It supersedes BS EN 1300:2004+A1:2011 which is withdrawn.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 secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 76366 3

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 November 2013.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 1300

November 2013

ICS 13.310

Supersedes EN 1300:2004+A1:2011

English Version

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

Unités de stockage en lieux sûrs - 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 14 May 2013.

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, 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.

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

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

Contents

Page

Foreword

This document (EN 1300:2013) 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 May 2014, and conflicting national standards shall be withdrawn at the latest by May 2014.

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

This document supersedes EN 1300:2004+A1:2011.

In comparison with EN 1300:2004+A1:2011, the following changes have been made:

— addition of definitions (Clause 3) and requirements (subclause 5.1.6) for contactless electronic tokens;

— addition of definitions (Clause 3) and requirements (subclause 5.1.7) for cryptography in distributed security systems;

— updating references to newer versions;

— changing of the requirements for the input unit (subclause 5.1.5.4);

— updating the test specimen of keys to a middle key cut design (subclause 7.3);

— clarification and optimization of the immersion test (subclause 8.2.6.3);

— correction of the heat resistance test (subclause 8.2.7.2);

— editorial clarifications among others in subclauses 5.1.5.1, 5.2.7, 5.3.3, 7.1, 8.2.2.1, 8.2.4.3.2, 8.2.6.2 and 8.3.3.3.2;

— addition of parameters for operating instructions in Annex A.

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

This European Standard has been prepared by Working Group 3 of CEN/TC 263 as one of a series of standards for secure storage of cash valuables 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*

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, 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 the United Kingdom.

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

EN 60068-2-1:2007, *Environmental testing — Part 2-1: Tests — Test A: Cold (IEC 60068-2-1:2007)*

EN 60068-2-2:2007, *Environmental testing — Part 2-2: Tests — Test B: Dry heat (IEC 60068-2-2:2007)*

EN 60068-2-6:2008, *Environmental testing — Part 2-6: Tests — Test Fc: Vibration (sinusoidal) (IEC 60068-2-6:2007)*

EN 60068-2-17:1994, *Environmental testing — Part 2: Tests — Test Q: Sealing (IEC 60068-2-17:1994)*

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 61000-4-4, *Electromagnetic compatibility (EMC) — Part 4-4: Testing and measurement techniques — Electrical fast transient/burst immunity test (IEC 61000-4-4)*

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

EN 61000-4-6, *Electromagnetic compatibility (EMC) — Part 4-6: Testing and measurement techniques — Immunity to conducted disturbances, induced by radio-frequency fields (IEC 61000-4-6)*

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

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
bolt stump or bolt stumps which form part of an HSL which enables or prevents movement of a blocking feature

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 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

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

3.12
reliability
ability to function and achieve the security requirements of this standard after a large number of duty cycles

3.13
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.

3.14
spying
attempt to obtain unauthorized information

3.15
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.

3.16
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

3.17
locking sequence
series of actions which start with an open door and are complete when the door is closed, bolted, locked and secure

3.18
open door
door is not in its frame

3.19
closed door
door is within its frame ready for throwing its bolt(s)

3.20
bolted door
bolts are thrown

3.21
locked door
boltwork cannot be withdrawn because of the HSL

3.22
secured door
door is closed, bolted and locked with an HSL in the secured HSL condition

3.23
secured HSL condition
blocking feature is thrown and can only be withdrawn after entering the opening code(s)

3.24
normal condition
after testing, the HSL specimen is in the secured HSL condition, and all design functions are operating

3.25
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

3.26
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)

3.27
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.

3.28
penalty time
time delay because of time exceeding the limit of trials

3.29
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

3.30
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)

3.30.1
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

3.30.2
symmetric cryptographic algorithm
cryptographic algorithm that uses a single secret key for both encryption and decryption

3.31
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.

3.32
cryptographic module
set of hardware and software that implements security functions for distributed systems and electronic tokens including cryptographic algorithms

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 5.1.5.3 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.

3.34
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 processing units

3.37
automatic key exchange
cryptographic protocol that allows two components that could have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel

3.38
availability
proportion of time a system is in functioning condition

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

All requirements shall be tested according to 8.1.2.

5.1.1 Requirements for all classes

5.1.1.1 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.

5.1.1.2 Where mnemonic codes are used with a HSL these shall be able to be changed.

5.1.1.3 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.

5.1.1.4 An input unit is a necessary part of a HSL although one input unit may operate more than one HSL (processing unit). Each HSL shall have a processing unit to validate the correct code from the input unit.

Each HSL shall also incorporate a blocking feature or be capable of causing movement of a blocking feature. If this feature has to be activated before first use a note to this effect is to be included in the instructions for the use of the lock.

5.1.1.5 If the blocking feature is not moved manually there shall be a means of indicating whether the HSL has been secured, locked and scrambled.

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

5.1.2 Class D HSL

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

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

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

5.1.3 Mechanical Key Operated HSL

5.1.3.1 For class A HSL (see Clause 4), the same code shall not be repeated until at least 80 % of the usable codes have been used.

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

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

5.1.3.4 It shall not be possible to remove the key from a 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.

5.1.3.5 The key shall not break under the applied maximum torque of 2,5 Nm. The test is to be conducted according to 8.2.1.4.

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

5.1.4 Lift heights for mechanical key locks

5.1.4.1 Usable codes shall not have more than 40 % of the coding elements (levers) of the same lift height.

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

5.1.4.3 In usable codes, the difference between the highest and lowest lift height shall be more than 60 % of the maximum lift height difference of the HSL.

5.1.5 Electronic HSL

5.1.5.1 Electronic HSL as of class B and with more than 2 user codes shall retain the records of the opening events used according to Table 1 and shall have the means to retain the record for at least 1 year, even in the event of a power failure.

5.1.5.2 When the electronic HSL is secured further communication with the processing unit shall only be possible by inputting a recognized code and to display the lock status.

5.1.5.3 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 has to be non accessible.

5.1.5.4 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.

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

5.1.5.6 Low Battery Indication: battery powered locks 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. Where it is possible to connect power from the outside it will not be necessary to meet this requirement.

5.1.5.7 The processing unit for code evaluation shall be located inside the secure storage unit.

5.1.5.8 As of class B, electronic HSL have to be tested against influences by power supply according to 8.2.5.

5.1.6 Electronic tokens

5.1.6.1 General

The manufacturer has to give a statement in his manuals that electronic tokens have to be secured as mechanical keys.

5.1.6.2 Contactless electronic tokens

5.1.6.2.1 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 distributed systems as in 5.1.7 shall be met.

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

5.1.6.2.2 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 has to be used to open the HSL.

5.1.6.2.3 Cryptographic key

The cryptographic key for symmetric algorithms shall have a minimum length of 64 bits for classes A and B and 128 bits for classes 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 has to be done by an authorized person in a secure environment. This has to be stated in the user instructions.

5.1.6.2.4 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.

5.1.6.3 Contacted electronic tokens

Contacted electronic tokens for locks other than class D do not have to meet the same additional requirements as contactless electronic tokens. The manufacturer then has to 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.

5.1.6.4 Multi-use (only valid for class B, C and D)

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.*

5.1.7 Requirements for cryptography in distributed security systems

5.1.7.1 Information security

5.1.7.1.1 General

This subclause focuses on confidentiality, authentication, integrity, availability, data transmission, information storage, cryptographic keys and their management.

5.1.7.1.2 Confidentiality

Security relevant information that is transmitted across a distributed system shall be encrypted to prevent unauthorized reading. For security relevant data transmission processes in distributed systems, symmetric algorithms such as TDEA 64 bit block and AES 128 bit block are the minimum requirements according to NIST SP 800-67 and FIPS 197 respectively. The encryption algorithm shall be used in a secure mode of operation such as CBC, CFB or GCM.

5.1.7.1.3 Authentication

Authentication is required to start communication between devices of a distributed system. The authentication method has to be described by the manufacturer.

5.1.7.1.4 Integrity

It shall be ensured that data has not been altered in an unauthorized manner since it was created, transmitted or stored. This includes the insertion, deletion and substitution of data. Accepted methods for ensuring integrity are MAC algorithms or digital signatures.

5.1.7.1.5 Availability

If a distributed system is temporary not available this condition shall not compromise the level of security.

5.1.7.1.6 Security relevant information storage

For storage of security relevant information in HSL class A, lower or no cryptographic concepts than mentioned in 5.1.7.1.2 may be chosen.

5.1.7.1.7 Cryptographic key management

Cryptographic keys shall be protected against unauthorized access. The method of storing, creating, transmitting and accessing the cryptographic keys has to be described by the manufacturer. These requirements also apply to the manufacturer's initialization process.

5.1.7.1.8 Cryptographic keys for data transmission

Distributed systems shall be equipped with cryptographic keys generated at random except for preset factory cryptographic key(s) for classes B, C and D. FIPS Pub 140-2 4.7.1 (random number generators) security requirements shall be considered for the generation of random numbers.

The cryptographic keys have to be field changeable from HSL class B on. They may be field changeable in HSL class A as well. If a new key is confirmed, the new key shall be the only usable one.

5.1.7.1.9 Cryptographic key modification

5.1.7.1.9.1 General

The preset factory cryptographic key(s) shall be modified before putting the distributed system into operation. If cryptographic keys are not field changeable (HSL class A only), measures shall be implemented to prevent those persons intimately involved in the production of locks to identify the customer location to which they are dispatched. This has to be ensured by means of a manufacturer's declaration. Non-changeable keys shall only be applicable for systems with class A locks.

5.1.7.1.9.2 Key exchange

Key exchanges shall use asymmetric methods (based on algorithms such as RSA, ECC) or symmetric methods (such as Kerberos 5). The mechanisms for key exchange shall provide at least the equivalent security strength as the methods of data transmission. To get an overview of appropriate key sizes and the equivalence between symmetric and asymmetric key lengths, refer to NIST SP 800-57. When the key exchange is triggered automatically or manually the frequency of the key exchange has to follow NIST SP 800-57.

5.1.7.1.9.3 Key change

The manufacturer has to provide a user instruction explaining the procedure and frequency for key changes. Changes shall be done only after input of an authorization code. If the key change is done out of band (outside of previously established communications method), subclause 5.1.7.1.7 has to be followed.

5.1.7.2 Security of distributed input unit

5.1.7.2.1 General

This requirement shall be met only if security related data are transmitted.

5.1.7.2.2 Physical security

In a distributed system any input unit has to follow 5.1.5.4, including class A locks.

5.1.7.2.3 Information security

Security relevant information has to be entered in trusted and dedicated input units only, following 5.1.7.1. Unauthorized attempts to access those input units shall block the input unit from normal use, e.g. will activate mechanisms that erase or render useless plaintext cryptographic keys (i.e. tamper response). Level 3 physical security requirements according to FIPS Pub 140-2, 4.5.1 shall be met at minimum.

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 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 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 figures 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.

5.2.2 HSL having over ride feature

HSL with an over ride 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 trials 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.

5.2.3.2 Manipulation

The minimum resistance values, M, given in Table 1 shall be exceeded by at least two of the three test specimens in the tests for manipulation resistance made according to 8.2.2.

5.2.4 Destructive burglary resistance

The minimum resistance values given in Table 1 shall be exceeded in tests in which an external force is applied according to 8.2.3.

5.2.5 Spying resistance

5.2.5.1 Any information entered into an electronic HSL shall be unrecognizable 30 s after entry, even if only part of the opening code has been entered.

5.2.5.2 For HSL classes C and D the included angle over which code information can optically be observed shall be not more than 30° about the centre-line as defined in 8.2.4.

5.2.5.3 Direct code input via the keypad using the fixed position of figures is not permitted for class C and D HSL. This does not apply if a one time code is used.

5.2.5.4 Compromising emanation of signals:

It shall not be possible to correlate unencrypted security relevant information with emitted signals from any component part of a distributed system. In connection with compromising radiation, special attention shall be paid to the transmission system because of coupling of radiation and/or wireless transmissions.

5.2.6 Electrical and electromagnetic resistance

5.2.6.1 Mains powered electronic HSL shall remain in the normal condition during mains supply voltage variations, voltage dips and short interruptions; tested according to 8.2.5.5.

During any power loss when an electronic HSL is in its secured HSL condition it shall remain secured (see 8.2.5.3).

Mains powered HSL shall be capable of being secured during a failure of mains supply lasting up to 12 h (see 8.2.5.4).

5.2.6.2 After testing in accordance with 8.2.5.5 electronic HSL tested for electrostatic discharge resistance shall meet the requirements of Table 2. During this testing specimens shall not change from the secured HSL condition for longer than 5 ms.

5.2.6.3 During the testing of electronic HSL for resistance to radiated electromagnetic fields in accordance with 8.2.5.8, the requirements of Table 2 shall be met.

5.2.6.4 After testing of a mains powered electronic HSL (and any attached cable of more than 10 m in length connected to external equipment) for resistance to fast transient burst in accordance with 8.2.5.6 the requirements of Table 2 shall be met. During this testing specimens shall not change from the secured HSL condition for longer than 5 ms.

5.2.6.5 After testing electronic HSL for surge immunity according to 8.2.5.7 the requirements of Table 2 shall be met. During this testing specimens shall not change from the secured HSL condition for longer than 5 ms.

5.2.7 Physical environmental resistance

All HSLs shall be tested according to 8.2.6.1 and 8.2.6.2 for resistance to vibration and shock, according to 8.2.6.4 for resistance to corrosion, and all electronic locks shall be tested for immersion according to 8.2.6.3.

5.2.8 Temperature resistance

5.2.8.1 Cold

The electronic HSL shall be in its normal condition after the test in accordance with 8.2.7.1 for 16 h at –10 °C.

5.2.8.2 Heat

The electronic HSL shall be in its normal condition after the test in accordance with 8.2.7.2 for 16 h at +55 °C.

Table 1 — Security Requirements for all HSL

Class and type	Minimum No of retained records of opening events	Minimum No of usable codes for each type of coding		Maximum No of trials per hour for each type of coding means		Manipulation resistance M	Destructive burglary resistance D
		Material Coding	Mnemonic Coding [b]	Any	Mnemonic	Minimum Resistance units RU	Minimum Resistance units RU
A							
Electronic	None	25 000	80 000	300		30	80
Mechanical	Not applicable	25 000	80 000	Not applicable		30	80
B							
Electronic	10 (as of 3 users)	100 000	100 000	100		60	135
Mechanical	Not applicable	100 000	100 000	Not applicable		60	135
C							
Electronic	50	1 000 000	1 000 000	30		100	250
Mechanical	Not applicable	1 000 000	1 000 000	Not applicable		100	250
D							
Electronic	500	3 000 000	3 000 000		10	620	500
Mechanical	Not applicable	3 000 000	3 000 000		10 [a]	620	500

[a] Excluding key operated locks.

[b] The minimum number of figures required, for electronic locks only, is six (6).

Table 2 — Minimum requirements for electrical and electromagnetic resistance at the test conditions shown

Resistance against radiated radio-frequency electromagnetic fields (Test method EN 61000-4-3)			
Test conditions	HSL class	Lock conditions [a]	
	A to B	O [b]	FS [b]
	C to D	n.a.	O [b]
	Test level	3 [c]	4 [c]

Resistance against conducted disturbances, induced by radio-frequency fields (Test method EN 61000-4-6)		
Test conditions	HSL class	Lock conditions [a]
	A to B	FS [b]
	C to D	O [b]
	Test level	3

Resistance to electrostatic discharge, fast transient bursts and high energy voltage surge			
	HSL class	Lock conditions [a]	
	A to D	O	FS
Test level	EN 61000-4-2	4	
	EN 61000-4-4		4
	EN 61000-4-5		4

[a] N = Normal operation O = Operable FS = Fail secure
[b] Denotes the condition in which the HSL should be after the test in the worst case.
[c] Frequency range 80 MHz to 2 GHz.

Table 3 — Physical environmental conditions

Vibration resistance (Test method EN 60068-2-6, endurance by sweeping)			
HSL class	Acceleration g	Frequency range Hz	Cycles
A to B	1	10 to 150	10
C to D	2	10 to 150	10

5.3 Reliability requirements

5.3.1 After being subjected to 10 000 cycles according to 8.3.1, the HSL shall be in its normal condition.

5.3.2 Code input by rotating a dial shall not deviate from the setting by more than 1 % of the total setting range after testing for dynamic code input to 8.3.3.

5.3.3 Code changeable mechanical HSL shall be in the normal condition after 100 code changes have been made, according to 8.3.2.

6 Technical documentation

The following technical documentation shall accompany the test specimen:

6.1 Detailed construction drawings, with dimensions and tolerances.

6.2 The calculation of usable codes and all relevant parameters for that calculation.

6.3 Characteristics of detaining features including:

— dimension of the bolt head or other blocking component;

— blocking feature movement during locking of the bolt head or blocking element.

6.4 All dimensional values necessary for linking or connecting the HSL to external devices (e.g. code input device, means by which blocking feature is moved) including:

— size of code entry hole (e.g. keyhole);

— sizes of spindles, dials and dial rings;

— size(s) of cable connections.

6.5 Detailed description of the means for setting and changing codes and any precautions to be observed.

6.6 Parameters for installation.

6.7 Operating instructions**.**

6.8 Software and hardware documentation for electronic HSL including:

— software structure;

— circuit diagram;

— program code listing.

6.9 Description of the software method used to:

— store codes;

— read out codes;

— protect the access to stored data and program;

— avoid memory damage;

— manipulation blocking.

6.10 Statement of the high security lock (HSL) class the HSL is expected to meet.

7 Test specimens

7.1 A minimum of four test specimens shall be provided. If manipulation resistance testing is to be carried out three additional specimens shall be provided. These three specimens shall have their opening codes selected at random and these codes shall not be or become known to the test teams prior to the test.

The applicant shall supply test specimens for manipulation testing mounted on a steel plate with cover according to 8.1.3.

NOTE Specimens for manipulation resistance testing can have specific dimensional values within the limits of the technical documentation, selected by the test house.

7.2 Each test specimen shall include all security relevant parts of the HSL, specifically:

— the input unit;

— the processing unit;

— the locking device;

— the blocking feature;

— any override device;

— any other part upon which the security of the specimen depends.

7.3 When the test specimens are mechanical key locks one specimen shall have two additional keys - as well as the correct key. One additional key shall have in a middle key cut one step which is one step increment height **higher** than the same step of the correct key; the other additional key shall have the same step one step increment height **lower** than that of the correct key.

8 Test methods

8.1 General

8.1.1 General

Test specimens are tested for their security and reliability. In security tests the objective is to unlock the test specimen or cause it to fail insecure; in reliability tests the objective is to establish whether the test specimen continues to function without loss of security after exposure to the tests.

Specimens of mechanical HSL for the manipulation resistance test (see 8.2.2) may be subject to up to 1 000 cycling operations (see 8.3.1.) before the manipulation test. These specimens shall not be subject to any other test prior to the manipulation test.

Testing against cryptographic requirements is based on examination of manufacturer's description of the system which has to contain a list of the referenced standards.

8.1.2 Evaluation by inspection

All requirements according to 5.1 have to be evaluated by inspection.

8.1.3 Test procedure

Simulate the use in a Secure Storage Unit by mounting the test specimens, according to the manufacturer's instructions, on a steel mounting plate and cover, both of which are free of holes other than those required for mounting in accordance with the technical documentation (see Clause 6) and Figure 1, for the following tests: manipulation resistance (see 8.2.2), destructive burglary resistance (see 8.2.3), spying resistance (see 8.2.4), electrical and electromagnetic resistance (see 8.2.5).

Where the dynamic code input is carried out by cycling equipment it shall not be necessary to use a simulated (dummy) Secure Storage Unit.

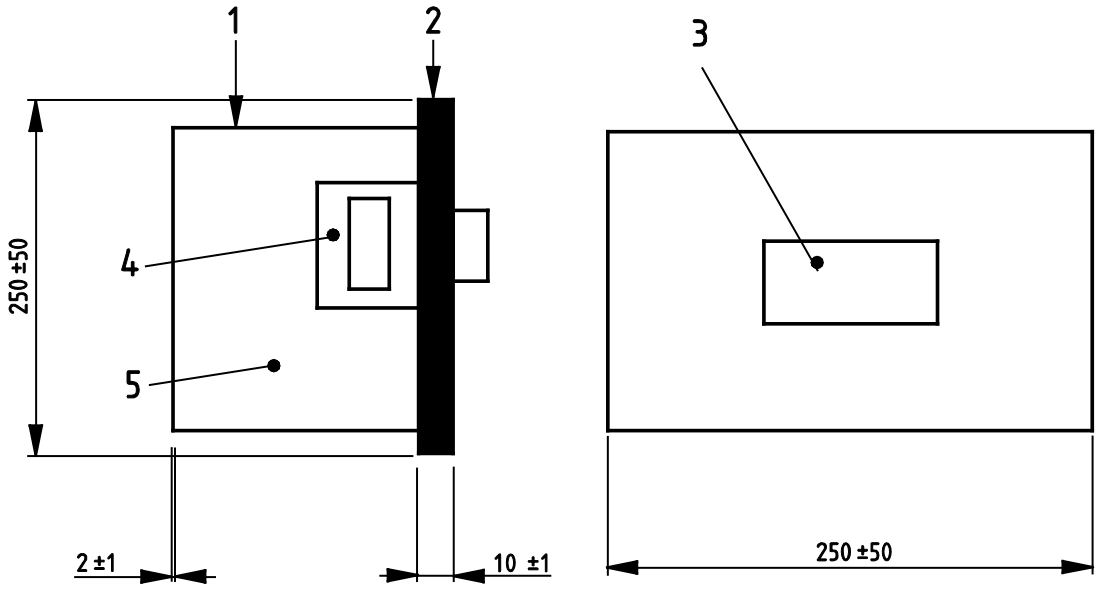
Allow access to the specimen in accordance with the technical documentation in Clause 6. When the test specimen is an electronic HSL the cover shall be made of steel and joined to the steel mounting plate by screws spaced at less than 50 mm around all four sides of the steel plate.

Carry out the manipulation resistance test (see 8.2.2), destructive burglary resistance test (see 8.2.3) and spying resistance test (see 8.2.4) against only those parts of the test specimen accessible when it is mounted on the steel plate and without forcibly penetrating the steel plate or the cover.

The burglary test shall exclude any attack against the lock case or its cap (cover), from inside the lock, which causes any part of the case or cap to be damaged, and/or partly removed or completely removed.

When the secured condition of the test specimen has to be monitored it shall be carried out to an accuracy of 5 ms.

Dimensions in millimetres



Key

1 steel cover
2 steel mounting plate
3 input device
4 lock
5 cover

NOTE Steel cover to a minimum of 20 mm distance from the lock.

Figure 1 — Schematic design of cover and mounting

8.2 Security tests

8.2.1 Usable codes

8.2.1.1 Assess the manufacturer's declaration of the numbers of usable codes (see 6.3) to ensure it is correct.

8.2.1.2 Use the procedure in the following example and the cyclic test device to calculate the number of usable codes of mechanical combination HSL:

a) the code wheels, less the last one to be set, are aligned to their opening numbers;

b) the last code wheel is then set to the test number; starting with its opening number minus 5 digits;

c) determine whether the lock opens. If the lock opens the minimum number, N min and the maximum number N max are recorded;

d) increase the test number by 0,25 digits;

e) repeat steps a) to d) until the test number is the opening number plus 5 digits.

The dialling tolerance T = N max – N min.

The number of usable codes is:

on a 3-wheel lock: Cn = (D1/T) x (D2/T) x (D3/T)

i.e. (100/1,75) x (100/1,75) x (80/1,75) = 149 271

on a 4-wheel lock: Cn = (D1/T) x (D2/T) x (D3/T) x (D4/T)

i.e. (100/1,75) x (100/1,75) x (100/1,75) x (80/1,75)

= 8 529 779

Dx = number of digits on wheel x minus the forbidden zone as declared by the manufacturer (usually on the last code wheel to be set).

8.2.1.3 For mechanical key locks, the keys having one step with one step height increment difference (see 7.3) shall be used with a maximum torque of 1,5 Nm to determine whether either will unlock the specimen.

8.2.1.4 For testing the key strength, the lock shall be mounted in a stand according to Figure 1. Then the correct key shall be fully inserted in the lock and consistently be increased to a torque of (2,5 $\pm$ 0,1) Nm for a period of $5\,^{+1}_{0}$ s. After this, the key shall be capable to be removed from the lock and reused to operate the same lock with a torque not exceeding 1,5 Nm.

8.2.2 Manipulation resistance

8.2.2.1 Principle:

Test specimens and technical documentation (see Clause 6) are examined and the method of assessing manipulation resistance is decided in accordance with the following:

Mechanical HSL in class A as of 80 000 usable codes which meet the design requirements of Annex B shall not be tested for resistance to manipulation.

Mechanical HSL in class B which meet the design requirements of Annex B shall not be tested unless the test house is unsure that the manipulation resistance requirements (see Table 1) have been met.

Electronic HSLs in all classes and all mechanical HSLs in classes C and D shall be tested for resistance to manipulation.

Mechanical HSLs in classes A and B which do not meet the design requirements of Annex B, or for which it cannot be shown that these design requirements are met, may be tested for resistance to manipulation at the applicant's request. In determining whether the requirements for resistance to manipulation are satisfied, the test result shall take precedent over the tolerance assessment.

8.2.2.2 Equipment:

8.2.2.2.1 Clock which measures hours, minutes and seconds.

8.2.2.2.2 Tools according to the criteria in Table 4.

8.2.2.3 Procedure:

Examine a sufficient number of test specimens (see Clause 7) together with the technical documentation (see 6.2) and Annex B and devise a test program of manipulation using tools (see Table 4) which shall be most likely, in the opinion of the testing team, to result in the lowest manipulation resistance values. Conduct a preliminary examination of unsealed specimens (see Clause 7) and trials and take any measurements necessary to determine which methods are to be used to attempt to open the HSL by manipulation.

8.2.2.4 **Manipulate** each of the three sealed test specimens once using the manipulation test procedure as determined in 8.2.2.3. Measure the time of manipulation with a test being terminated when the resistance to manipulation value M for the Class (see Table 1) has been exceeded.

8.2.2.5 **Expression of results:**

Calculate the resistance to manipulation value, M, from the following formula:

$$M = t + B$$

where

t is the time taken in minutes to unlock the test specimen;

B is the basic unit value and is one of two values (0, 15 Table 4) which is appropriate to the highest category of tool used;

M is the manipulation resistance value in resistance units (RU).

Table 4 — Tool list for manipulation resistance testing of mechanical and electronic HSL

Number	Category Name	Basic Units	Description	Examples Mechanical	Examples Electronic
1.	Commonly available tools, hand tools and instruments	0	Commonly available tools or equipment which can be purchased by any person from retail hardware stores. The tools are sufficiently small to be inconspicuously carried. No special skills are required for their effective use. They do not need mains electricity and their use does not cause such noise as would attract attention	Screwdriver	Voltmeter
				Pliers	AMP-meter
				Tongs	Soldering iron
				Tweezers	Wires
				Files	Phase-meter
				Punches	Personal computer
				Hammers	Batteries
				measuring items	Power supplies
				magnifying glasses	
2.	HSL opening tools	15	Any HSL opening tools and instruments which can be purchased from special tool supply companies and available only to bona fide locksmiths or are specially designed, manufactured or modified. For effective use the tools require special skills and a detailed knowledge of the HSL and HSL opening methods. It is possible that those tools will be specific and highly effective against only one type of HSL.	Picking tools	Spectrum analyser
				Lock spares	Oscilloscope
				Key blanks (uncut)	Sound amplification equipment
				Trial keys	Optic probes
				Sound amplification equipment	Detectors for electro-magnetic radiation
				Optic/fibre optic probes	Automated opening machines
				Dialling machines	

8.2.3 Destructive burglary resistance

8.2.3.1 Principle

Test specimens and technical documentation (see Clause 6) are examined and a method of assessing the destructive burglary resistance is devised and implemented.

8.2.3.2 Equipment

8.2.3.2.1 Clock which measures hours, minutes and seconds.

8.2.3.2.2 Tools from Category A of EN 1143-1.

8.2.3.2.3 Tools according to the criteria in Table 4.

8.2.3.3 Procedure

Examine the test specimen(s) together with technical documentation (see Clause 6) and conduct any trials and take any necessary measurements to decide the method and tools which will result in the lowest destructive burglary resistance value. Test one specimen and measure the time of the test. The test may be terminated when the destructive burglary resistance value for the class (see Table 1) has been exceeded.

8.2.3.4 Expression of results

Calculate the destructive burglary resistance value, D, from the following formula:

$$D = 5t + \sum BV + B$$

where

D is the destructive burglary resistance value in resistance units (RU);

t is the time taken in minutes to unlock the test specimens;

$\sum BV$ is the sum of the basic values for all of the tools used from category A of EN 1143-1;

B has a value of 0 or 15 according to the highest basic unit value of any tools used from Table 4.

8.2.4 Spying resistance

8.2.4.1 Principle

The test specimen is to be mounted in accordance with Figure 1 and held in a vertical position at a height convenient for observing any positions on the HSL and from where the code being input can be seen.

Tests are made to recognize the information being input.

Two screens are positioned against the test specimen to limit the spying angle.

Spying trials are made to determine if any information being input can be recognized outside the included angle.

8.2.4.2 Equipment

8.2.4.2.1 **Test rig** capable of holding the mounted test specimen in a vertical position.

8.2.4.2.2 **Clock** which measures hours, minutes and seconds.

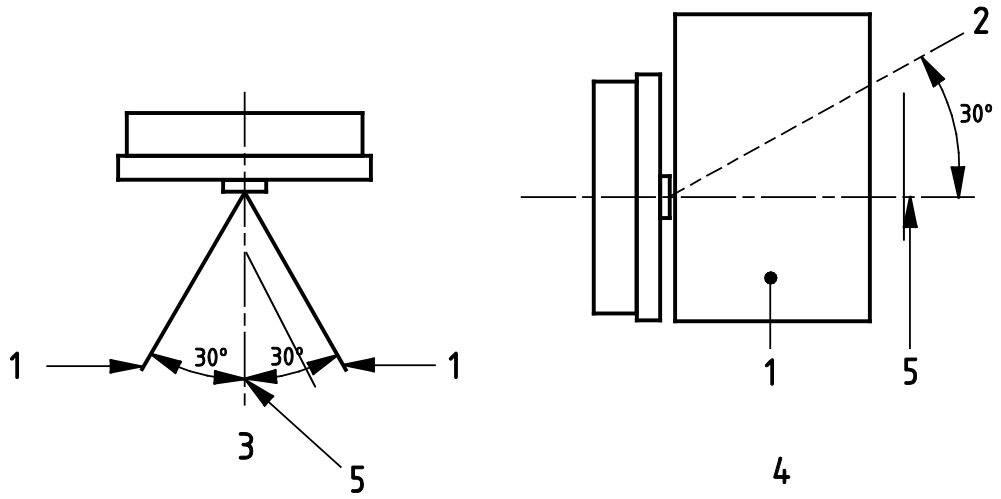
8.2.4.2.3 **Two screens** capable of defining a limited angle of spying.

For HSL classes C and D the spying test may need to be made in various lighting conditions.

8.2.4.3 Procedure

8.2.4.3.1 Take one electronic HSL and input an opening code. Observe whether information input is unrecognizable 30 s after the last digit entry. Carry out the test inputting the complete code and then only part of the code.

8.2.4.3.2 Position two screens (see 8.2.4.2.3) in front of the test specimen at a horizontal angle of 60° in accordance with Figure 2 and whilst the codes are entered assess whether any information can be recognized in a vertical angle of 30° up from the test specimen's centre line.



Key

1 screen
2 view angle
3 top view
4 side view
5 centre line

Figure 2 — Two schematic diagrams showing top and side views of spying equipment

8.2.5 Electrical and electromagnetic resistance

8.2.5.1 Principle

Electronic HSL test specimens in their normal condition before each test are tested for electrical and electromagnetic resistance in accordance with Table 2. A power loss as well as of class B on a power supply influence test according to 8.2.5.3 is also to be included.

8.2.5.2 Procedure

Test samples in accordance with the requirement of 5.2.6 and assess the HSL after each test to determine if it is in its normal, operating or fail secure condition, as appropriate to the requirements.

8.2.5.3 Power loss and power supply influence test

Place the test specimen in the secured condition and remove power. Assess whether it remains in the secured condition.

After that, test possible unintentional unlocking at power supply with DC or AC by consistent increase from 0 to 220 V, the lock being connected to external accessible cables.

8.2.5.4 Securing during power failure

Place a mains powered HSL test specimen in the unsecured condition. Remove the power. Assess whether the HSL can be secured 12 h after the power has been removed.

8.2.5.5 Electrostatic discharge

Carry out electrostatic discharge tests in accordance with EN 61000-4-2 using the test levels of Table 2 against parts of the HSL test specimen which are touched by the user during any operation, for example code entry, unlocking, locking, code change. The polarity of the mounting plate is + or - therefore both polarities shall be tested. The cover (see 8.1.3) may be removed for this test.

For HSL which are to be fitted to safes without a metal housing additional tests may be conducted on a test specimen with no mounting, or to a test specimen on a non-conductive mounting, but they are not part of the classification scheme.

8.2.5.6 Fast transient bursts

Test mains powered locks in accordance with EN 61000-4-4 using the test levels of Table 2.

8.2.5.7 Surge immunity

Test in accordance with EN 61000-4-5 using the test levels of Table 2.

HSL test specimens may be first tested at the highest level. If these high levels are resisted testing shall not be carried out at the lower levels.

8.2.5.8 Radiated electromagnetic fields

Test in accordance with EN 61000-4-3 and EN 61000-4-6, using the test values of Table 2.

8.2.5.9 Expression of results

Assess whether there is any change in the secured condition of the specimen HSL during testing or after, or whether it remains in the secured condition during and after the test, according to Table 2.

8.2.6 Physical environmental resistance

8.2.6.1 Vibration

Test HSL specimens which are in operating condition, for vibration resistance, in each of the three axes x, y and z, according to EN 60068-2-6 using the test values in Table 3.

Mode of Test: (1) endurance by sweeping

(2) ten (10) cycles

After exposure of vibration, the test specimens have to be in operating and in secured condition.

8.2.6.2 Shock test

8.2.6.2.1 General

During the test there shall be a continuous monitoring (see 5.2.7) whether the secure condition of the test specimen changes for more than 5 ms. Also assess whether the test specimen is in an operating condition after exposure to the test with five drops of $50\,^{0}_{-5}\ g$.

8.2.6.2.2 Principle

HSL specimens are dropped from a height of 1m to induce impact shocks. Five drops are conducted in an axis chosen by the tester. After five drops with $50\,^{0}_{-5}\ g$ the condition of the specimen is to be assessed (see 5.2.7). Depending on the lock design, the test house can decide to conduct an additional test with up to maximum 50 shocks with more than 50 g using the same equipment.

8.2.6.2.3 Equipment

A test rig which allows the test specimen, when mounted on a rigid mounting plate in accordance with the method specified in the technical documentation (see Clause 6), to fall vertically through (1 000 ± 5) mm and be decelerated. Deceleration is measured on the mounting plate and only the mounting plate is to contact any part of the test rig.

8.2.6.2.4 Procedure

a) Operate the test specimen so that the blocking element is in the secured HSL position;

b) raise the test specimen so that it will fall through 1 000 mm ± 5 mm;

c) make five (5) impacts with $50\,^{0}_{-5}\ g$ in the chosen one axis and direction and assess whether the secured condition is satisfied;

d) conduct additional shocks with more than 50 g if required, using the same equipment.

8.2.6.2.5 Expression of results

Record the condition of the test specimen after the shock test. After exposure to additional shocks with more than 50 g, the test specimen does not have to be in operating condition any more, but in secured condition.

8.2.6.3 Immersion test

Test the electronic HSL in its operating condition and according to EN 60068-2-17:1994 test Qf with the processing unit as well as the locking device being sunk into water at a depth of 1 m during 30 min or as dielectric fluid is in touch with the processing unit. The HSL shall not open unintentionally.

8.2.6.4 Corrosion test

After testing for corrosion resistance by exposure to three cycles (8 h of exposure to SO_2 and 16 h of exposure to ambient atmosphere) in accordance with EN ISO 6988, the HSL shall be in an operating condition. A completely assembled HSL is to be subjected to this test but batteries may be excluded.

8.2.7 Temperature Resistance

8.2.7.1 Cold

Test the electronic HSL, which is in the normal condition, for 16 h at –10 °C in accordance with EN 60068-2-1:2007, test Ab. After the test when the test sample has reached a temperature of at least +5 °C record its condition.

8.2.7.2 Heat

Test the electronic HSL, which is in its normal condition, for 16 h at +55 °C in accordance with EN 60068-2-2:2007, test Bb. Directly after the test record the condition before the test sample has cooled down to less than 45 °C.

8.3 Reliability testing

8.3.1 Cycling

8.3.1.1 Principle

One HSL test specimen which is in the normal condition before each test, is to be repeatedly subjected to the following test cycle: code input, unsecuring, unlocking, locking, securing.

For electronic HSL the input unit may be tested for reliability separately from the processing unit and locking device. If this is done the software may be modified by the manufacturer to enable this separate test to take place.

8.3.1.2 Cycling equipment

Cycling equipment is specially designed to be able to input an opening code to achieve unlocking, locking and securing. It may also enable code changing to be effected.

8.3.1.3 Procedure

Subject the test specimen to the number of cycles defined in 5.3.1. During the test, the bolt shall be exposed to a load of 2,5 N while 5 000 cycles have to be conducted with the load against bolt extension direction and 5 000 cycles in bolt extension direction.

8.3.1.4 Expression of results

Assess and record the condition of the HSL.

8.3.2 Code changes

8.3.2.1 Principle

One HSL specimen in a normal condition is repeatedly subjected to the following code change procedure:

— entry of valid code;

— code changing activity, e.g. inserting/turning a change key in a mechanical combination lock;

— entry of the new code;

NOTE For some electronic HSL it will be necessary to repeat the code entry.

— setting the new code, e.g. turning/removing the change key in a mechanical combination lock;

— operating the lock with the new code at least three times.

The code changing sequence may be carried out manually or by using the cycling equipment (see 8.3.1.2).

8.3.2.2 Procedure

Subject the specimen to the number of code changes defined in 5.3.3.

8.3.2.3 Expression of Results

Assess and record the condition of the HSL.

8.3.3 Dynamic code input of mechanical combination HSL

8.3.3.1 Principle

The test specimen used in the cycling test and in the normal operating condition is subjected to repeated acceleration, velocity and deceleration conditions.

8.3.3.2 Equipment

Specially designed equipment for repeated code input by controlled acceleration and velocity.

8.3.3.3 Procedure

8.3.3.3.1 Take the specimen used for the cycling test (see 8.3.1), rotate the mechanism for 6 revolutions with 10 rad s^{-1} in one direction.

If the HSL does not unlock input other codes which are within one percent of the setting range of the original opening code and assess whether the HSL unlocks.

8.3.3.3.2 Take the test specimen used in 8.3.3.3.1 and input the opening code with 10 rad per second rotation, decelerated to $800\ ^{+300}_{-100}$ rad s^{-2} to zero speed. Verify if the lock unlocks.

8.3.3.4 Expression of results

Assess and record whether the lock was unlocked.

9 Test report

9.1 Allocate a unique identification number to the test report.

9.2 Report the following:

— name of manufacturer and place and year of manufacture;

— technical documentation supplied in accordance with Clause 6;

— the manufacturer's identification of the test specimen;

— date and place of testing;

— results of tests including descriptions of methods, tools used and calculations for manipulation and destructive burglary;

— the classification achieved during assessment to this European Standard.

10 Marking

Each HSL case shall be legibly and permanently marked in a position which is visible when the HSL is attached to a secure storage unit.

The marking shall comprise at least the following:

a) identification of the manufacturer;

b) model number;

c) year of manufacture;

d) classification;

e) number of this European Standard.

If the resistance grade of the HSL varies according to the type of code input unit with which it is associated this information shall be marked on the HSL.

Annex A
(normative)

Parameters for installation and operating instructions

A.1 Installation instructions

The overall security of an HSL depends on the method of installation and all information to assist installation shall be provided by the manufacturer.

Parameters for installation instructions include the following:

— dimensions of the bolt head or other blocking components;

— blocking feature movement, e.g. of the bolt head from the locked to the unlocked position;

— force which can be exerted by the blocking feature for at least 10 000 cycles;

— materials of secure storage unit to which the lock can be fitted;

— foot print for the fixing screws with indication of the possible threads;

— data concerning the fixing screws which can be used (threads, length, material, strength or, if applicable: only with provided screws);

— recommended torque for the fixing screws;

— recommendations for the screw locking (washers, lock washers, glue);

— position and shape as well as minimum and maximum size for keyholes, spindle holes, cabling bores;

— recommended interfaces to bolt works;

— other data for lock bolt load;

— recommendations for protecting the lock against destructive attacks;

— interface parameters (spindle, spline,…) for mechanical combination locks;

— for electronic locks data on how bolt switches have to be installed, if applicable;

— recommendation that security relevant parts of a HSL should not be accessible to unauthorized persons when the door of the secure storage unit to which it is fitted is open.

The test house may provide a list of sensitive or expected weak points as information for use during the burglary test of the safe or strongroom door (EN 1143-1) (optional).

A.2 Operating instructions

The operating instructions shall contain all facts important for the user/operator in a clear and understandable manner.

The subsequent instructions shall be included:

a) General

1) Security guidelines how to keep keys, cards, tokens, etc. secure.

b) Key locks

1) The key is always to be removed after the opening and locking procedure so that no unauthorized persons have access to it.

2) In the case of a key loss, the lock is to be exchanged immediately or the opening code is to be changed to a new code.

c) Code locks

1) The factory code has to be changed as the HSL is being put into operation by the end user.

2) No simple codes which are easy to guess (e.g. 1, 2, 3, 4, 5, 6) shall be chosen for the coding.

3) No personal data (e.g. birthdays) or other data that could be derived from having knowledge about the code holder shall be chosen for the coding.

4) After code changing, the lock shall be tested several times with the secure storage unit's door in open state.

Only applicable for mechanic code locks: When reaching the secured HSL condition (3.23) the code carriers are to be scrambled.

d) Electronic Tokens

1) Cryptographic key transmission during the initialization process has to be done by an authorized person in a secure environment.

2) Which security relevant information is stored unencrypted, if applicable.

3) 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.

e) Distributed Systems

1) Procedure and frequency for key changes.

Annex B
(normative)

Determination of manipulation resistance due to the design requirement

B.1 General

These design requirement criteria are known to be good indicators of resistance to manipulation for some specific HSL designs. Enough experience has been gained of the design criteria which affects manipulation resistance to enable it to be identified and quantified. For other designs the critical criteria cannot yet be given, but after sufficient testing has been carried out such criteria may be established. Such information, when available, will be included in a future revision of this standard.

B.2 Key locks

B.2.1 General

The code identification mechanism of this example of a HSL key lock involves a bolt-stump component entering the lever gates when they are all correctly aligned. For such locks resistance to manipulation depends upon certain dimensional tolerance and design features of the levers, lever pack and bolt-stump.

Grade A and Grade B HSL key locks which satisfy the criteria given in B.2.2, B.2.3 and B.2.4 and the design requirements in B.2.5 may be judged to be sufficiently resistant to manipulation (see Table 1) and therefore no testing to assess such resistance is necessary.

B.2.2 Gate clearance

The difference between the width of the lever gate and the width of that part of the bolt stump which enters the lever gate during unlocking, shall not exceed half the lever gate movement caused due to one lift height increment. That is:

$$C \leq \frac{H}{2}$$

where

C is the difference between gate and bolt stump widths as calculated below;

H is movement of the lever gate entry due to one lift height increment (see Figure B.1).

C shall be calculated and allowance be made for the corner radii (see Figure B.2) on the lever gate and bolt stump as follows:

$C = S2 - S1 + 0{,}3\ (R1 + R2 + R3 + R4)$

where

S1 is the smallest value for the bolt stump width which satisfies the nominal dimension and tolerances of the manufacturer's drawings. If the bolt stump width is not constant, S1 shall be the width at the point where the R3 and R4 corner radii end.

S2 is the width at which the corner radii R1 and R2 end. If the lever gate is not parallel, see Figure B.3 to determine S2.

RI, R2, R3 and R4 are the largest values of corner radii of the lever gate and bolt stump which satisfy the nominal dimensions and tolerances given in the manufacturer's drawings.

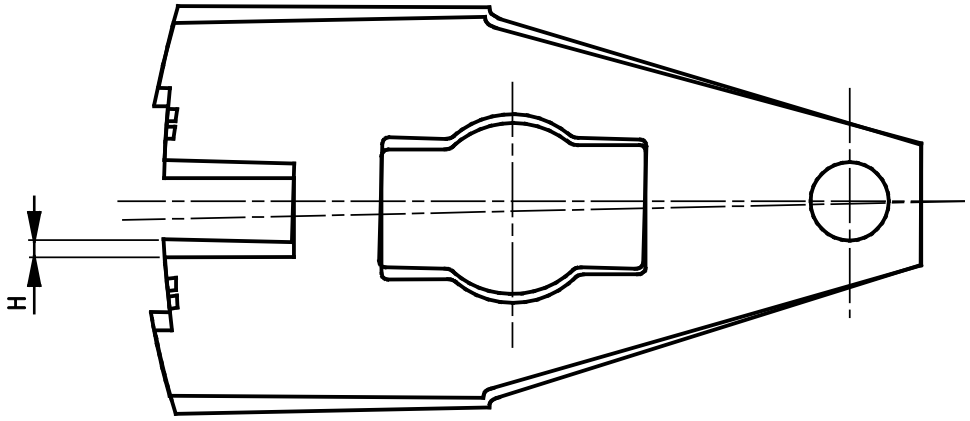
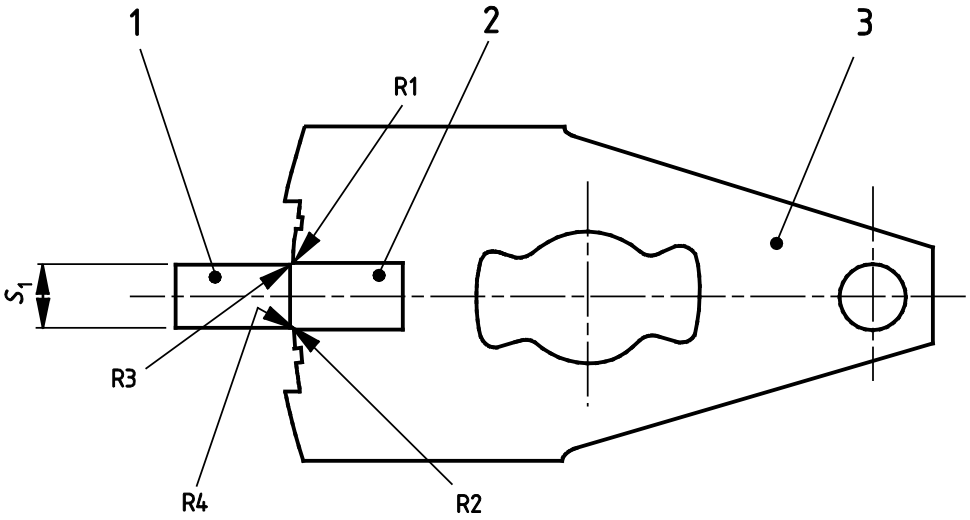


Figure B.1 — Schematic diagram showing movement of lever gate due to one lift height increment



Key

1 bolt stump
2 gate
3 lever

Figure B.2 — Schematic diagram showing corner radii on lever gate entry and bolt stump

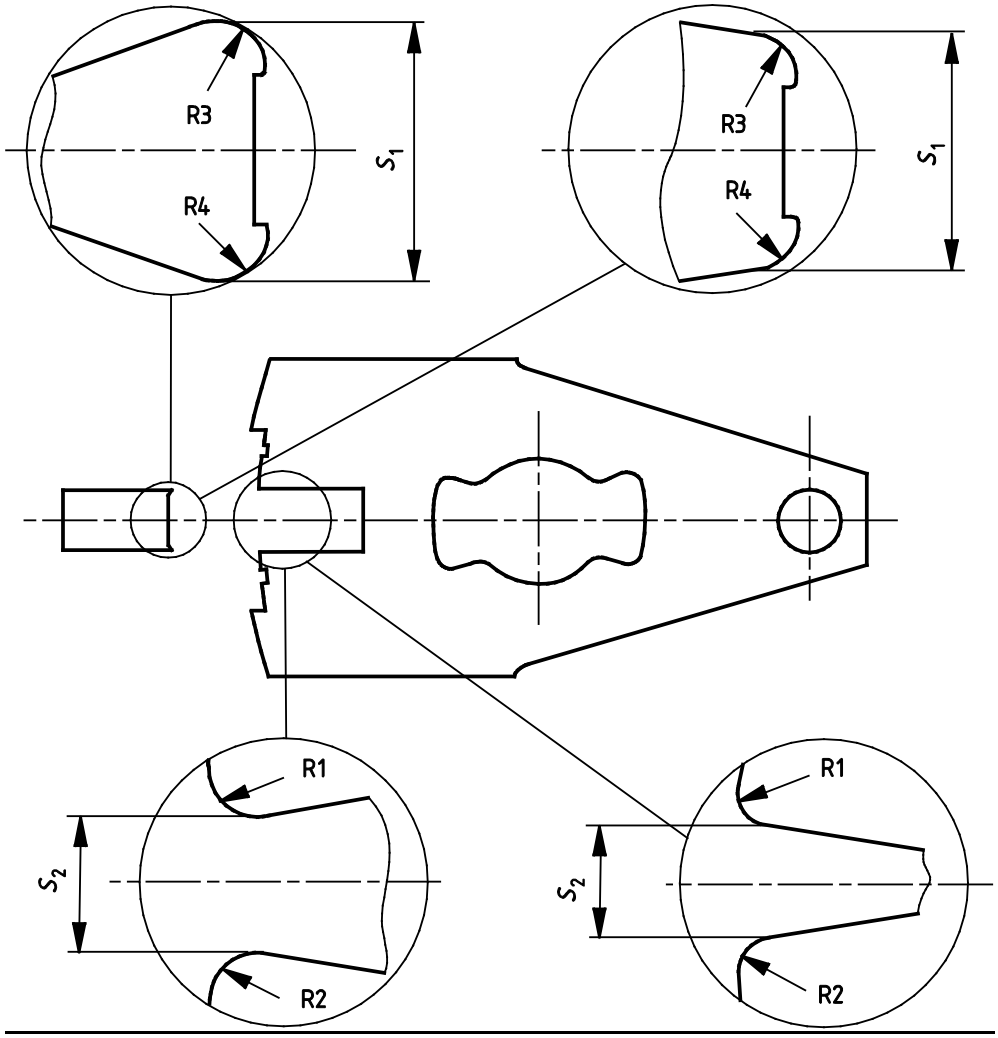
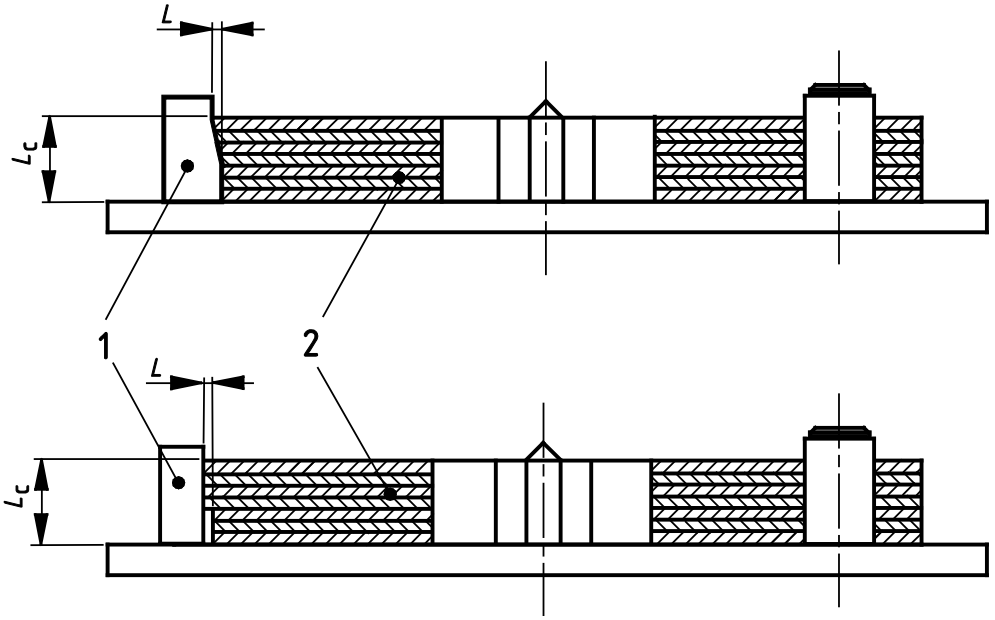


Figure B.3 — Schematic diagram highlighting corner radii on lever gate entry point and face of bolt stump



Key

1 bolt stump
2 levers

Figure B.4 — Schematic diagram showing separation between bolt stump and levers

B.2.3 Bolt stump

When the bolt stump is in contact with any one lever the separation between the bolt stump and any other lever (see Figure B.4) shall satisfy the following:

$$L \leq \frac{L_c}{50}$$

where

L is the maximum separation between the gate entry face of the bolt stump and the surface of any lever (being those parts of the lever other than the gate and false notch which could be contacted by the gate entry face of the bolt stump);

L_c is the width of the lever pack.

B.2.4 False notches

Levers of class A and B key locks shall have false notches (see Figure B.5). For class B locks the positions of the false notches shall correspond to gate positions. There should be no difference between the clearance of the bolt stump and false notches on the levers.

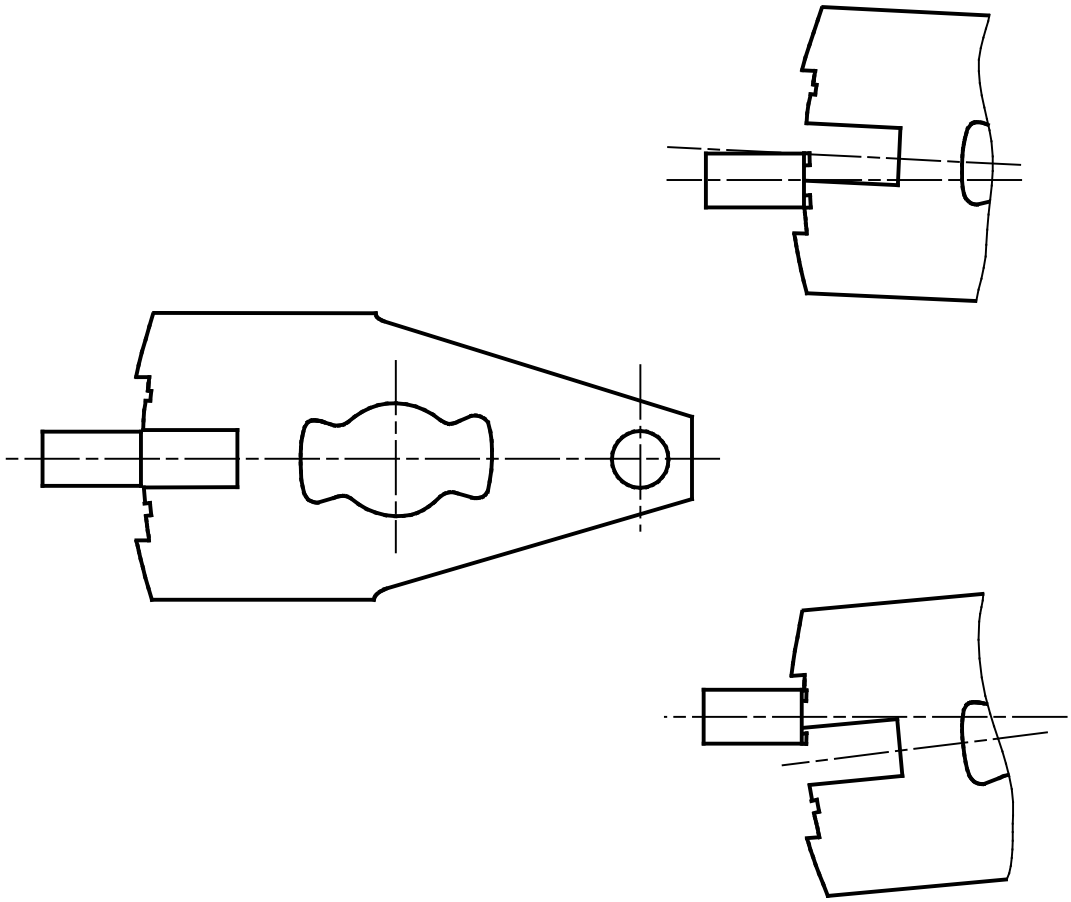


Figure B.5 — Schematic diagram showing false notches

B.2.5 Additional design requirements

B.2.5.1 The minimum number of double-acting levers shall be seven (7) for class A locks and nine (9) for class B locks. Double-acting levers are those which have to be lifted to a prescribed height to align their gates with the position of bolt stump. If lifted too high or too low the misalignment of the lever gates prevents the bolt stump from sufficiently moving into them to retract the bolt.

B.2.5.2 The cross-section area of the keyhole shall not exceed 100 mm^2.

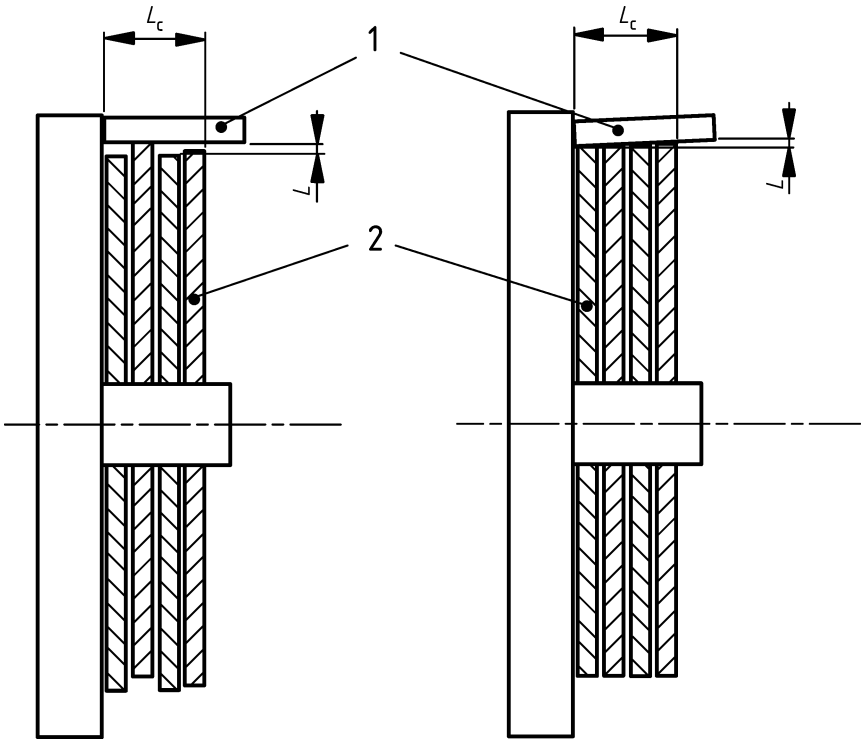
B.2.5.3 It shall not be possible to obtain details of the opening code from the lever shapes or by the amount by which the levers can be lifted. If this requirement is not met a manipulation test should be carried out to establish whether the requirement for Classes A and B are met.

B.3 Mechanical combination locks

B.3.1 General

The code identification mechanism of HSL combination locks of the type used in this example involves a fence component entering the wheel gates when all the wheels are correctly aligned. For such locks, resistance to manipulation depends upon certain dimensional tolerance and design features of the wheels, wheel gates and fence.

Class A and class B HSL combination locks which satisfy the criteria given in B.3.2 and B.3.3 are judged sufficiently resistant to manipulation (see Table 1) and shall not require testing for resistance to manipulation (see 8.2.2).



Key

1 fence
2 wheels

Figure B.6 — Schematic diagram showing separation between fence and wheels

B.3.2 Fence

Measure the force with which the fence contacts the wheel pack. If the force does not exceed 0,35 N then the distance between the fence and any other wheel shall satisfy the following:

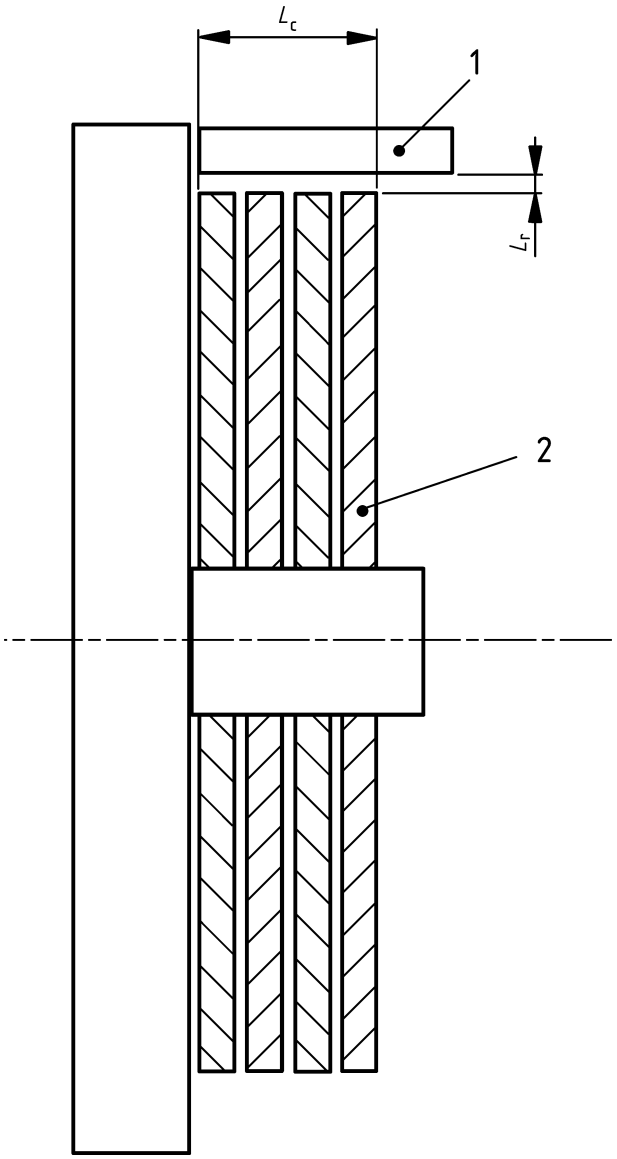
$$L \leq \frac{L_c}{50}$$

where

L is the distance between the gate entry face of the fence and the surface of any wheel (being those parts of the wheel other than the gate which could be contacted by the gate entry face of the fence were it not prevented by the other wheels), see Figure B.6;

L_c is the width of the wheel pack.

When the force with which the fence contacts the wheel pack exceeds 0, 35 N the value of L to any of the wheels shall not exceed 0,2 mm.



Key

1 raised fence
2 wheels

Figure B.7 — Fence raised away from wheels

B.3.3 Wear test

After the reliability cycling test (see 8.3.1) and with the fence in the raised position the distance (L_r) between its gate entry face and the surface of the wheels (see Figure B.7) shall satisfy the following:

$$L_r \geq \frac{L_c}{100}$$

Annex C
(normative)

Manufacturer's Declaration (applies only to key operated locks)

We declare, that during the manufacture of the following key lock: Model_____

at our factory_____, the following measures were taken:

Code Variations: a permutation table has been created to produce the following number of usable codes_____

It is guaranteed that a code will be repeated at the earliest after_____ produced codes_____

Requirement

The following restrictions have been observed during the selection of codes:

a. no fixed precedence for calculation and existing scheme have been used

b. no more than 40 % identical code cuts/lift heights of the total number of levers have been used in the lock (1)

c. no more than two identical code cuts/lift heights have been placed next to each other (1)

d. the difference between the highest and lowest code cuts/lift heights is more than 60% of the maximum height difference of the lock

Key Marking

a. there are no letters, numerals or symbols on the key from which the opening code may be identified

b. no documentation (in any form) which may accompany the key will provide coding information

Knowledge of Lock Location

Measures have been instituted to prevent those persons intimately involved in the production of locks to identify the customer location to which they are despatched.

Distributed Systems

If cryptographic keys are not field changeable (HSL class A only), measures are implemented to prevent those persons intimately involved in the production of locks to identify the customer location to which they are dispatched.

Signature_____

Name (Printed)_____

Date_____

Title in Company_____

(1) In the case of code changeable locks the declaration refers to the key.

Annex D
(informative)

Lock dimensions

Dimensions in millimetres

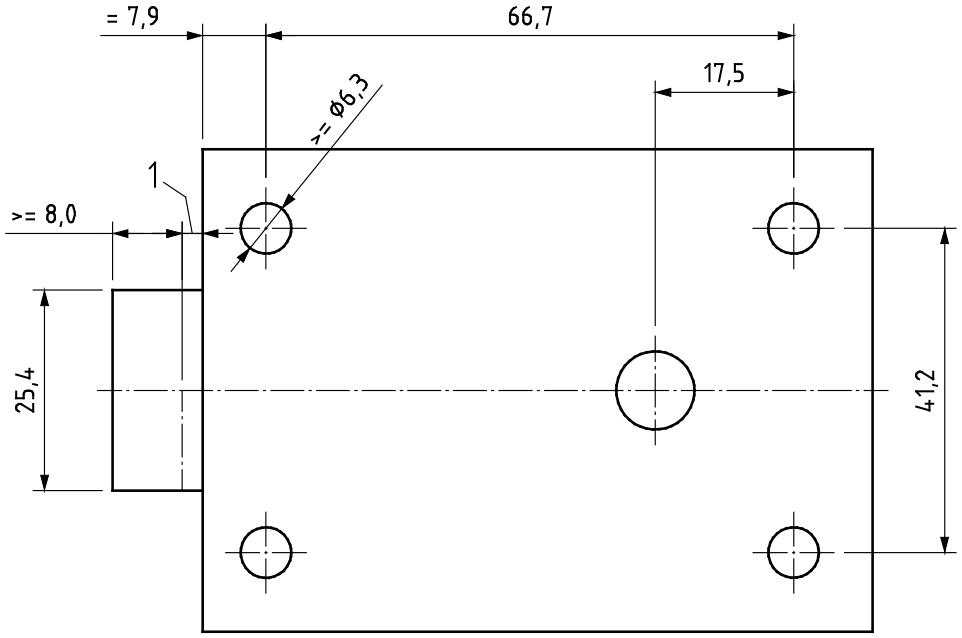


Figure D.1 — Lock dimensions

Bolt projections ≤ 1 mm when lock is open.

Annex E
(informative)

A-deviations

This European Standard does not fall under any Directive of the EU.

In the relevant CEN-CENELEC countries these A-deviations are valid instead of the provisions of the European Standard until they have been removed.

For Swedish additional requirements:

References to existing national Swedish laws and regulations concerning the use of high security locks.

The EN 1300:2013 does not fulfil the national Swedish legislations and regulations (see Table 1).

The EN 1300:2013 does not meet the following Swedish legal requirements:

— The subclause 5.1.5.3 in EN 1300:2013 is not in line with the national Swedish regulations; the Swedish law does not accept HSL-controlled remotely as distributed systems.

— Manipulation resistance, minimum M 180.

— Temperature test: –40 °C/30 min and +70 °C/16 h.

— Cycling test. 25 000 cycles. 25 000 cycles corresponds to appr. 15 years daily use (5 opening/locking per day). After cycling test the lock shall be tested with a key with ½ differ wrong on its highest position. The lock shall not be possible to open with this test.

— Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test. EN 61000-4-37.

Table E.1

Document	Reference	Issued by	Comment
Vapenlagen - Weapons Act	SFS 1996:67	Swedish National Law - The Swedish parliament	**Swedish Weapons Act (SFS 1996:67)** Under the Weapons Act, it is stated that anyone possessing firearms or ammunition is required to ensure that no unauthorized person can gain access to them. Accordingly, all firearms including essential parts and ammunition must be stored in secure cabinets, safes or strong rooms tested and certified in accordance with minimum SECURE CABINETS STANDARD. The above rules also stipulate that before leaving the premises where the weapon and ammunition are being stored, it must be ensured that the storage cabinet has been safely locked accordingly with the minimum HIGH SECURITY LOCK STANDARD *Class B*. Furthermore, the Swedish police authority has the right to check whether weapons are stored in the correct manner. Inadequate storage may result in the revocation of the firearm license.
Public Access to Information and Secrecy Act	SFS 1967: 1997	Swedish National Law - The Swedish parliament	
Regulations and general guidance on the Weapons act	FAP 551-3	The National Police Board	
Regulations and general guidance on storage and transportation of firearms and ammunition by the Police and other State authority.	FAP 943-1	The National Police Board	
Regulations and general guidance on firearm storage by arms traders and associations	FAP 556-2	The National Police Board	
Regulations and general guidance on safety protection	FAP 244-1	The National Police Board	
Storage of explosive goods	SRVFS 2006:10	MSB – Swedish Civil Contingencies Agency	

Bibliography

[1] EN 60721-3-3, *Classification of environmental conditions — Part 3: Classification of groups of environmental parameters and their severities — Section 3: Stationary use at weatherprotected locations (IEC 60721-3-3)*

[2] EN 60721-3-4, *Classification of environmental conditions — Part 3: Classification of groups of environmental parameters and their severities — Section 4: Stationary use at non-weatherprotected locations (IEC 60721-3-4)*

[3] EN ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025)*

[4] NIST SP 800-57 — *Recommendation for Key Management — Part 1: General*

[5] NIST SP 800-67 — *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*

[6] FIPS PUB 140-2 — *Security Requirements for Cryptographic Modules*

[7] FIPS 197 — *Advanced Encryption Standard (AES)*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™