

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

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 1300:2018 sisaldab Euroopa standardi EN 1300:2018 ingliskeelset teksti.	This Estonian standard EVS-EN 1300:2018 consists of the English text of the European standard EN 1300:2018.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 19.12.2018.	Date of Availability of the European standard is 19.12.2018.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 13.310

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

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 3 September 2018.

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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



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

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

Contents

Page

European foreword.....	4
Introduction	6
1 Scope	7
2 Normative references	7
3 Terms and definitions	8
4 Classification.....	14
5 Requirements	14
5.1 General requirements	14
5.1.1 General.....	14
5.1.2 Requirements for all classes	14
5.1.3 Class D HSL.....	14
5.1.4 Mechanical key operated HSL.....	15
5.1.5 Lift heights for mechanical key locks.....	15
5.1.6 Electronic HSL	15
5.1.7 Electronic tokens.....	16
5.1.8 Requirements for cryptography in distributed security systems	17
5.1.9 Firmware updates.....	19
5.2 Security requirements	19
5.2.1 Usable codes.....	19
5.2.2 HSL having over ride feature	20
5.2.3 Manipulation resistance	20
5.2.4 Destructive burglary resistance	20
5.2.5 Spying resistance.....	20
5.2.6 Electrical and electromagnetic resistance	20
5.2.7 Physical environmental resistance	21
5.2.8 Temperature resistance	21
5.3 Reliability requirements	23
6 Technical documentation.....	24
7 Test specimens.....	25
8 Test methods	26
8.1 General.....	26
8.1.1 General.....	26
8.1.2 Evaluation by inspection	26
8.1.3 Test procedure	26
8.2 Security tests.....	27
8.2.1 Usable codes.....	27
8.2.2 Manipulation resistance	28
8.2.3 Destructive burglary resistance	31
8.2.4 Spying resistance.....	31
8.2.5 Electrical and electromagnetic resistance	32
8.2.6 Physical environmental resistance	33

8.2.7	Temperature resistance.....	35
8.3	Reliability testing.....	35
8.3.1	Cycling.....	35
8.3.2	Code changes.....	36
8.3.3	Dynamic code input of mechanical combination HSL	36
9	Test report	37
10	Marking	37
Annex A (normative) Parameters for installation and operating instructions.....		38
A.1	Installation instructions.....	38
A.2	Operating instructions.....	39
Annex B (normative) Determination of manipulation resistance due to the design requirement		40
B.1	General	40
B.2	Key locks	40
B.2.1	General	40
B.2.2	Gate clearance.....	40
B.2.3	Bolt stump	43
B.2.4	False notches	43
B.2.5	Additional design requirements	44
B.3	Mechanical combination locks.....	44
B.3.1	General	44
B.3.2	Fence	45
B.3.3	Wear test.....	46
Annex C (normative) Manufacturer's declaration.....		47
Annex D (informative) Typical locking device dimensions.....		49
Annex E (normative) Determination of burglary resistance due to design requirements		50
E.1	General	50
E.2	Electronic HSL with separate processing unit not included in the locking device	50
E.2.1	Scope of design requirement.....	50
E.2.2	Design requirement.....	50
Annex F (normative) Firmware declaration		51
Annex G (informative) A-deviations		52
Bibliography		55

European foreword

This document (EN 1300:2018) 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 June 2019, and conflicting national standards shall be withdrawn at the latest by June 2019.

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 1300:2013.

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

General changes:

- references have been updated in Clause 2;
- definitions in Clause 3 have been added (locking element, unsecured condition, firmware, application software and trusted device). Other definitions have been defined more precisely;
- Clarifications in 5.1.2.4, 5.1.5.1, 5.1.5.3, 5.1.6.7, 5.1.8.2.3, 5.2.6.3, Clause 6, 8.2.5.8, 8.2.6.1, Clause 10 and Figure 1, Annex D.

Technical changes for any type of lock:

- the requirements for HSL with more than one mode of authentication have been added in 5.2.1
- the shock test has changed (see 8.2.6.2);
- the immersion test is changed and now done with salt water. In addition, it is now done with the input unit sunk in water and in a second new test with the input unit outside of the water (see 8.2.6.3);
- Cycling test has been updated (see 8.3.1.1);
- The manipulation test has been renewed. A third basic value has been added (see 8.2.2.5) and the power supply test is now required for electronic locks (5.1.6.8 and 8.2.5);
- The test report shall initiate the name and version of this standard (9.2);
- The manufacturers declaration in Annex C has been updated.

Technical changes for mechanical key operated locks:

- The requirements for the production of mechanical key operated HSL have been raised (see 5.1.4.1).

Technical changes for electronic locks:

- New requirements for electronic HSL have been added for instance in 5.1.6.1, 5.1.6.2, 5.1.6.3, 5.1.6.8, 5.2.5.4, 5.2.6.1, 5.2.6.3, Table 2, 8.2.5.5, 8.2.5.6, 8.2.6.4, and Annex A. This includes a new EMC test with higher frequency.
- Requirements for one-time-code locks have been added in 5.1.6.9 and Annex A
- The requirements of class A locks of the type “electronic token” and “distributed system” have been raised to the requirements of class B (see 5.1.7.4, 5.1.8.1.6, 5.1.8.1.8, 5.1.8.1.9.1 and 5.1.8.2.2)
- Requirements for the viewing protection of distributed systems with remote input units have been added.
- Requirements for firmware and firmware updates have been added in 5.1.9, Table 1 and in Annex F (“firmware declaration”).
- Design requirements for a certain type of electronic lock have been added in new Annex E.

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

This 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*

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

Introduction

This document also specifies requirements for high security electronic locks (HSL) which are controlled remotely. Regarding distributed systems, this standard responds to the state of the art requirements when it was written down. It is mandatory that the standard has to be revised with a frequency of 3 years as the research in the area of cryptography and relevant attacks evolve with high speed as well as the referenced standards.

1 Scope

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

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

- a) recognized code for preventing code altering and/or enabling/disabling parallel codes;
- b) recognized code for disabling time set up;
- c) integration of alarm components or functions;
- d) remote control duties;
- e) resistance to attacks with acids;
- f) resistance to X-rays;
- g) resistance to explosives;
- h) time functions.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

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

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

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

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

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

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

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

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

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

NIST/SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*

FIPS PUB 140-2:2002, *Security Requirements for Cryptographic Modules*

FIPS 197, *Advanced Encryption Standard (AES)*

3 Terms and definitions

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

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

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1

High Security Lock

HSL

independent assembly normally fitted to doors of secure storage units

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

3.2

code

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

3.2.1

opening code

identification information which allows the HSL to be opened

3.2.2

recognized code

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

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