BUREAU OF INDIAN STANDARDS

DRAFT FOR COMMENTS ONLY

(*Not to be reproduced without the permission of BIS or used as an Indian Standard*)

भारतीय मानक **मसौदा**

सरक्षा उपकरणों हेतु इलेक्ट्रॉनिक लॉक — विशिष्ट

Draft *Indian Standard*

ELECTRONIC LOCKS FOR SECURITY EQUIPMENTS — SPECIFICATION

ICS 13.310

Security Equipment Sectional Committee, MED 24	Last date for comments **31 January 2025**

FOREWORD

(*Formal clause to be added later*)

Over last few years, Electronic locks have entered the high security products market to a great extent, and it is foreseen that the use of these locks will gain popularity in coming years. This standard will be used to assure the consumers for required specifications for Electronic locks (Including Various Input like Keypad, Biometric, pin etc.) to make them compatible for use in high security products.

The availability of an Indian standard is one of the most important steps in establishing the minimum requirements for Electronic locks which provide an assurance to the customer's adequate security level.

For the purpose of deciding whether a particular requirement of this standard is complied with, the final value, observed or calculated, expressing the result of a test or analysis, shall be rounded off in accordance with IS 2 : 2022 'Rules for rounding off numerical values (*second revision*). The number of significant places retained in the rounded off value should be the same as that of the specified value in this standard.

Draft *Indian Standard*

ELECTRONIC LOCKS FOR SECURITY EQUIPMENT — SPECIFICATIONS

1 SCOPE

This standard specifies features, specifications and alarm notification requirements for electronic locks used on high security equipment and access control systems used to store currency, precious metals and important documents.

The following features may be included as optional:

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 REFERENCE

The standards listed in Annex A contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed in Annex A.

3 TERMINOLOGY

3.1 Biometric — The term ‘Biometric’ refers to any features of human body including but not limited to fingerprints, retina, face, palm and veins which may be used to define unique identity of an authorized person to operate security equipment

3.2 Duress — When an authorized person is forced to operate security equipment against his wish, it is termed as ‘under duress’ condition.

3.3 Silent and/or remote alarm — When, after detecting the unauthorized operation/ Duress, an alarm is sent to person/s situated at various locations without alerting the unauthorized person operating the equipment, it is termed as silent alarm for duress and/or remote alarm for unauthorized operation.

3.4 Auto-Dialer — A device that dials predefined phone numbers or/ and messages on predefined events to raise alerts.

3.5 Master/Manager and User — The operator who registers as first user of the Electronic lock is termed as Master/ Manager and the subsequent operators are termed as’ User.’

3.6 Administrator **—** The authorized person who has privileges like enrolling new users, deleting existing users, downloading required data from electronic lock and setting the system in maintenance mode is termed as 'administrator'.

3.7 Dual Control system — The system which opens only when any two of the registered users operate the system simultaneously/ one after other.

3.8 HSL — High Security Lock

3.9 Code — identification information required which can be entered in the HSL and which, if correct, enables the security status of the HSL to be changed

3.10 Opening code — Identification information which allows the HSL to be opened

3.11 Recognized code — Identification information which allows access to the processing unit. It may also be an opening code

3.12 Parallel code — Opening code which has identical function to that of an existing opening code but constructed of different figures

3.13 Coding — Any method by which the code is held

3.14 Material code — Code defined by the physical features or other properties of a token

3.15 Mnemonic code — Code consisting of numeric and/or alphabetic information

3.16 Biometric code — Code comprising human characteristics

3.17 One Time Code — Code generated through an algorithm and is useful only for one-time use.

3.18 Input unit — Part of an HSL which communicates code to a processing unit

3.19 Processing unit — Part of an HSL which evaluates whether the input code is correct and enables or prevents movement of the locking device.

3.20 Locking device — Mechanism which forms part of an HSL and enables or prevents movement of a blocking feature, on presentation of a code.

3.21 Token — Object whose physical form or properties defines a recognized code

3.22 FAR — False Acceptance Rate

3.23 FRR —False Rejection Rate

3.24 EER — Error Expectance rate

3.25 AES — Advanced Encryption Standard

3.26 Encryption — Procedure that renders the contents of a message or file non-legible to anyone not authorized to read it. During the encryption procedure, a cryptographic algorithm using cryptographic key is used to transform plain text into ciphered text.

3.27 Input device — This is an electronic circuit which will take input from human interface and convert it in electronics signals to be sent to controller. e.g. Keypad having capacitive sense or feather touch keys, biometric reader like fingerprint sensor, etc.

3.28 Controller — It is electronics circuit which take inputs from input device, compares with pre-filled data and decides whether lock needs to be opened, drives the motor or solenoid which operates the locking mechanism.

3.29 Output Device — Output device will get activated from controller in specific defined condition/s. e.g. LEDs or Display, Automatic telephone dialer, etc.

4 CLASSIFICATION

Electronic locks shall be of 2 types

4.1 Type 1 — The Electronic locks which are 'Fail Secure' i.e. in power-failed condition, the lock will remain locked and will not provide access to the equipment.

a) Recommended for — Security Equipment using High Security Electronic lock as main layer of access security

4.2 Type 2 — The Electronic locks which are 'Fail Safe' i.e. in power-failed condition, the lock will be opened and will provide access to the equipment.

a) Recommended for —

i) Security equipment using High Security Electronic lock as part of multilayered security
ii) Access control systems

5 CONSTRUCTION AND OPERATION REQUIREMENTS

The Locks may be Battery Operated OR operated by 230 V AC Power supply.

5.1 Low Battery Indication — Battery-powered locks shall operate for at least 3000 complete lock opening and closing operations (Unauthenticated Lock cycle test report to be completed in 2 days). In case of low battery power, an audible or visual signal shall occur during or immediately after an operation. After the first low battery signal at least Twenty-five (25) complete opening and locking cycles shall still be possible. Where it is possible to connect power from the outside it will not be necessary to meet this requirement.

5.2 Communication between Input Device and controller must be encrypted. The data that is sent by the input device to the hardware of the lock shall be at least 128-bit AES.

5.3 In case of biometric lock, the input device shall only read and authenticate the biometric data of the user and shall not take any decision on the access to be granted or not. The Type of sensor can be Optical/ Capacitive/ Swipe etc. The data is to be shared to the lock hardware to make further decisions. The sensors used shall be capable of detecting the liveliness of the bio-tissue presented to the system for authentication e.g. Finger, Iris, Face etc. Reader must be able to distinguish between live fingerprint and dead fingerprint (e.g. Rubber Mould, Photo, fingerprint of dead body, etc.

5.4 Sensor resolution (desired minimum accuracy) for a biometric reader shall not be less than 500 dpi (*see* ISO 19794-2).

5.5 Input device for a lock using fingerprint as input, shall be capable of registering normal fingerprints.

5.6 In duress mode the lock should be capable of communicating with the external world on real time basis to convey the present condition to provide necessary help during catastrophic conditions.

5.7 The lock shall have one Input Port and one Output Port as Standard feature. Additional Input / Output ports may be Provided on the lock.

5.8 Mode of Operation – The Lock shall always be operable under Single or Dual control mode.

5.9 The Power adapter or SMPS used for the locks operating on 230V AC, must meet the requirements of IS 13252 (Part 1) /IEC 60950 Part 1.

5.10 Features of Lock (Minimum)

a) Duress Alert
b) Audit Trail

6 CRITERIA FOR CONFORMITY

The Electronic lock shall conform to the requirements of this standard, only if they successfully pass the tests as specified in this standard.

6.1 Bolt forcing test shall conform as per **8.2** of IS 17566.

6.2 The manufacturer shall declare additional type of tests prior to testing and the conformance shall be decided accordingly (*see* Annex C). Following are the minimum tests to be carried out for all type of locks

a) Electromagnetic radiation disturbance
b) Radiated radio frequency, Electromagnetic field immunity test
c) Electrostatic immunity discharge test

6.3 For Locks operating on 230V power supply, following test shall be conducted in accordance with IS 13252 (Part 1) /IEC 60950 Part 1 (*see* Annex C).

a) Electromagnetic radiation disturbance
b) Radiated radio frequency, Electromagnetic field immunity test
c) Mains Terminal Disturbance Voltages 150 KHz to 350 MHz
d) electrostatic immunity discharge test
e) Voltage dips & short interruptions immunity test
f) Electrical Fast Transients / burst immunity test.
g) Immunity to conducted disturbances, induced by radio frequency fields
h) Surge Immunity Test
i) Resistance Test – As per Annex B

7 PERFORMANCE TESTS

7.1 Endurance Test

The lock (fail secure or fail safe) shall withstand minimum 3,000 cycles of operation, where one cycle constitutes one locking and one unlocking.

7.2 Temperature Resistance Tests

7.2.1 *Cold Test*

Keep the lock at -10 °C for 16 Hours. After removing the lock from cold environment, allow it to come to at least +5 °C and operate. Lock shall operate in normal manner for at least 20 cycles.

7.2.2 *Hot Test*

Keep the lock at +55 °C for 16 Hours. After removing the lock from hot environment, allow it to cool down to less than +30 °C and operate. Lock shall operate in normal manner for at least 20 cycles.

8.1 Recording and Reporting of Test Results

Test report shall include the following:

a) Identification of test specimen
b) Date(s) and place of testing
c) Composition of testing team indicating the roles of the members
d) Description of each test in chronological order of events giving details of point of test, instruments, tools & method used and measurements depending on the tests.
e) Graphs (where applicable) and readings of different instruments used during the test.
f) Photographs of test sample taken before, during and after each test along with the setup.
g) List of tools used with details of critical technical specifications and calibration certificates traceable to NABL.
h) Report on all requirements of the Specification, with values wherever applicable

8.1.1 The test results shall be reported in terms of ‘Pass’ / ‘Conform’ or ‘Fail’ / ‘Does not conform’

9 TECHNICAL DOCUMENTATION AND DESIGN DEFINITION

9.1 The manufacturer shall provide a detailed operational manual of the test specimen, along with the sample offered for testing, indicating the following:

a) A statement of the product designation;
b) Information about any materials or devices intended to generate gas, smoke, electrical arcing or any other substance which may cause harm or injury to the test team members during testing;
c) A list of the models covered by the same design shall also be indicated by their designations, in the event of samples being submitted for type approval or revalidation by a certifying authority;
d) Detail description of the means for setting and changing codes and any precautions to be observed;
e) Recommended methods of installation; and

f) Software and hardware documentation for electronic Lock including software structure.

9.2 The documentation on basis of which type approval or revalidation is obtained, shall be authenticated by the certifying authority and the testing agency. Copies of the authenticated document shall be retained by the certifying organization and the manufacturer and shall be the reference point for future validations or disputes.

9.3 Any deviation from the approved technical documentation, beyond the tolerances permitted in this standard, shall constitute a design change and shall necessitate a revalidation of the design.

10 MARKING

10.1 Marking of Electronic Lock

Sticker/s displaying the following information shall be fixed on the Electronic unit.

a) Manufacturer's name
b) Manufacturer's Trademark (If any)
c) Classification
d) Model Number & Serial Number of the unit.
e) Month & Year of manufacturing
f) Batch number (If any)

NOTE — For the sake of convenience in marking, the manufacturer may devise a codified system combining some or all the information specified, provided all information can be effectively traced back.

10.2 BIS Certification Mark

The product may also be marked with the Standard Mark.

10.2.1 The product(s) conforming to the requirements of this standard may be certified as per the conformity assessment schemes under the provisions of the *Bureau of Indian Standards Act*, 2016 and the Rules and Regulations framed thereunder, and the product(s) may be marked with the Standard Mark

ANNEX A

(*Clause* 2)

LIST OF REFERRED INDIAN STANDARDS

IS No.	*Title*
IS 17566 : 2021	Key locks for security Equipment — Specification
IS 13252 (Part 1) : 2010/IEC 60950 Part 1 : 2005	Information technology equipment - Safety: Part 1 general requirements (*second revision*)
ISO 19794-2 : 2011	Information technology — Biometric data interchange formats Part 2: Finger minutiae data

ANNEX B
RESISTANCE TEST
[*Clause* 6.3(i)]

B-1 PRINCIPLE OF TESTING

The test is intended to simulate an actual attack situation with the use of tools that are most likely to or might happen by some natural phenomena like thunderstorms, lightening or malfunctioning in power supply from electricity supply or other machines working in the periphery. The aim of the attack is to establish the resistance offered by the electronic device while attempting to open the lock without actuating any alarms.

NOTE — The opening of the lock shall be treated successful if not a single alert is sent by the system.

B-2 EXPLORATORY TESTS

An exploratory test shall not be done on the test specimen.

B-3 ACCEPTANCE CRITERIA

The criteria for a successfully completed test are:

a) During test - The display (if Present) of the lock should not hang up, should not display garbage or reset. Bolt should remain locked.

b) After Test - The display (if Present) of the lock should not hang up, should not display garbage or reset. Bolt should remain locked and there should be no loss of data.

B-4 TESTING CONDITIONS

a) Prior to performing the test, exploratory tool attacks cannot be carried out.
b) Non-destructive lock manipulation or lock picking attacks are not allowed.
c) Dust cleaners brush may be used for cleaning the test specimen.
d) Testing shall not be done in areas or against features which have been weakened by earlier tests.

B-5 TEST PROCEDURE

a) The team shall study the electronic lock along with the documentation provided by the manufacturer and accordingly prepare a test plan and document the same with reasons.

b) The team leader shall ensure that the operators use the appropriate procedures that are likely to have maximum destructive impact on the object of attack.

ANNEX C

TEST EQUIPMENTS

(*Clause* 6.2 and 6.3)

C-1 TEST EQUIPMENT LIST

Table C-1 Tools for Electromagnetic radiation disturbance

Anechoic chamber	EMI Test receiver	Ultra-broad band antenna
5 mtrs or 8 mtrs or 10 mtrs	20 Hz to 25 GHz	30 MHz to 1000 MHz
NOTE — This equipment's are used to radiate / receive electromagnetic radiations on / from the electronic lock. The range of the equipment's are described as above		

Table C-2 Tools for Radiated radio frequency, electromagnetic field immunity test

Anechoic Chamber	Signal generator	Power Amplifier	Log period antenna	Double ridge horn antenna
5 mtrs or 8 mtrs or 10 mtrs	9KHz to 22 GHz	10 KHz to 6 GHz	80 MHz to 1000 MHz	0.5GHz to 6 GHz
NOTE 1 These tools are used to radiate / receive electromagnetic radiations on / from the electronic lock. 2 The range of the equipment are as described above.				

Table C-3 Tools for Mains Terminal Disturbance Voltages 150 KHz to 350 MHz

Artificial Mains Network	EMI Test receiver
9KHz to 30 MHz	9KHz to 2750 MHz
NOTE — These tools are used to transmit radio frequency disturbances over the power supply of the electronic lock	

Table C-4 Tools for Electrostatic Immunity Discharge Test

Electrostatic discharge simulator with discharge gun
Range 0.2 to 30 KV
NOTE —These tools are used for discharging electrostatic charges on the electronic lock

Table C-5 Tools for Voltage Dips and Short Interruptions Immunity Test

EMC compact generator dips part. Dips (Interrupts) AC voltage
Range 0 up to 260 V rms. Dips mode <1 period,>1 period. Event duration: <1 period: 1 up to 2999 dips >1 period: 1 up to 2999 dips Switching time: 1 up to 5 microseconds
NOTE — These tools are used to give voltage dips on the power supply voltage of the electronic lock.

Table C-6 Electrical fast transient's / Burst Immunity Test

Fast transient noise simulator with capacitive clamp
250 V to 4KV ±10% in both polarities. Rise time 5ns ± 30% Pulse width 50 ns ± 30% Pulse repeating frequency 2.5KHz, 5KHz & 100KHz
NOTE — These tools will impose fast transients on power supply of the electronic lock.

Table C-7 Immunity to Conducted Disturbances Induced By Radio Frequency Fields

Continuous wave simulator
Output level 1 to 10V Frequency band 9 KHz to 250 MHz Modulation 80% Modulating frequency 1 KHz
NOTE — These tools will superimpose radiofrequency noise on the power supply of the electronic lock

Table C-8 Surge immunity test

EMC compact generator with digital storage oscilloscope and HV probe
Waveform at open circuit: Rise time: 1.2 micro sec ± 30% Time of half value: 50 micro sec ± 20% Adjustable Voltage range: 400 upto 4 KV ± 10% Polarity positive / negative / alternate. Waveform at short-circuit: Rise time: 8 micro sec ± 20% Time to half value 20 micro sec ± 20% Maximum current: 2000 A ± 10% Source impedance: 2Ω.
NOTE — These tools are used to superimpose surge on the power supply of the electronic locks.