BUREAU OF INDIAN STANDARDS

DRAFT FOR COMMENTS ONLY

भारतीय मानक **मसौदा**

सुरक्षा के लिए इलेक्ट्रॉनिक ताले उपकरण - विशिष्टताएँ

Draft *Indian Standard*

ELECTRONIC LOCKS FOR SECURITY EQUIPMENT — SPECIFICATIONS

ICS 13.310

Security Equipment Sectional Committee, MED 24	Last date for comments is **8 September 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, 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 shall 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 security equipment used to store currency, precious metals and important documents or used as access control system to secure premises.

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 TERMINOLOGIES

3.1 Biometric — The term 'Biometric' refers to any features of human body including but not limited to fingerprints 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 user wish, it is termed as 'under duress' condition.

3.3 Silent or remote alarm — When, after detecting the unauthorized operation or Duress condition, 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 remote alarm for unauthorized operation.

3.4 Auto-Dialer — A device that dials predefined phone numbers and/or 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 lock which opens only when any two of the registered users operate using their individual programmed code(s) simultaneously/one after another.

3.8 HSEL — High Security Electronic Lock is designed with advanced and enhanced security features for high-risk applications.

3.9 EL — Electronic lock equipped with basic security features suitable for general purpose applications involving low-risk environments where moderate protection is sufficient.

3.10 Code — Identification information required which can be entered in the HSEL and which, if correct, enables the security status of the HSEL to be changed

3.11 Opening code — Identification information which allows the HSEL to be opened

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

3.13 Input unit — Part of an HSEL which communicates code to a processing unit.

3.14 Processing unit — Part of an HSEL which evaluates whether the input code is correct and enables or prevents operation of the locking device.

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

3.16 AES — Advanced Encryption Standard

3.17 GIPO - General-Purpose Input/Output

3.18 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.

3.19 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.

3.20 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.

3.21 Output Device — Output device will get activated from controller in specific defined condition/s are met.

3.22 Audit Trail — A secure, tamper-evident chronological record of access-related events within a high-security locking system. It includes information such as the identity of the user, date and time.

3.23 Connectivity — The capability of a high-security locking system to securely interface with internal/external devices, networks, or systems through wired or wireless communication

methods. This enables functions such as remote access control, data exchange, system integration, monitoring, and configuration.

3.24 Input Port — An Input port is a hardware interface (GIPO Pin) that allows to receive data, signals, or status to an input system or device.

3.25 Output Port — An output port is a hardware interface (GIPO Pin) that allows to send data, signals, or status to an external system or device.

4 CLASSIFICATIONS

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.

- 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.

- Recommended for — Security Equipment using High Security Electronic lock as part of multilayered security

4.3 Features of Lock (Minimum)

4.3.1 Opening Code(s) shall be stored in Processing unit not physically accessible from outside

4.3.2 There shall be pairing logic between Input unit and Processing unit. Once input unit changed pairing process is mandatory (*applicable for L3, L4)*.

4.3.3 Locks are Categories based on the security features as mentioned in the below table.

Table 1 - Category of Security features

Category of Security features	Duress	Connectivity	Audit Trail
EL- L1	×	×	×
EL- L2	×	×	✓
HSEL-L3	×	✓	✓
HSEL-L4	✓	✓	✓

5 DESIGNATIONS

The Electronic Locks shall generally be designated by their types & feature categories. The designation shall be given in the following manner:

Examples:

"Fail Secure" HSEL having Connectivity and Audit Trail features shall be designated as ***HSEL - Type 1 – L3***

"Fail Safe" EL having only Audit Trail features shall be designated as ***EL - Type 2 – L2***

6 CONSTRUCTION AND OPERATION REQUIREMENTS

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

6.1 The Locks shall be constructed so that it will operate only when the intended code(s) are used.

6.2 Life cycle testing of Locks shall operate for at least intended lock opening and closing operations (*As per Clause 9.1*), for battery operated HSEL/EL is permissible to change to new batteries during cycle test if required.

6.3 Low Battery Indication 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.

6.4 Communication between Input Device and controller shall be encrypted. The data that is transmitted from the input device to the controller shall be encrypted using 128-bit AES encryption or proprietary secure storage feature (*applicable for L3, L4*).

6.5 The fingerprint sensor used in the lock may be of any suitable type, such as optical, capacitive, or other technologies that meet the required performance and security criteria.

6.6 The fingerprint sensor shall be capable of detecting the liveness of the biological tissue presented for authentication (e.g., finger, palm). The sensor shall be able to distinguish between live biometric traits and artificial or non-living replicas, such as rubber moulds, photographs, or fingerprints from a deceased individual.

6.7 In the case of a biometric fingerprint lock, the input fingerprint sensor shall be limited to reading and transmitting fingerprint data for authentication. It shall not independently initiate or control the operation of the locking mechanism. Upon receiving the data, the controller shall determine whether to activate the locking mechanism.

6.8 Sensor resolution (desired minimum accuracy) only for a fingerprint reader shall not be less than 500 dpi (*refer* ISO 19794-2)

6.9 The input device of a HSEL utilizing fingerprint recognition shall be capable of capturing and registering fingerprint images for the purpose of extracting fingerprint templates.

6.10 There shall be a provision in the HSEL *(L4 refer Table 1)* to activate duress mode. In a keypad-based lock, duress mode may be activated using a separate duress code, by adding or subtracting a predefined number from the existing user code, or through any other method. In a fingerprint-based lock, a separate fingerprint shall be registered specifically for activating duress mode or through any other method.

6.11 In duress mode, the lock shall be capable of real-time communication with external systems to report the condition and enable appropriate response or assistance during critical or emergency situations.

6.12 The lock shall have one Input Port and one Output Port as a Standard feature for Firmware update, Audit trail, power source, triggering an alarm, indicator LED, or audible buzzer systems etc. *(Applicable for L3, L4)*. Provision for additional input and/or output ports may also be provided, as required.

6.13 The Lock may be operable Dual (L3 &L4 *refer Table 1)* control mode.

6.14 Audit Trail logs numbers shall be according to security level of the Locks. (L2 – min 100 logs; L3& L4 - min 1000 logs).

6.15 For locks that operate with keypad, minimum codes length required shall be six characters (Applicable for L3/L4)

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

6.17 The lock shall be constructed for installation in a position or location such that it does not reduce the burglary/fire resistant qualities of the security product on which it is being used.

6.18 For lock with sliding bolt, throw of the bolt shall be minimum 7mm from unlocked to locked position. For locks with rotational bolt movement, rotation of the bolt shall be minimum 90 degrees from unlocked to locked position

7 MATERIALS

The critical quality parameters of the materials used for the mechanical components shall be declared by the manufacturer at the time of type approval and records of details of material shall be maintained for conformity during routine production.

8 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.

8.1 The manufacturer shall declare additional type of tests prior to testing and the conformance shall be decided accordingly. The following are the minimum tests to be carried out for battery operated locks.

a) Radiated Emissions test as per the generic standard IEC 61000-6-4 and following the basic standard CISPR 32

b) Electrostatic discharge immunity test as per the generic standard IEC 61000-6-2 and following the basic standard IEC 61000-4-2

c) Radio-frequency electromagnetic field immunity test as per the generic standard IEC 61000-6-2 and following the basic standard IEC 61000-4-3

d) Power-frequency magnetic field (PFMF) immunity test as per the generic standard IEC 61000-6-2 and following the basic standard IEC 61000-4-8

8.2 For Locks operating on Single phase Supply or those that are connected to the Public Power Supply Systems, the following tests shall be performed as a minimum.

a) Conducted Emissions test as per the generic standard IEC 61000-6-4 and following the basic standard CISPR 32

b) Radiated Emissions test as per the generic standard IEC 61000-6-4 and following the basic standard CISPR 32

c) Electrostatic discharge immunity test as per the generic standard IEC 61000-6-2 and following the basic standard IEC 61000-4-2

d) Radio-frequency electromagnetic field immunity (Radiated Susceptibility) test as per the generic standard IEC 61000-6-2 and following the basic standard IEC 61000-4-3

e) Fast transients' immunity test as per the generic standard IEC 61000-6-2 and following the basic standard IEC 61000-4-4

f) Surge immunity test as per the generic standard IEC 61000-6-2 and following the basic standard IEC 61000-4-5

g) Radio-frequency common mode (Conducted Susceptibility) test as per the generic standard IEC 61000-6-2 and following the basic standard IEC 61000-4-6

h) Power-frequency magnetic field (PFMF) immunity test as per the generic standard IEC 61000-6-2 and following the basic standard IEC 61000-4-8

i) Voltage Dips and Interruptions test as per the generic standard IEC 61000-6-2 and products operating **less than 16A** IEC 61000-4-11 or products operating **more than 16A** IEC 61000-4-34 or products operating on **DC supply** IEC 61000-4-29 whichever is applicable

8.3 Type test or Type Approval (*As per clause 8.1 or 8.2*) shall be required before the product introduction into the market. Type approval Certificate is one time test and is kept on record (file) for the third party Inspection/verification.

8.4 For locks that incorporate wireless features such as for example (Bluetooth, Wi-Fi, 3G, 4G, or 5G, etc) the manufacturer shall declare that the integrated wireless module is certified in accordance with the applicable regulatory (e.g. WPC Certificate from Department of Tele communication) and industry standards.

9 PERFORMANCE TESTS

9.1 Endurance Test

The lock (fail secure or fail safe) shall withstand intended number of operation, where one cycle constitutes one locking and one unlocking.

EL - L1 & L2 – 1000 cycles

HSEL - L3 & L4 – 3000 cycles

9.2 Temperature Resistance Tests

9.2.1 *Cold Test*

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

9.2.2 *Hot Test*

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

9.3 BOLT FORCING TEST

Bolt forcing test shall conform as per IS 17566 (*clause* 8.2)

9.4 SALT SPRAY CORROSION TEST

All mechanical components of the lock shall be able to comply with the salt spray corrosion test (*refer IS 17566 (Clause 8.3)*)

9.5 VIBRATION TEST

Test HSEL locks which are in normal condition, for Vibration test, in each of three axes x,y & z , as per the below mentioned table:

Acceleration (g)	Frequency (Hz)	Cycles
1	10 to 150 to 10	10
2	10 to 150 to 10	10

Applicable for EL - L2 and HSEL – L3 & L4

10 RECORDING AND REPORTING OF TEST RESULTS

10.1 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

10.2 The test results shall be reported in terms of 'Pass' / 'Conform' or 'Fail' / 'Does not conform'

11 TECHNICAL DOCUMENTATION AND DESIGN DEFINITION

11.1 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.

11.2 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.

11.3 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.

12 MARKING

12.1 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.

12.2 BIS Certification Mark

The product may also be marked with the Standard Mark.

12.2.1 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/ISO/IEC STANDARDS

IS No.	*Title*
ISO 19794-2	Information technology — Biometric data interchange formats Part 2: Finger minutiae data
ISO 19794-4	Information technology — Biometric data interchange formats Part 4: Finger image data
IS 17566	Key locks for security Equipment — Specification
IS 13252 (Part 1) IEC 60950 (Part 1)	Information technology equipment - Safety: Part 1 general requirements (*second revision*)
IEC 61000-6-4 / CISPR 32	Conducted Emission (CE) Radio interference Measurement test
IEC 61000-6-4/ CISPR 32	Radiated Emission (RE) Radio interference Measurement test
IEC 61000-6-2/ IEC 61000-4-2	Immunity to Electrostatic Discharges (ESD) test
IEC 61000-6-2/IEC 61000-4-3	Radio-frequency electromagnetic field immunity (Radiated Susceptibility) test
IEC 61000-6-2/IEC 61000-4-4	Fast Transient Immunity (EFT) test
IEC 61000-6-2/IEC 61000-4-5	Surge Immunity test
IEC 61000-6-2/IEC 61000-4-6	Radio-frequency common mode (Conducted Susceptibility) test
IEC 61000-6-2/ IEC 61000-4-8	Power Frequency Magnetic Field (PFMF) test
IEC 61000-6-2/IEC 61000-4-11/ IEC 61000-4-34/ IEC 61000-4-29	Voltage Dips & Interruptions (VDI) test