KENYA STANDARD

KS 2112-2-5: 2009
ICS ……...

Electrical Security Systems —

Part 2-5:

Access control systems: Biometric Readers

First Edition 2009

TECHNICAL COMMITTEE REPRESENTATION

The following organizations were represented on the Technical Committee:

Eveready Batteries Kenya Ltd.
Associated Battery Manufacturers
Kenya Railways Corporation
Securicor Alarms (K) Ltd.
Kenya Power & Lighting Company Ltd.
Automotive Industrial Battery Manufacturers (A.I.B.M) (K) Ltd.
Ministry of Energy
Jomo Kenyatta University of Agriculture and Technology — Electrical Engineering Department.
General Electric
Kenya Pipeline Company
Standard Chartered Bank
Kenya Police
Ministry of Information and Communication
Chloride Exide
KK Security Group
BM Security Services

Kenya Bureau of Standards — Secretariat

REVISION OF KENYA STANDARDS

In order to keep abreast of progress in industry, Kenya Standards shall be regularly reviewed. Suggestions for improvements to published standards, addressed to the Managing Director, Kenya Bureau of Standards, are welcome.

KENYA STANDARD

KS 2112-2-5: 2009
ICS ……

Electrical Security Systems —

Part 2-5:

Access control systems: Biometric Readers

KENYA BUREAU OF STANDARDS (KEBS)

Head Office: P.O. Box 54974, Nairobi-00200, Tel.: (+254 020) 605490, 602350, Fax: (+254 020) 604031
E-Mail: info@kebs.org, Web:http://www.kebs.org

Coast Region
P.O. Box 99376, Mombasa-80100
Tel.: (+254 041) 229563, 230939/40
Fax: (+254 041) 229448

Lake Region
P.O. Box 2949, Kisumu-40100
Tel.: (+254 057) 23549, 22396
Fax: (+254 057) 21814

Rift Valley Region
P.O. Box 2138, Nakuru-20100
Tel.: (+254 051) 210553, 210555

Foreword

This Kenya Standard was prepared by the Extra Low Voltage Equipment Technical Committee under the guidance of the Standards Projects Committee, and it is in accordance with the procedures of the Kenya Bureau of Standards.

During the preparation of this standard, reference was made to the following documents:

SANS 2220-2-5:2005 Part 2-5: Access control systems: Biometric Readers

Acknowledgement is hereby made for the assistance derived from these sources.

Electrical security systems

Part 2-5: Access control systems: Biometric readers

1 Scope

1.1 This part of KS 2112 specifies the characteristics of biometric readers intended to be used in access control systems.

1.2 KS 2112-2-1 specifies the general characteristics of access control systems.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of KS 2112. All standards are subject to revision and, since any reference to a standard is deemed to be a reference to the latest edition of that standard, parties to agreements based on this part of SANS 2220 are encouraged to take steps to ensure the use of the most recent editions of the standards indicated below. Information on currently valid national and international standards can be obtained from Kenya Bureau of Standards

IEC 60050-191, *International electrotechnical vocabulary – Chapter 191: Dependability and qualityof service*.

IEC 60300 (all parts), *Dependability management*.

KS 2112-2-1, *Electrical security systems – Part 2-1: Access control systems: General characteristics*.

KS 2112-2 *Electrical security installations – Part 2: Access control*.

3 Definitions

For the purposes of this part of KS 2112, the definitions given in KS 2112-2 apply.

4 Requirements

4.1 General

4.1.1 Construction

A biometric device shall contain a sensor that recognizes a person's physical characteristics, such as:

a) fingerprints;

b) hand geometry (finger position and length);

c) retina patterns;

d) voice patterns; or

e) signature.

4.1.2 Components

A biometric reader shall consist of:

a) a sensor;

b) an enclosure; and

c) a personal identification number (PIN) keypad (optional).

4.1.3 Sensor

As the measurement of a person's physical characteristics will not correspond 100 % with the previously stored records of the physical characteristics, a threshold of an acceptable level of analogy detected by the sensor shall be set in the biometric system. The threshold shall be adjustable by a designated responsible person only.

4.1.4 PIN keypad

If a PIN keypad (from which a personal identification number can be entered) is used, access shall only be granted on validation of both the PIN and the measured physical characteristics.

4.1.5 Reliability

The MTBF (mean time between failures) (guaranteed by the supplier) of a biometric reader (assessed in accordance with IEC 60050-191 and IEC 60300 (all parts)) under normal operating conditions shall be as given by the supplier (see 5.2).

4.1.6 Interface capability

If a biometric reader is connected to a central processor, it shall be by means of standard communications protocol.

4.1.7 Updating

As a person's physical characteristics can change with time, it shall be possible to update the stored record for each person.

4.1.8 System capacity

The biometric system software and data base shall accommodate characteristics of the required number of persons.

4.1.9 Safety

The biometric device shall comply with all relevant health and safety requirements and regulations (see 5.3).

4.2 Environmental requirements

When a biometric device is tested in accordance with 6.3, it shall not be adversely affected and shall not be damaged.

4.3 Functional requirements

When a biometric reader is tested in accordance with 6.4 and 6.5, it shall comply with the following requirements.

4.3.1 Operating time limits

The operations listed in column 1 of table 1 shall be completed within the time limits given in columns 2 or 3, even if the data base is filled to its capacity.

Table 1 — Time limits

1	2	3
Type of system	**Initialization time** s, max.	**Comparison time** s, max.
Fingerprint	60	5
Hand geometry	30	2
Retina pattern	60	3
Voice pattern	60	5
Signature	120	15

The rate of rejection of authorized users shall be not more than one in twenty.

4.3.3 False acceptance rate

The rate of acceptance of unauthorized users shall be as specified by the supplier.

5 Marking

5.1 General

Each biometric reader shall bear the markings required by KS 2112-2-1.

5.2 Additional information

The following information shall be supplied together with each biometric reader:

a) performance characteristics:

– number of points of comparison measured;

– false rejection rate limits; and

– false acceptance rate limits;

b) power supply requirements;

c) wiring and mounting instructions;

d) output ratings;

e) instructions for adjustment, including specification of any special tools required;

f) program for maintenance and servicing;

g) advice on the application of the biometric reader, to avoid inappropriate use and potential false operation;

h) the number of persons whose characteristics can be stored;

i) any other information considered useful by the manufacturer; and

j) the MTBF.

5.3 Safety

In addition to the information listed in 5.2, the manufacturer shall provide a certificate for each retina scanner that indicates compliance with the relevant health and safety requirements. It shall also indicate the permissible light level to which the human eye may be repeatedly exposed.

6 Inspection and methods of test

6.1 Inspection

Visually examine each biometric reader in the sample for compliance with all the relevant requirements of this part of KS 2112 for which tests to assess compliance are not given in 6.3 to 6.5 (inclusive).

6.2 Conditions of test

Carry out the tests (other than the environmental tests) under the following standardized atmospheric conditions:

– temperature: 15 ℃ to 35 ℃;

– humidity: 25 % to 75 %;

– atmospheric pressure : 86 kPa to 106 kPa.

6.3 Environmental tests

Carry out the environmental tests given in table 2

Table 2 — Environmental tests and severities

1	2
Test	**Severity**
Dry heat*	3
Cold* – Hand, voice	3
Signature, finger, retina	2
Sinusoidal vibration	1
Damp heat, steady state*	1
Variation in power supply*	2
Electrical spikes*	4
Electrostatic discharge*	1
Electromagnetic fields	4
Impact	1
*Carry out this test while the system is connected to its power supply and is functioning.	

6.4 False rejection rate test

6.4.1 Apparatus

Install the biometric reader in accordance with the manufacturer's instructions and link it up to the required processor software program.

6.4.2 Procedure

Load into the biometric system the characteristics of any person to be read by the biometric reader, in accordance with the manufacturer's instructions. Follow the manufacturer's instructions to present a person's characteristics in order to gain access. Repeat this exercise 20 times and check for compliance with 4.3.1 and 4.3.2.

6.5 False acceptance rate test

6.5.1 Apparatus

As in 6.4, without changing any setting of the biometric reader.

6.5.2 Procedure

Load into the biometric system the characteristics of any person to be read by the biometric reader, in accordance with the manufacturer's instructions. Follow the manufacturer's instructions to present a person's characteristics in order to gain access, but present characteristics not loaded on the system for a number of times in accordance with the supplier's stated false acceptance rate, and check for compliance with 4.3.3.