

# Kaba elolegic Reader

Contactless Access Control Reader





## Kaba elolegic reader

The simple solution for economic access control or contactless switch

#### Applications

The Kaba Elolegic reader is a standalone reader needing only a dc power supply. It can therefore be fitted anywhere where access is to be controlled, e.g. on industrial and commercial business premises, sports clubs, multi occupancy residential buildings, medical facilities parking sites etc.

It is particularly useful when adding to an existing Mechanical Master System utilising the existing cylinders as the reader can be used with any Legic media in any mix of keys and cards or card and fobs etc. The elolegic reader can be used in conjunction with other members of the Kaba elolegic Family

#### Features

- ✤ 2400 Users
- Choice of Media: Prox Card, Smart Key, Fob, Watch etc.
- 8 Time Zones
- Big Event Memory
- Simple Programming
- Options:Programmer
- Frogram
   Software
- Securely Encrypted Media Communication
- Stand Alone system with
- Contemporary look
- Fits standard wall outlets
  Standard & Secure
- Versions
- 10cm read/write range

#### **Technical Data**

Power Supply

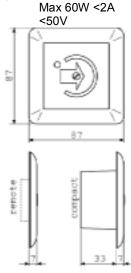
Protection Temperature Humidity

Output Relay

IP40 or IP55 -25...+70° C 0...95%rH Non Condensing Potential Free

12 to 24 vdc

max 2.0VA/W



### Operation

When the user presents the Legic media to the reader, the electronic processor in the reader identifies the unique media chip number. If the chip number has been previously programmed into the reader memory, a valid signal is sent to the door release relay, which is operated for the pre-set time. This relay can be used to operate any electrical door-locking device.

#### Kaba UK Limited

Lower Moor Way Tiverton Devon EX16 6SS Tel: 0870 000 5625 Fax: 0870 000 5397 www.kaba.co.uk info@kaba.co.uk

## Legic<sup>®</sup> Technology

The media used contains a tiny Legic chip and antenna. The data transfer of Kaba Legic guarantees a secure and contactless communication. Data transfer is encrypted in both directions. Each time a media communicates, a new random password is used. Copying the data transferred for later use is pointless. Each media is given a unique number when manufactured and once programmed is unchangeable and virtually impossible to copy.

