

Biometric Readers

	Page
Bioblock: Fingerprint Security Reader Kits	110
Bioblock: Standalone Cabling Diagram	110
Basis of Biometrics: Fingerprint Minutia Capture	111



BIO-SBLBDSTR



BIO-SBLSDDSTR

BIO-SBLBDSTR & BIO-SBLSDDSTR
BioLock Fingerprint Reader Kits (Black or Silver)

The first truly weather-proof metal fingerprint reader in standalone or multi unit mode for securing entry to your home or office. Utilising radio frequency scanning technology, this system gives a very high level of security at an affordable price.

Designed and manufactured in Australia, the BioLock fingerprint reader kit is a brilliant new product which opens your door by recognising your unique fingerprint. No keys, no hassles, and one touch access to any authorised or designated user at home or in the office. The BioLock kit is supplied with free PC software called BioKey, which provides full access control and time management reports. You can also organise BioLock to turn lights on and off, arm and disarm alarm systems, open garage doors or gates etc.

Stand alone mode capacity:

50 finger templates and more than 20,000 log transactions.

Multi unit mode capacity:

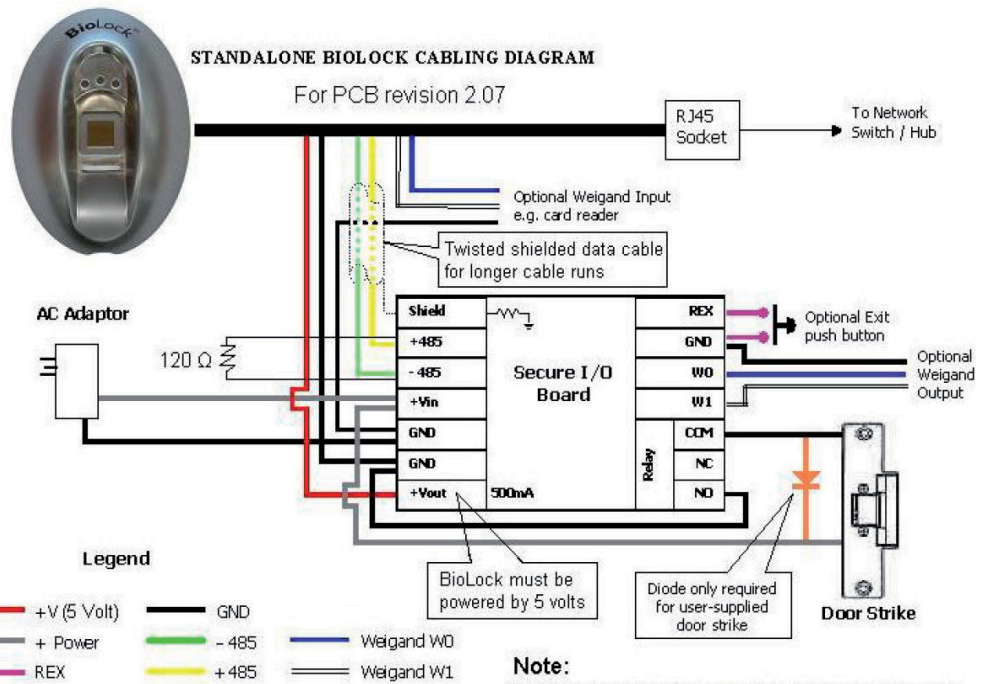
100 finger templates and unlimited log capacity.

- Mounting: Any flat surface via 4 screws (included) or bolts
- Environment: Waterproof IP65
- Power: 12V DC 1A power adapter
- Inputs: Request to Exit (REX) connection
 Wiegand input for proximity or other cards or barcode readers
 Tamper switch for firmware control
- Outputs: Relay NO/NC contact
 Wiegand output on each secure relay board
- Modes: Standalone, networked, or networked with emergency standalone fall-back
- Communications: 10BaseT 10MB/s Ethernet LAN (required for network mode), RS485 (secure relay board)
- Control: Built-in web-server, optional Windows software, and off-line PIN entry for multi-unit
- Remote access: Via built-in web-server, and Ethernet for multi-unit
- PIN code: Set or cancelled by web-server, or finger sensor
- Colours: Gloss chrome (silver) or matt black finish
- Both modes available in one package
- Dimensions (mm): 75 (W) x 105 (H) x 27 (D) - (size of a PC mouse)

EX GST INC GST

\$	BIO-SBLBDSTR	BIOLOCK FINGERPRINT STANDALONE READER KIT - BLACK
	BIO-SBLSDDSTR	BIOLOCK FINGERPRINT STANDALONE READER KIT - SILVER

Standalone BioLock Cabling Diagram

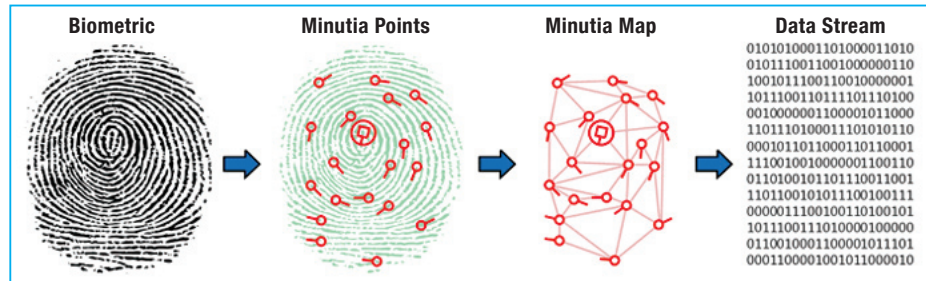


Note:
 Cable longer than 5m use Fig 8 for BioLock power and twisted shielded data cable for RS485 and termination resistors.

Note: For cable longer than 5 meters use figure-8 cable for BioLock power, and use twisted shielded data cable for RS485 and termination resistors.

Basics of Biometrics - Finger Minutia Capture

The unique nature of a fingerprint makes it ideal for use in automated recognition systems. A fingerprint is made of a series of ridges and grooves. Once a fingerprint is captured the system locates the minutia points. These minutia points occur where the lines of the ridges begin, end, branch off and merge with other ridge lines. These points are then mapped and a line is drawn between each point. This creates a map of how each point relates to the other points. The map is then stored as a data stream called a minutia template in a database for future comparison with other presented fingerprints. It is important to note that during the entire process no fingerprint images are stored on the system and a fingerprint image cannot be recreated from the minutia template.



Differences between Identification and Authentication

Identification (also known as 1:Many, 1:X or One to Many)
Using specialised indexing techniques a sample is effectively matched against all templates in the database. In specialised high end systems a sample can be matched in against hundreds of thousands

Put simply, a person does not have to provide any input other than their biometric.

Authentication (also known as Verification, 1:1 or One to One)
The sample is matched against one pre-selected template.

Put simply, a person swipes a card or enters a user code to select a biometric template to match against.

Measuring Biometric Effectiveness

There are 2 commonly used gauges for measuring the effectiveness of biometrics matching technology.

1. False Rejection Rate (FRR) as known as False Non-Match Rate (FNMR)
FRR is a value that measures the percentage of times a biometric sample is matched against a single or multiple biometric templates where a biometric template exists but the likeness between the sample and template is below the decision threshold setting so no match occurs.

Put simply, it is the number of times people do not get identified when they should be identified.

2. False Accept Rate (FAR) also known as False Match Rate (FMR)
FAR is a value that measures the percentage of times a biometric sample is matched against a single or multiple biometric templates where a biometric template does not exist but the likeness between the sample and template is above the decision threshold setting so a match incorrectly occurs.

Put simply, it's the number of times people get identified when they should not be identified.

Notes