

Access Control



CCTV Systems



Intruder Alarms



DDA Systems



Barriers



Biometrics



ID Card Systems



# Fingerprint Access Control Applications Guide



Axxess 28 Limited

Unit 18 The Rosemary Centre, Blackwater, Camberley, Surrey, GU17 0LS

Telephone: 0845 680 0228 Facsimile: 0845 680 0229

Email: [sales@axxess28.com](mailto:sales@axxess28.com) Internet: [www.axxess28.com](http://www.axxess28.com)

Registered in England No. 2640434

## Typical Access Control Security Levels

Access Control



CCTV Systems



Intruder Alarms



DDA Systems



Barriers



Biometrics



ID Card Systems



### Security Characteristics

### Disadvantage

#### Key



Requires the person to have a key to gain access

Keys can be borrowed, easily copied, lost and stolen.

#### Keypad Only



Requires the person to know the pin number to gain access

PIN numbers can be shared between people.

#### Card Only



Requires the person to have a valid card to gain access

Cards can be borrowed, copied, lost and stolen.

#### Card & PIN



Requires the person to have a valid card and know the pin number to gain access

Cards can be borrowed, copied, lost and stolen and PIN numbers can be shared between people.

## Fingerprint Readers Key Features

Access Control



CCTV Systems



Intruder Alarms



DDA Systems



Barriers



Biometrics



ID Card Systems



- ✓ A positive link between a person and their PIN or card.
- ✓ Easy, increased security.
- ✓ Wide range of interfaces for PIN entry device (Proximity, magnetic stripe, Wiegand, Watermark, Keypad, Smart Card).
- ✓ Choice of fingerprint template location – internal, Magstripe track 3 and contactless Smartcard (Mifare, Legic or HID iClass)
- ✓ Fully automatic network for easy template database maintenance.
- ✓ Fast – verification in approx 1 second.
- ✓ Selectable user security levels.
- ✓ Easy to follow LED and LCD instructions.
- ✓ User definable LCD screen for multi-lingual display.
- ✓ No PC required.
- ✓ Standalone.
- ✓ Copes with “difficult” users via individual security levels.
- ✓ Prevents unauthorised access
- ✓ No changes to existing system – low cost integration.

## Access Control



## CCTV Systems



## Intruder Alarms



## DDA Systems



## Barriers



## Biometrics



## ID Card Systems



# Fingerprint Readers



## Verid+

Retro fit onto your existing access control by using the card readers as the pin input device.



## Verid+ PIN Keypad

Use standalone on one door or as part of a system.



## Verid+ with integral HID Proximity Reader

Retro fit onto your new or existing access control using HID cards and readers on general access controlled doors.



## Verid+ Contactless Smartcard

Use contactless MIFARE, Legic and HID iClass smartcards for carrying your fingerprint data on the card.



## Verid+ Event Logger

Use standalone on one door or as part of a system to log user events at the reader.

Access Control



CCTV Systems



Intruder Alarms



DDA Systems



Barriers



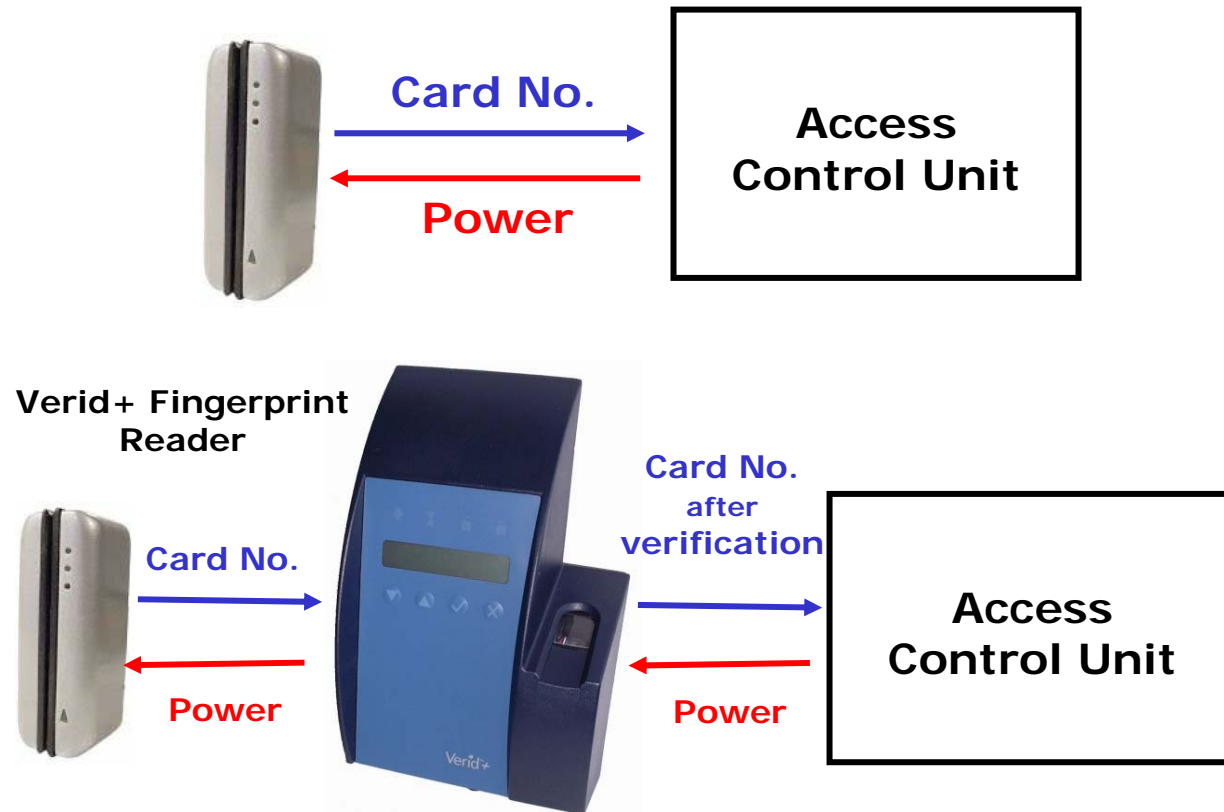
Biometrics



ID Card Systems



## Retro-fitting Verid with existing Access Control (Single Door Position)



- Fingerprints are enrolled locally at the door / fingerprint reader position.
- The Verid passes the card / pin number to the ACU after successful verification.
- The Verid passes on an error code of zeros to the ACU after unsuccessful verification and use of a card / pin not enrolled on the Verid fingerprint reader. The ACU cannot monitor the card / pin numbers that have not successfully verified or card / pin misuse.

## Fingerprint Reader Basic System

Commercial and Industrial Security Systems and Solutions

Access Control



CCTV Systems



Intruder Alarms



DDA Systems



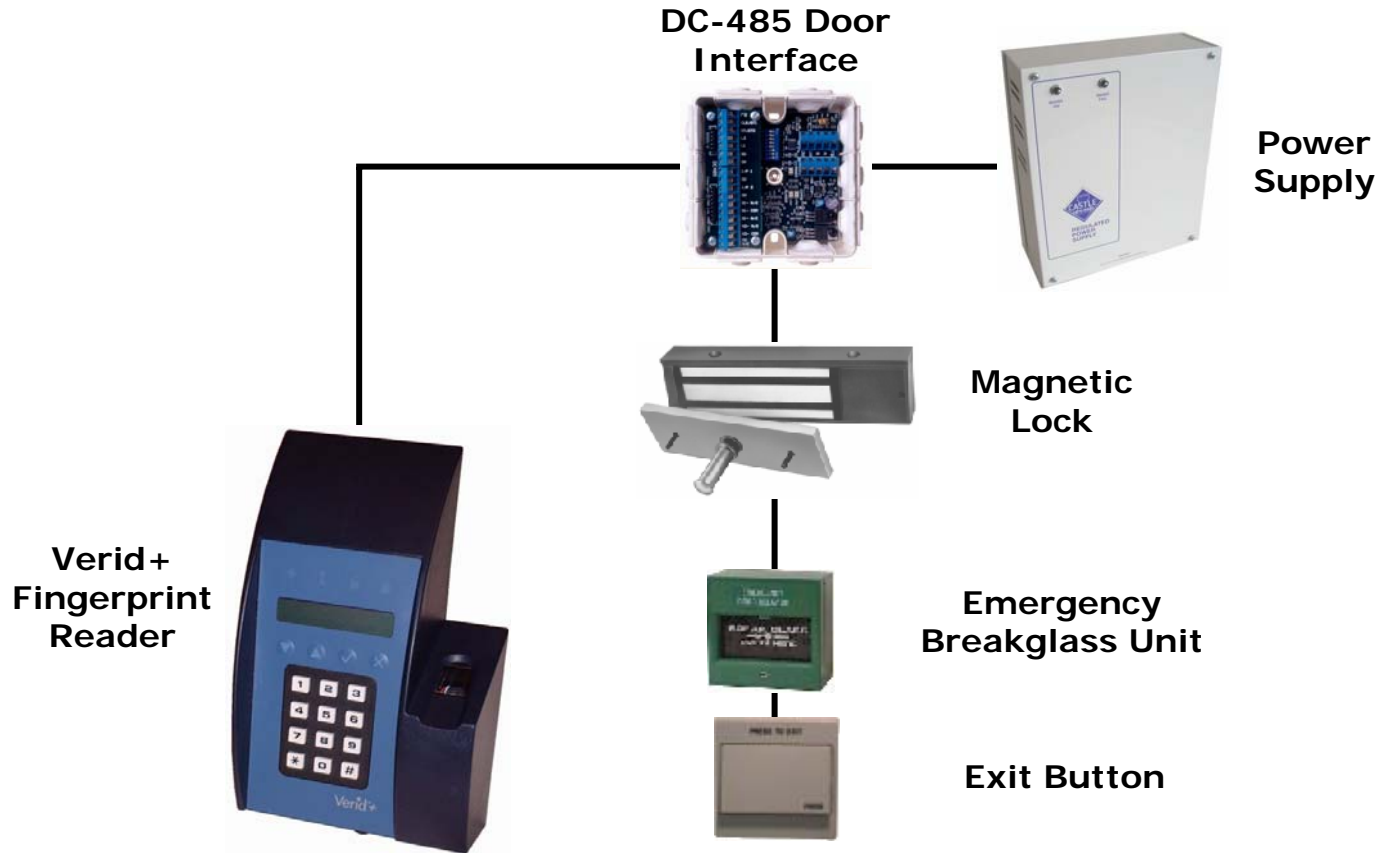
Barriers



Biometrics



ID Card Systems



- Fingerprints are enrolled locally at the door / fingerprint reader position.
- In this mode any enrolled finger that is successfully verified will send a data signal to the DC-485 door interface to release the lock. Unsuccessful verifications will not release the lock.
- No events are logged.
- The DC-485 door interface is use to connect the door furniture to on the secure side of the door.

## Fingerprint Reader Logger System

Commercial and Industrial Security Systems and Solutions

Access Control



CCTV Systems



Intruder Alarms



DDA Systems



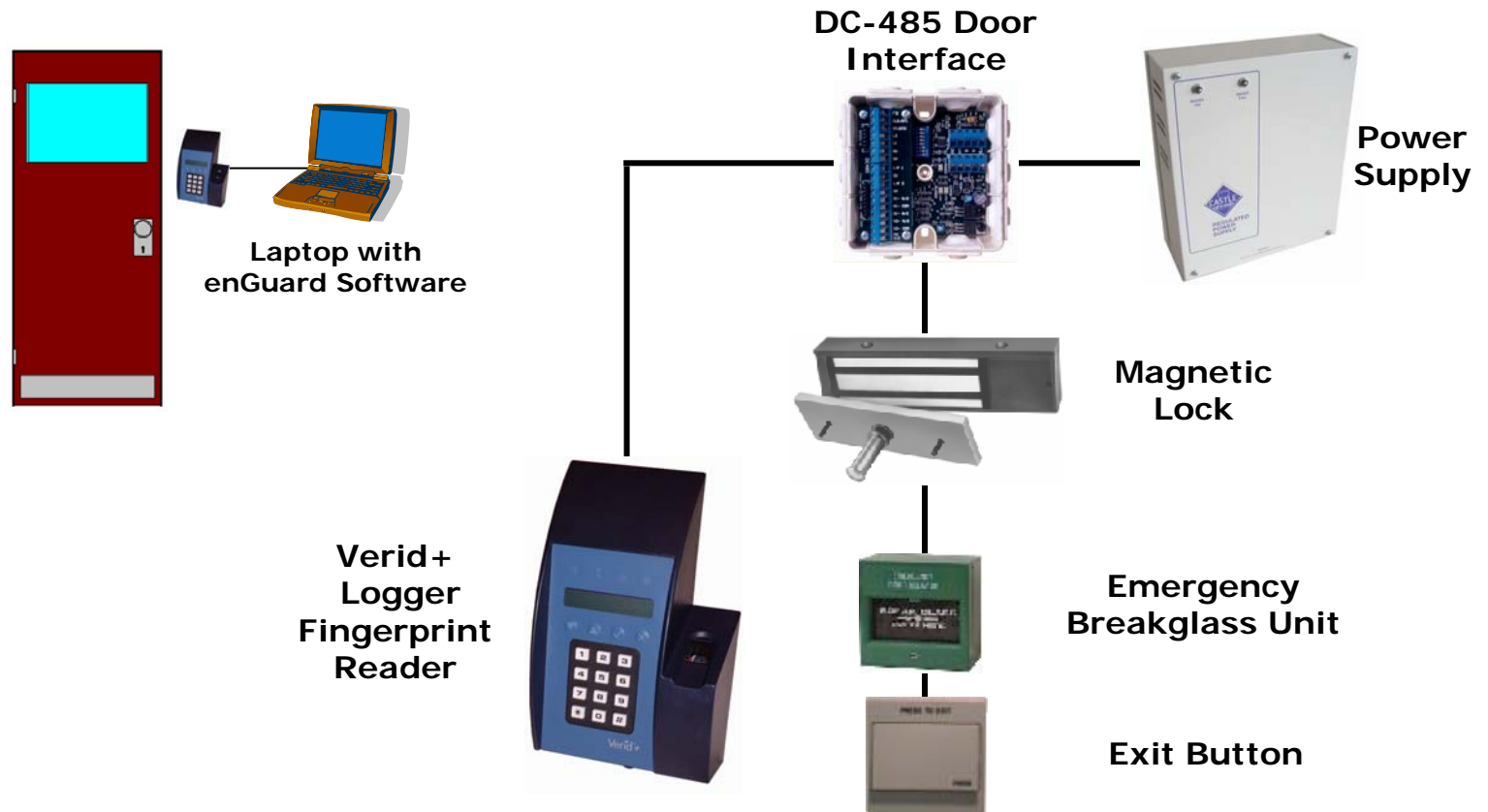
Barriers



Biometrics



ID Card Systems



- Fingerprints are enrolled locally at the door / fingerprint reader position.
- In this mode any enrolled finger that is successfully verified will send a data signal to the DC-485 door interface to release the lock. Unsuccessful verifications will not release the lock.
- The Verid+ Logger logs Verify Passed (plus In and Out), Verify Fail and Unknown PIN against time and date.
- The enGuard software on a laptop is used to download events.

## Fingerprint Access Control System

Access Control



CCTV Systems



Intruder Alarms



DDA Systems



Barriers



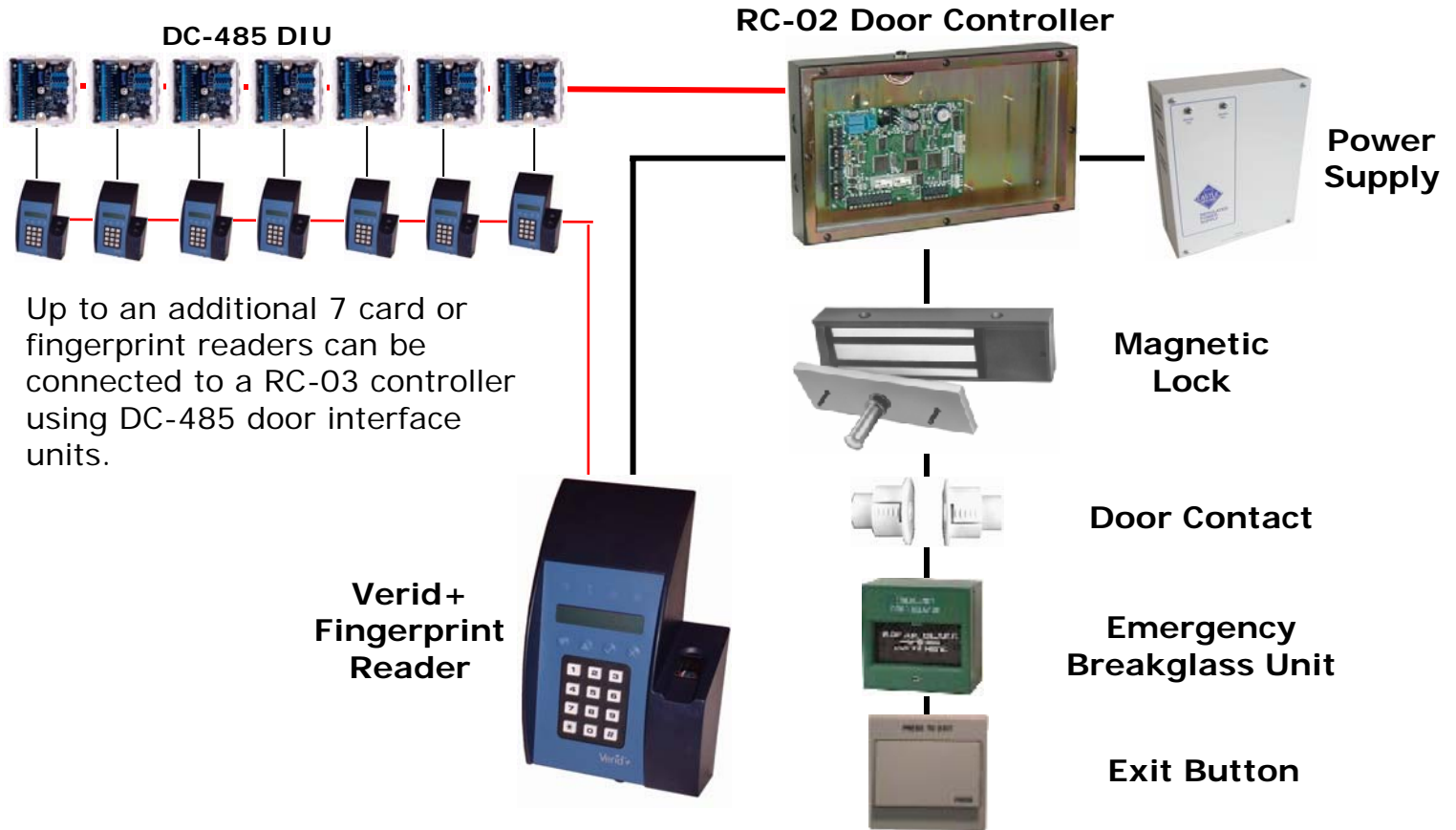
Biometrics



ID Card Systems



Commercial and Industrial Security Systems and Solutions



- Fingerprints are either enrolled locally at the door / fingerprint reader position or at the PC position if you want to store and distribute fingerprint template automatically.
- The RC-03 logs Verify Passed (plus In and Out), Verify Fail, Unknown PIN and all door alarms against time and date.
- The enGuard software is either manually synchronised via laptop or permanently connected over your network to the RC-03 to update cards and download alarms and events.

# Fingerprint Access Control Packages

Access Control



CCTV Systems



Intruder Alarms



DDA Systems



Barriers



Biometrics



ID Card Systems



Commercial and Industrial Security Systems and Solutions

Fingerprint Verification	Basic	Logging	System
Fingerprint Verification	X	X	X
Local enrolment	X	X	X
Enrolment at PC			X
Events Logged: Verify passed IN, Verify passed OUT, Verify passed, Verify failed and unknown PIN		X	X
<b>Door Controls</b>			
Request to exit	X	X	X
Door status monitoring			X
Lock release relay output	X	X	X
Local Alarm relay output (for sounders & CCTV etc)			X
Events Logged: door forced, held, not opened, exit request			X
User adjustable unlock time			X
User adjustable alarm time			X
<b>Access Control</b>			
Outside In support (all successful fingerprint verifications allow access)	X	X	
Time and entry zones			X
Timed operations			X
T&A reports		X	X
Events Logged: wrong time, wrong entry zone, wrong door, pre-issued PIN and expired PIN misuse			X
<b>Reports</b>			
Activity report to printer or file		X	X
<b>Communications</b>			
RS-232		X	X
LAN/WAN		X	X
<b>Capacity</b>			
Fingerprint users	5000	4500	5000
Logged events	0	4092	13500
Number of doors	1	1	Up to 8*

## Access Control



## CCTV Systems



## Intruder Alarms



## DDA Systems



## Barriers



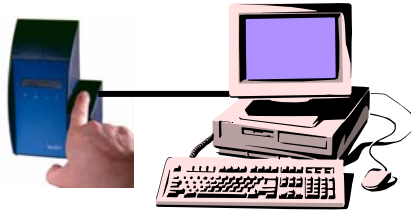
## Biometrics



## ID Card Systems



# Fingerprint Access Control Key Biometric Features



- Fingerprint enrolment and verification at any enGuard Server or Client PC.
- Fingerprint Template storage in the enGuard database.
- Fingerprint Templates are intelligently distributed using LAN/WAN, GSM and dial-up modem.
- Supports Fingerprint reader *Transparent* and *Inhibit* modes.
- enGuard reports fingerprint readers events: Unknown PIN, Verify Passed, Verify Passed IN, Verify Passed OUT and Verify Failed.
- Attendance logging from a Verid and PIN keypad.
- Attendance In/Out Board.
- Template On Card encoding of magstripe and contactless MIFARE, LEGIC and HID iClass smartcard.

## Access Control



## CCTV Systems



## Intruder Alarms



## DDA Systems



## Barriers



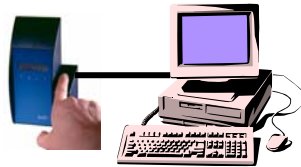
## Biometrics



## ID Card Systems



# Fingerprint Access Control Key Biometric Benefits



- Centralised enrolment means users can enrol at the PC(s) where the card or pin is issued without the need to go to any fingerprint door location.

- Template storage allows automatic distribution, database backup and Template-On-Card re-issuing without re-enrolment.



- Template transfer over LAN/WAN allows simple and effective administration of multi-site systems using the existing structured cabling – no need to run more cables.

- The site(s) security “state” can be user programmed to be in *Transparent* (Card or pin only – no fingerprint verification required) and *Inhibit* (no access to anyone) modes via time schedules and triggered via system events or alarms.



- Enhanced PIN reports from fingerprint readers allow system managers to audit check pin misuse and users with verification problems.



- A Verid with keypad input allows T&A clocking from a single point without the concern over “buddy clocking”.