

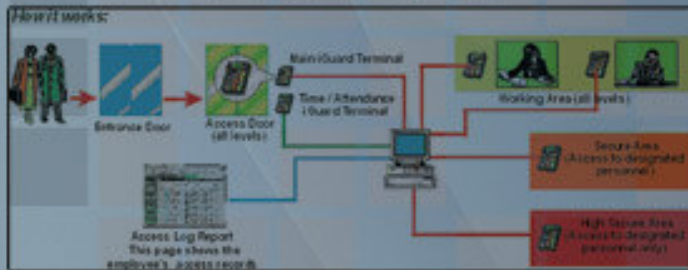


AVI INFOSYS

Define → Design → Deploy

iGuard

is Biometric and fingerprint identification system



Designed for business. Rather than using the traditional optical fingerprint scanner, it uses the most advanced capacitive fingerprint sensor for fingerprint acquisition to achieve the highest fingerprint-identification results.



Fingerprint / Contactless Smart Card Access Control & Time Attendance System

BASIC FEATURES

- Provides framework for centralized attendance monitoring even for offices at remote locations.
- Supports both biometric fingerprint & contactless smart-card authentication.
- Employees TCP/IP as a communication protocol.
- Fingerprint can be stored on smartcard.
- Capacitive fingerprint scanner.
- Supports upto 20000 users with a super-master.
- Physically robust yet attractive device which is easy to install.

ADVANCE FEATURES

MASTER/SLAVE CONFIGURATIONS

Multiple iGuard™ units can be setup as a Master/Slave network. Under this configuration one iGuard™ would be assigned as the Master and all other units are configured as slaves. When a user enroll in any one of these iGuard™ units, his/her user information, including the fingerprint information, would be replicated to all other iGuard™ units in the same master/slave network, so the same user does not need to enroll multiple times in order to have the access rights to all these units.

Embedded web - sever enables remote administration of the device. Ideal solution for large enterprises with offices at multiple locations.

iGuard™ Super Master

(Dedicated Server for the iGuard™ LM Series)



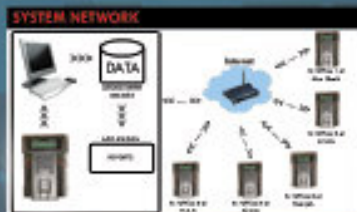
AVI INFOSYS

Define → Design → Deploy



iGuard™ Super Master

With an iGuard™ SuperMaster installed, the maximum no. of users of iGuard™ LM Series network will be increased upto 20,000 users. The iGuard™ SuperMaster will reside in your IT closet attached to your network through and RJ45 TCP-IP connection. Each iGuard™ LM Series on your network will synchronize with the iGuard™ SuperMaster and update fingerprint records, user access privileges and update transaction logs through our network automatically.



SPECIFICATIONS

	SC / FSC	SuperMaster
Power	12VDC, 800mA	12VDC, 800mA
Fingerprint Sensor	n/a / Yes	n/a
Contactless Smart Card reader & writer (built-in)	Yes	n/a
Web and Database Server		Built-in
Network Security (SSL)		Optional
Auto Data Synchronization (i.e., master / slave configuration)		Yes
Maximum Transaction Records stored	10,000	20,000
Static / Dynamic IP Assignment	Yes (Support existing DHCP Server)	
Non-volatile memory	16MB	32MB
Computer Supported (with Internet Browser)	Macintosh, Windows 95/98/NT/ME/XP, Linux and Unix Machine	
Valid Characters for Employee ID	0-9, A-B (maximum - 10 characters)	
Display	16 x 2 LCD with Backlight	16 x 2 LCD with Backlight
LCD Multi-Lingual	Yes	Yes
Two Finger Enrollment	Yes	
Fingerprint Sensor Type	Capacitive	n/a
Fingerprint Sensor Resolution	500dpi	n/a
Fingerprint Sensor scan area (mm)	12 x 15	n/a
Image Capture Time	< 1 sec.	n/a
Verification Time	< 1 sec.	n/a
False Rejection Rate	< 1 %	n/a
False Acceptance Rate	< 0.01%	n/a
Automatch Count	30	n/a
Network Protocol	TCP/IP, HTTP	
Network Interface	Ethernet (10-Base T)	Ethernet (100-Base T)
Other Interface	Wiegand (Output Only)	
Real Time Clock	Last for approx. 2 days without power	
External Controls	Door Strike Open-Door Switch Break-in Alarm Door Status n/a	
Dimension (mm)	105(W) x 38(D) x 150(H)	254(W) x 193(D) x 61(H)
Certification	CCC Pending	

How it works - as an Access Control System

STEP 1



Enter Employee ID

iGuard™ analyzes & compares a person's fingerprint against the previously enrolled record. If the two fingerprints match, the person is authenticated and if the time is within the authorized

STEP 2



Place the thumb on the sensor

Access Time restriction - you can define the authorized time for each individual or for a group of individuals.

Terminal restriction - you can specify who has the rights to access a particular terminal. It is useful in a multi-device environment, where multiple doors are controlled by different devices.

STEP 3



The door is unlocked if authenticated

Password/Fingerprint Access - you can define the period in which password can be used instead of fingerprint for access. This is particularly useful if you want to just use password to access during normal office hours, but to restrict the access to authorized people only after office hours. period for entry, the device will signal & release the electric door lock.

AVI INFOSYS LLC

PO Box : 26813

Dubai, United Arab Emirates.

Phone : +971-4- 2579040 Fax: +971-4-2579041

Email : info@avi-infosys.com

Web : www.avi-infosys.com

RESELLERS ADDRESS