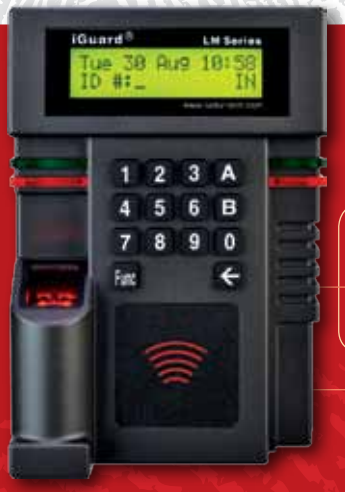
iGuard™

Biometrics Fingerprint / PIN / Smartcard based

Time Attendance and Access Control System with Web based Software

AVI INFOSYS

Define → Design → Deploy



iGuard™

We are currently using SecuGen® SDA03M sensor for LM520-FOSC (FBI Certified, FIPS 201/PIV Compliant, GSA APL Listed).

- A new model with SDA04 sensor (FBI Certified, FIPS 201/PIV Compliant, GSA APL Listed) will be introduced in mid. 2010 to address the high end market.

- The SecuGen SDA03M is very rugged, accurate, and affordable as it is designed for long-lasting performance in high traffic and tough environments.

- "Lucky Technology has deployed earlier generations of the iGuard with the United States Air Force and the US Army and in Afghanistan and thousands of schools, universities and business buildings worldwide," stated Wayne Wilkerson, President of Lucky Technology's US Operations.

- SecuGen's OEM sensors are used by device manufacturers all over the world and are widely recognized as among the most effective and affordable solutions for successfully integrating fingerprint capture and matching into third party devices.

iGuard™ Technology Overview

Each iGuard™ Biometric / Smart Card Security Appliance has a built-in Web Server enables all the computers in the corporate network to directly simultaneously access the device using any Internet Browser, such as Microsoft Internet Explorer Netscape Navigator. Different computer platforms such as Apple Macintosh, Microsoft Windows Linux machines can access the device. No additional software is required. So whether you are in an airport lounge or a hotel room, you can always check if your employees are already in the office or not, and you can even control, modify or disable their access rights to your office remotely via internet connection provided your iGuard Biometric / Smart Card Security Appliance is connected to an external IP address or your network is available through a VPN connection that is reachable from your location.

iGuard™ Super Master is a back-end server of iGuard™. With Super Master installed, the maximum no. of users of iGuard™ Master / Slave network will be increased to 5000 or up. And, Super Master is designed base on the iGuard™ patented embedded Web Server technologies, which enables all computers, such as Apple Macintosh, PCs & Unix machines, in the corporate computer network to setup, maintain and access the information of the device simultaneously using the well-known Internet Browser.

An ISO 9001:2008 Certified IT Solutions

iGuard SuperMaster

www.avi-infosys.com

iGuard ™ Features

Multi Factor Authentication:

With iGuard, users can be authenticated and verified through Fingerprint, Smartcard or Password. And depending on the different time period, you can set up the iGuard that the users can just simply presents his smartcard to get authorized (such as during high-traffic period), or requires the high-security fingerprint verification (such as after office hours or during weekends and holidays).

Access Rights:

When you can easily and conveniently assign different access rights to your employees, you can plan your security better and maximize the effectiveness of the human resources. And with the built-in Web Server technology, iGuard empowers you to manage the access rights of each individual employees or a group of employees easily anytime, anywhere using any web-enabled computers or mobile devices. For example, you can assign the staff members of the marketing department the rights to get in the office premises during weekdays from nine to five only, or prevent a particular employee from entering the computer server room. Reports: iGuard includes three built-in reports: Access Log, Attendance Report & Daily In/Out report, that can be accessed via any web-enabled computer with web browser. Should more sophisticated reports be required, such as for the payroll purposes, the information can be downloaded and saved in in Microsoft Excel format and in plain text format. In addition, the access records can be saved in any PC in the network in the popular ODBC database format in real-time manner, and other applications can conveniently obtain the information from the ODBC (the required software, iServer is available free-of-charge in our download page)

Economical:

All the necessary hardware and software is built-in to the device, including the hardware to connect the system to the corporate network. All you need to do is to plug-in the popular RJ-45 network cable to the back of the device. No other hardware and wiring is necessary. In contrast, all other existing security systems use the old RS232 & RS485 wiring system to connect to the dedicated computers (not to the corporate network), and it usually involves a lot of extra wiring works.

Small Footprint:

iGuard is a wall-mounted unit elegantly designed with extremely small footprint. In fact, it is the smallest stand-alone biometrics device available in the market today. It can be mounted easily and conveniently without requiring a lot of space.

Simplicity:

iGuard is an Internet-Ready Security System, and is the first and the only network appliance security product in the market that uses TCP/IP as the protocol to communicate with other iGuards and the outside world. The protocol enables the device to directly connect to the corporate network via the existing cable wiring. And since the TCP/IP protocol is the Internet protocol, it allows all computers in the corporate network to access the device using the Internet Browser software. As a result, users do not need to learn to use a new software to access and administer the device, and most users can start using the device in minutes. In contrast, all other similar security systems use proprietary protocol & wiring, and proprietary software is required to access these systems and for compatibility purposes, iGuard also supports conventional interfaces including Wiegand, RS-485

An ISO 9001:2008 Certified IT Solutions Provider Company

Smartcards for iGuard™ readers

Technical Specifications

- RF contactless operates at 13.56 MHz
- Standard NXP Mifare Card
- 1K bytes,15 sectors, 48 bytes each
- R/W is protected by encryption key, 48 bit triple DES
- Raw data is scrambled by 64 bit DES.
- High Security, suitable for all applications.
- Free sectors can be reserved for multiple any purposes
- Print your own brand on this card

How it works as an Access Control System

iGuard™

STEP 1
Enter Employee ID

STEP 2
Place the thumb on the sensor

STEP 3
The door is unlocked if authenticated

iGuard analyzes & compares a persons fingerprint against the previously enrolled record. If the two fingerprints match, the person is authenticated. And if the time is within the authorized period for entry, the device will signal release the electric door lock.

The iGuard Security System analyzes and compares a persons fingerprint against the previously enrolled record. If the two fingerprints match, the person is authenticated. And if the time is within the authorized period for entry, the device will signal and release the electric door lock.

- 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.
- 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.

The Access Control Mode controls the employees from entering the business premises. The system controls the electronic door strike to lock / unlock the door. Users can be assigned to different departments and the authorized time for members in each department can also be controlled. In a multi-device environment, the access rights for each department in accessing authorized people only after office hours.

The Access Control Mode controls the employees from entering the business premises. The system controls the electronic door strike to lock / unlock the door. Users can be assigned to different departments and the authorized time for members in each department can also be controlled. In a multi-device environment, the access rights for each department in accessing

An ISO 9001:2008 Certified IT Solutions Provider Company

www.avi-infosys.com

iGuard™

Technical Specifications:

	FP / SC / FSC	Super Master
Power	12VDC, 600mA	12VDC, 800mA
Fingerprint Sensor	Yes / n/a / Yes	n/a
Contactless Smart Card reader writer (built-in)	n/a / Yes/ 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	
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 - 8 characters	
Display	20 x 2 LCD with Backlight	n/a
LCD Multi-Lingual	Yes	n/a
Two Finger Enrollment	Yes	
Fingerprint Sensor Type	Secugen	n/a
Fingerprint Sensor Resolution	500dpi	n/a
Fingerprint Sensor scan area (mm)	12 x 15	n/a
Image Capture Time	< sec.	n/a
Verification Time	< 1 sec.	n/a
False Rejection Rate	< 1 %	n/a
False Acceptance Rate	< 0.01%	n/a
Auto-match Count	30	n/a
Network Protocol	TCP/IP, Wiegand, RS485, RS232 (Optional)	
Network Interface	Ethernet (100-Base T)	
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

www.avi-infosys.com

www.vistasad.com

An ISO 9001:2008 Certified IT Solutions Provider Company

TOLL FREE 800 AVI (800-284)

AVI INFOSYS
Define → Design → Deploy

AVI INFOSYS LLC
Master Suite B # 1203, Pent House Office,
Bel Rasheed Twin Towers, Al Qusais - III,
Damascus Street, PO Box: 26813.
Dubai, United Arab Emirates
Tel: +971 4 258 8260, Fax: +971 4 258 8270
Email: info@avi-infosys.com
Web: www.avi-infosys.com

RESELLERS ADDRESS

INTERNATIONAL OPERATIONS