



# BIOMETRIC ACCESS CONTROL & TIME ATTENDANCE

**MXTA-IG-LM520-FOSC**

## Web Server

The built-in Web Server based upon the Linux® platform enables all the computers in the corporate network to directly access the device via the well-known Internet Browser, such as Microsoft Internet Explorer or any modern web browser.

The computers are platform-independent, and different computer platform such as Apple Macintosh, Microsoft Windows & Unix machines can access the device. No additional software is required. Administration, Reporting and Access can all be done simultaneously via the built-in web server.

## Built-In Database Server

The built-in Database Server allows authenticated computers on the network to query the information of the device, and can easily retrieve the various reports via the Internet Browser, such as the transaction logs, attendance reports, time sheets, and more.

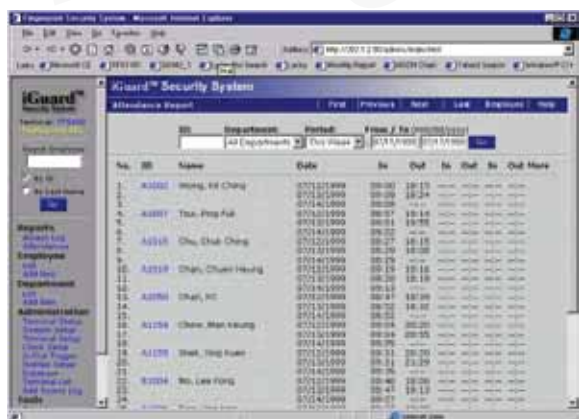
All the information is real-time information, instead of week-old or day-old data. In contrast, other systems must use dedicated computers running special proprietary software to retrieve the information, and usually dedicated HR persons are required to perform the functions.

## Optional Mifare® Smart Card Function

Each iGuard comes equipped with the renowned Philips Mifare Contact-less Smart Card Reader. (MIFARE® is an interface platform for contact-less smart cards and readers according to the ISO 14443-A Standard). With this option, users can both use the conventional fingerprint biometrics, PIN and/or the smart card for user authentication.

Having a secondary statement of user identity such as a smart card or PIN dramatically improves the security of your system. The smart card can also function as an employee badge for a visible level of security within your facility.

Each user will have his / her own smart card, which stores the user information including the name, company & branch code, and the fingerprint information.





# BIOMETRIC ACCESS CONTROL & TIME ATTENDANCE

## MXTA-IG-LM520-FOSC

### iGuard Technical Specification.

	SC / FSC / FOSC
Power	12VDC, 600mA
Fingerprint Sensor	n/a / Capacitive / Optical
Contactless Smart Card reader & writer (built-in)	Yes
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
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,7, Linux and Unix Machine
Valid Characters for Employee ID	0-9, A-B (maximum - 10 characters)
Display	16 x 2 LCD with Backlight
LCD Multi-Lingual	Yes
Two Finger Enrollment	Yes
Fingerprint Sensor Type	n/a / Capacitive / Optical
Fingerprint Sensor Resolution	500dpi
Fingerprint Sensor scan area (mm)	12 x 15
Image Capture Time	< 1 sec.
Verification Time	< 1 sec.
False Rejection Rate	< 1 %
False Acceptance Rate	< 0.01%
Automatch Count	30
Network Protocol	TCP/IP, HTTP
Network Interface	Ethernet (10-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
Dimension (mm)	SC/FSC:105(W) x 38(D) x 150(H) FOSC: 105(W) x 55(D) x 150(H)



It is a full-featured Access Control and Time & Attendance appliance incorporating:

- Incorporates the SecuGen SDA03M Optical Scanner
- Finger Scan & Contactless Smart Card capable
- Manage up to 1,000 users
- View last 10,000 events
- Embedded Web Server interface
- True platform independence
- DHCP or Static IP
- Webcam enabled
- Wiegand output capable
- Standardized report generation to CSV or MS Excel
- Manage users with up to 128 departments to customize access to doors - including holiday configuration
- Quickly and easily add, disable, enable or delete users



# BIOMETRIC ACCESS CONTROL & TIME ATTENDANCE

## MXTA-IG-LM520-FOSC

### BIOMETRIC ACCESS CONTROL & TIME ATTENDANCE

The iGuard Biometric Security System is a complete Access Control and Time & Attendance device that is built upon three core technologies:

- Biometric Authentication with Smart Card Capability
- TCP-IP Connection - Internet Protocol Standard
- Self Contained Processing with Built-in Patented Web Server

These iGuard terminals are small in size - but are extremely powerful. Each iGuard terminal is capable of stand alone operation without the use of a PC or server to process the transactions. All that is required to administer the iGuard is a PC with a web browser anywhere on your network or around the world.

The iGuard systems were designed to be used as a time & attendance device. Each time an employee checks in or checks out they must register on the iGuard terminal. By using Biometric authentication the iGuard virtually eliminates "buddy punching" and other time keeping fraud.

Downloading the transaction logs and record of hours worked is simple using a PC with any web browser. These logs can be downloaded in either CSV (Comma Separated Value) for importation into your payroll software or database or may be downloaded readily populated in a Microsoft Excel spreadsheet for review.

The iGuard Biometric Security System addresses the fundamental issue of facility access security by incorporating a connection to a 12v Low Voltage strike release that automatically releases the door when an authorized user is authenticated at the terminal. Each time this strike release is opened a transaction is recorded in a log on the iGuard that can be downloaded and reviewed over TCP-IP.

There is even an option for an automatic logging database using SQL for real time access control logs.

Networking multiple iGuard systems together over a LAN or WAN in a master/slave configuration will allow you to secure multiple doors within your enterprise - even if they are not in the same facility. All that is required to network these devices is a simple RJ45 connection and a static IP address on your network. It really is that easy to control access to your facility.

