

TRAINEE NOTES

Overview of Product Training

FingerTec® has variety of products to fit into nowadays market for time attendance, access control or 2-in-1 functions. There are 5 types of products, which are

- a. Time attendance models
- b. Time attendance & access control models
- c. Multimedia models
- d. Card reader/writer
- e. Fingerprint mechanical door lock

While FingerTec® software includes the followings

- a. TCMS v2
- b. FRSI 2 server
- c. OFIS TA
- d. Data Processor

The above software work with all FingerTec® models to analysis attendance and access records, to prepare reports, to export data to 3rd party system etc.

At the same time FingerTec provides software development kits (API command sets) to system integrator or software developer to build up unique solution with FingerTec® hardware. The BioBridge SDK can works with most programming languages in the market.

Chapter 1 Time Attendance Model

1.1 Introduction

There are total 4 models apply to pure time attendance applications. These models do not equipped with access control module and therefore it cannot support any door lock system. They are mainly to verify users and to capture their clocking activities. The main benefits are to prevent buddy-punching and systematic attendance capturing process. These models are AC100, TA102, TA103, TA103R, TA100T and TA100DIY.

The advantages of time attendance models are

- a. Low cost – the implementation cost of these models are lower compare to other FingerTec® models.
- b. Stylish and contemporary design
- c. Easy installation – DIY concept without required special tools and technician.
- d. Multi verification methods – each model can support verification by fingerprints and password. For TA103R, it can support RFID cards, and optional for HID cards and Mifare cards.
- e. Large users capacity – The fingerprint capacity either 1500 or 2800, support up to 1400 users (each user with 2 fingerprint enrolled).
- f. Large transaction logs – Transaction logs storage varying from 100,000 to 120,000.

TRAINEE NOTES

- g. Additional time attendance feature
 - I. Siren
 - II. Work Codes
 - III. Receipt printing
 - IV. Extended user ID
 - V. DIY attendance report

1.2 Useful Features

1.2.1 Siren

Siren also known as scheduled bell, and it is available in TA102, TA103R and TA100T. User can configure time period to trigger a siren or bell i.e. 8am bell rings to alert start to work. There are 2 types of schedules can be set.

- a. Daily schedules – 25 schedules (1 schedule for 1 time period) for a day. The 25 schedules are repetitive everyday.
- b. Weekly schedule – 20 schedules for a day i.e. Monday – 20 schedules, Tuesday – 20 schedules etc. Total of 140 schedules per week. The schedules are repetitive every week.

1.2.2 Work Codes

Work codes are number representing reason of clocking i.e. 15 – emergency leave, 23 – going to meet client etc. Administrator predefines the work codes and reason for users. Users will insert the relevant work codes when they are verified at the terminal. The information then display in software for administrator to review and check.

The feature is available in AC100, TA102, TA103R and TA100T.

1.2.3 Extended User ID

The default user ID length of AC100, TA102, TA103R and TA100T is 5-digits. However for certain users with large user capacity, they require longer user ID. Administrator can upgrade the terminal so it can support up to 9-digit user ID, to represent wider range of information.

1.2.4 Printing Receipt

This feature can added into AC100, TA102, TA103R and TA100T by firmware upgrade. Terminal is connecting to a receipt printing machine. Every time user verifies at the terminal, machine prints a receipt to the user. The date and time of verification and user ID are printed on the receipt. There are total 4 different printing formats.

1.2.5 DIY Time Attendance Report

This feature is only available in TA100DIY. Administrator does not need to use any software to print time attendance report. The TA100DIY contains settings (predefined by administrator) to calculate attendance of each user. Users need to press button to define clocking status i.e. Clock-In, Break, Resume, Clock-Out etc during verification. Terminal allocates the data automatically and output time attendance reports. Administrator downloads the reports into USB flash disk then to view and print it by using a PC and printer.

TRAINEE NOTES

1.3 Enrolment & Verification Methods

1.3.1 Basic

The basic enrolment and verification is fingerprint or password. For fingerprint, there are 2 types of verification methods, which are 1:1 (1 to 1) and 1:N (1 to many).

1:1 matching – user must insert his/her User ID into the terminal and then follow by fingerprint verification. Terminal will search into database for the fingerprint templates belong to the User ID. User places finger to scanner to capture his/her fingerprint. Terminal matches the fingerprint templates from database and the user's fingerprint to verify he/she.

1:N matching – user places finger to the scanner, and terminal captures the fingerprint templates. Terminal starts to search into database for the match fingerprint, then to verify the user.

Password is suitable for those do not applicable to use fingerprint. The password is numeric number and varying from 1 to 5-digit.

1.3.2 Cards

FingerTec® models can read cards for enrolment and verification. The types of cards are RFID, HID and Mifare. The standard of cards as below:

RFID card

- 64-bit 125kHz RFID/EMID cards.
- FingerTec® terminals can optional to read the 10-digit card number, last 8-digit or last 5-digit.
- User only waves the card to terminal, and terminal can captures the card number from it to enrol and verify.
- Nothing can write into the card because it is hard coded with specific card number.

HID card

- 26-bit HID 1325 cards.
- Same working operation as RFID cards as above.

Mifare card

- MF IC S50/S70 13.56MHz.
- FingerTec® terminals can write fingerprint templates of users into the cards directly, without to store into the memory of terminal.
- Terminal reads the fingerprint templates from card, then to match with the user's fingerprint.
- However user can optional not to store fingerprint into the card, but use it as RFID cards do. *This feature is applicable to selective models only.*

1.3.3 Various verification combination

Administrator can choose the relevant combination of verification method i.e. fingerprint + RFID card, fingerprint + password etc to apply to users. There are total 15 types of verification combination ready to use. This is to increase security and to allow to integrate with 3rd party system. *This feature is applicable to selective models only.*

1.3.4 Data Transmission

The most common data transmission for FingerTec® terminals are

1. TCP/IP – general network connection concept by using RJ45 pin. It can supports multi terminals and widely used in network structures.
2. RS232 – conventional 9-pin serial port for short distance connection. It can only connect from 1 terminal to 1 PC, and not suitable for network structures.
3. RS485 – conventional serial connection by using data converter. The converter tends to convert RS485 signal to RS232 then to input into PC. It requires a data converter and can support up to 1000m of connection distance. It can supports network connection by using Daisy Chain concept.

USB flash disk (pen drive) – In case wiring is not possible at the installation environment, USB flash disk is a good solution. User can use the USB flash disk to transfer data (user information, password, fingerprint, card information and transaction logs) among terminals and PC. The content of USB flash disk is encrypted to avoid any misuse of attendance data, access records, user information etc. Only terminals or software can decrypted the content to read and write it. *USB flash disk is only available for selective models.*

Chapter 2 Access Control & Time Attendance

2.1 Introduction

These models provide a complete solution for both access control and time attendance recording to employees. The models are suitable for small and medium offices, warehouses, retail outlets, educational centres etc.

The advantages are

- a. Complete solution for both time attendance and access control
- b. Stylish and robust design – for better appearance and decoration
- c. Easy installation – well designed for wall-mounted, flexible stand for hassle free installation, compatible to all kinds of electronic door lock system
- d. AdapTec AC – complete power supply cum door access controller with backup power system
- e. Various verification methods – higher security for highly secured zone
- f. Large user capacity and transaction storage – to support most of the working environment
- g. Integrated with useful time attendance features
- h. Integrated with useful access control features

2.2 Useful Time Attendance Features

2.2.1 Work Codes

Refer page 2 for details.

2.2.2 Extended User ID

Refer page 2 for details.

2.2.3 Printing Receipt

Refer page 2 for details.

2.2.4 Short message display

Administrator can upload short messages to the terminals to show to the users during verification i.e. "replacement holiday on Monday", "Happy birthday to Allan" etc. There are 2 types of short messages,

- Public message – to display to all users after verification process
- Personal message – only to display to dedicated users

Administrator can predefine the time period for users to view the messages. The messages are deleted automatically after the effective time period.

2.3 Useful Access Control Features

2.3.1 Door Sensor

Administrator can install a door sensor (magnetic switch) to the door and controlled by terminals. The door will trigger internal buzzer and alarm system during the following scenarios,

- Door force opened without verification or push exit button
- Door is not closed firmly after certain time period

2.3.2 Tamper switch

There is a tamper switch at the back of the terminals. The switch must compress firmly to the wall (or mounting surface) during installation. Any illegal dismantle will release the switch immediately. Terminal trigger alarm system (if connected to any) to alert administrator in case of illegal dismantle.

2.3.3 Duress Option

User can trigger alarm system via terminal during emergency or any tail gating to entrance. User can either following to trigger alarm

- Duress finger (special enrolled fingerprint)
- Duress password (special enrolled password)
- Duress button (press UP button and follow by any verification)

2.3.4 Alarm Output

The terminal supports 2 types of alarm output, NO (normally open) and NC (normally closed). The types of alarm output fit into different alarm system.

TRAINEE NOTES

2.3.5 Antipassback

2 terminals are install to guard same door. User must verify every time when he/she is coming in or leaving out a zone. The terminal stops and block user to access if he/she miss the previous verification. The screen of terminal displays "Antipassback" and door lock system does not respond.

The antipassback is to prevent any tail gating incident and to generate Entry-Exit reports of all users.

2.3.6 Master Slave

R2i is a slave terminal to capture and send fingerprints, card information to master terminal for verification. The R2i does not have any memory, access control module, or time attendance module. The R2i is does not have any LCD display, instead it only has fingerprint scanner and card reading antenna.

R2i connects to master (R2) by a unique cable (1 meter or 3 meter). R2i installs and work with R2 to guard an entrance to provide a complete access control solution with affordable cost.

2.4 Enrolment and Verification

The enrolment and verification include

- 1:1 matching
- 1:N matching
- Password
- Cards
 - RFID card
 - Mifare card
 - HID card
- Various verification combination

Details in page 2.

2.5 Data Transmission

The most common data transmission for FingerTec® terminals are

- TCP/IP
- RS232
- RS485
- USB flash disk (pen drive)

Details in page 3.

The terminals come with Wiegand Input and Output to ease integration with 3rd party controller. Terminals provide standard 26-bit Wiegand output and input.

Chapter 3 Multimedia Models

3.1 Introduction

The multimedia models are coming with 3.5" or 8.0" 65k color TFT screen display for better visual effects. The models are running on Linux platform for faster processing and to embed with more powerful features to the models. These models are providing 2 types of working scenarios, which are

- 1 – time attendance only
- 2 – time attendance and access control

The advantages are as below:

1. Photo display – to upload and to display company photo or advertisement as wallpapers or screen savers.
2. Movies playback – to upload and display company advertisement video during idle model.
3. Interactive display and icons – to ease operation with convenient and comprehensive 4-direction navigation key button.
4. Shortcut key buttons – to enable 1 touch access to particular function.
5. Photo capture – to capture users photo during enrolment and verification and save as reference.
6. Optional to upgrade with WiFi or GPRS connectivities.

3.2 Useful Time Attendance Features

3.2.1 Work Codes

Refer page 2 for details.

3.2.2 Extended User ID

Refer page 2 for details.

3.2.3 Printing Receipt

Refer page 2 for details.

3.2.4 Short message display

Refer page 2 for details.

3.3 Useful Access Control Features

3.3.1 Door Sensor

Refer page 4 for details.

3.3.2 Tamper switch

Refer page 4 for details.

3.3.3 Duress Option

Refer page 4 for details.

3.3.4 Alarm Output

Refer page 4 for details.

TRAINEE NOTES

3.3.5 Antipassback

Refer page 4 for details.

3.3.6 Master Slave

Refer page 4 for details.

3.4 Enrolment and Verification

The enrolment and verification include

- 1:1 matching
- 1:N matching
- Password
- Cards
 - RFID card
 - Mifare card
 - HID card
- Various verification combination

Details in page 2.

3.5 Data Transmission

The most common data transmission for FingerTec® terminals are

- TCP/IP
- RS232
- RS485
- USB flash disk (pen drive)
- Wiegand input and output

Details in page 3.

Chapter 4 Card Reader

4.1 Introduction

The card reader models are suitable for

1. Time attendance only
2. Time attendance and access control

The models can support

1. RFID cards
2. Mifare cards
3. HID cards

Refer to details in page 2.

TRAINEE NOTES

The advantages of the models are

1. Complete solution for both time attendance and access control
2. Stylish and robust design
3. Easy installation - DIY concept without required special tools and technician.
4. Large users capacity – The fingerprint capacity either 1500 or 2800, support up to 1400 users (each user with 2 fingerprint enrolled).
5. Large transaction logs – Transaction logs storage varying from 100,000 to 120,000.

4.2 Useful Time Attendance Features

4.2.1 Work Codes

Refer page 2 for details.

4.2.2 Extended User ID

Refer page 2 for details.

4.2.3 Printing Receipt

Refer page 2 for details.

4.2.4 Short message display

Refer page 2 for details.

4.3 Useful Access Control Features

4.3.1 Door Sensor

Refer page 4 for details.

4.3.2 Tamper switch

Refer page 4 for details.

4.3.3 Duress Option

Refer page 4 for details.

4.3.4 Alarm Output

Refer page 4 for details.

4.3.5 Antipassback

Refer page 4 for details.

4.3.6 Master Slave

Refer page 4 for details.

TRAINEE NOTES

4.4 Enrolment and Verification

The enrolment and verification include

- Password
 - Cards
 - RFID card
 - Mifare card
 - HID card
- Various verification combination

Details in page 2.

4.5 Data Transmission

The most common data transmission for FingerTec® terminals are

- TCP/IP
- RS232
- RS485
- USB flash disk (pen drive)
- Wiegand input and output

Details in page 3.

Chapter 5 Mechanical Door Lock

5.1 Introduction

The FingerTec Keylock Series is a mechanical lock system enhanced with fingerprint verification technology. The Keylock Series support password and cards as verification methods too. Furthermore a mechanical key is provided as backup overwrites system.

The advantages are

1. Sleek design
2. Robust structures
3. Nano technology and stainless steel mechanical rotating structure make it lasts for 10 years under normal usage.
4. Only required 4 1.5V AA battery to power on it.
5. The batteries can last for 15,000 unlocking activities.

5.2 Enrolment and Verification

The enrolment and verification include

- 1:1 matching (Keylock 8800 only)
- 1:N matching
- Password
- Cards (Keylock 8800 only)
 - RFID card
 - Mifare card
 - HID card

Details in page 2.

PRODUCT TRAINING



TRAINEE NOTES

5.3 Data Transmission

Only KeyLock 8800 has USB pen drive as data transmission channel.

Details in page 3.

Chapter 6 Software

Introduction

The FingerTec Software is a powerful time control management system designed for efficient, effective and user-friendly environment for its users. The FingerTec software is consists of:

- a. TCMSv2
- b. FRIS 2 Server
- c. OFIS TA
 - e. Data Processor
 - f.

This software operates on window-based system, which offers easy application and installation.

The advantages are

Combination of time attendance and access control systems with one comprehensive software.

- 1. Ease the burden of manual reporting
- 2. Reducing human errors
- 3. Producing comprehensive information.
- 4. Smooth data transfer
- 5. Easy connectivity from hardware device to PC.

6.1 TCMSv2

6.1.1 Introduction

TCMSv2 is software for all FingerTec models. You will save time to learn and familiarize with it because all FingerTec models are using the same software. The software features both time attendance and door access and it's bundled together with the product. There are 17 different languages in the TCMSv2 software in order to suit various markets both local and international. The language available in the TCMSv2 software is:

Arabic	Chinese Simplified	Chinese Traditional	English	Farsi
French	German	Indonesian	Italian	Malay
Portuguese(Portugal)	Portuguese (Brazil)	Russian	Spanish	Thai
Turkish	Vietnamese			

TRAINEE NOTES

Advantages of TCMSv2 software:

1. Easy upgrade – Free upgrades and installation downloads are available online from anywhere.
2. TCMSv2 come with user manual and user guide VCD that allows self-learning.
3. More technical guidelines and advices are posted online free at:
 - i- <http://user.fingertec.com> (for end user)
 - ii- <http://tips.fingertec.com> (for reseller)

6.1.2 The Basics

The TCMSv2 current version is TCMSv2.2 and is built with Visual FoxPro 9. In TCMSv2, you will require to insert the product and activation key for each terminal as protective measure. Without the product and activation key, you may not be able to download the data from the terminal.

The software allows configuring settings in terminals. With the TCMSv2, you can download & upload users information (IDs, fingerprints, passwords, Card IDs etc.) among all models.

Example: You have 5 terminals; enrolment can be done at one of the 5 terminals. Then you can download the users information into the TCMSv2 software. After that you can upload the user information to the other 4 terminals.

You can download the transaction logs from the terminal and stored into the software. The transaction logs will be used to prepare reports for both time attendance and access control. In TCMSv2 software, there are 3 levels of access, which are:

1. Administrator – full access
2. Login – preview and print reports
3. Head of department – preview and print reports for same department.

6.1.3 Time Attendance Features

Clocking schedules is use to set up the company working time. You are free to define the clocking time by grouping concept.

The TCMSv2 can support up to 999 clocking schedule and cover most common working scenario, which are normal working hours, over night shifts, rotational shifts, open shifts and flexi working hours. During the verification at the terminal, users don't need to define status because the TCMSv2 will automatically allocate the data in the attendance sheet based on the clocking schedule assign to the user.

In settings under clocking schedule, you can configure the company rules for:

1. Grace period for late in and early out
2. Overtime (OT) calculation
3. Deduction of lunch or dinner time

There are 6 columns in the attendance sheet, which are easy and understandable viewing. The TCMSv2 provides the 6 columns to allocate time attendance data for IN, Break, Resume, OUT, OT and Done. Besides, you can change it to IN – Lunch – Resume – Dinner – Resume –

TRAINEE NOTES

OUT. In the attendance sheet, the work time, OT time and short time will be calculated automatically based on the assigned clocking schedule.

The Ad-hock features added to provide more flexibility in the attendance sheet. You can edit the clocking, working, OT and short time. The edited data will appear in the bold colour and the original transaction will keep as records.

The TCMSv2 allows you to export the attendance data to ASCII, XLS or ODBC. The exported data can be imported into payroll or third party system for further calculation. Before export the data, you can predefined the data field position and length of field based on the payroll system or third party system format.

In the report generation, user and administrator can preview or print the time attendance and access control reports. The reports provides a clear viewing of attendance data (in-out time, work time OT, late in, early out etc.) There are 12 types of time attendance reports, which are ready to use. Other than that, the report also can save into digital format (DOC, XLS, PDF, JPG etc)

6.1.4 Access Control Features

Time Zone, Group Time Zone & Access Codes

It is use to configure the terminal to allow users to access into a certain zone for a certain time period only or to disallow users to access the door. The time zone function only applicable to door access terminal model.

For example, a storeroom is allowed to access only from 12:00 to 06:00p.m. Other than the configured time zone, the user may not be able to access the door.

You can configure the time zone by grouping for easy handling.

The time zone and user can be uploaded to selected terminals. So only these users can verify and open the door.

Entry – Exit zone

You can configure the entry and exit terminal at the access zone configuration. This function is use for the anti pass back function to record time when user come in or leave.

Online Monitoring

To get the online monitoring, you can use the clocking data audit list. When the user verified at the terminal, his/her ID and transaction is shown on the software screen. This allows an easy monitoring of each staff's movement.

Reports

4-access control reports are ready to be used in TCMSv2; it can be saved into digital format. Example: - DOC, XLS, PDF, JPG etc.

TRAINEE NOTES

Raw data exporting

In the clocking data audit list, you can export the raw data into TXT file. You can adjust the desired format, which you want to export. This raw data can be used with other third party system.

6.1.5 TCMS V2 Viewer

TCMS V2 Viewer is an application, which support login of normal users to check their attendance data and to print reports by themselves. You only need to install the TCMSv2 viewer at the PC with the TCMSv2 software. No special software is required to be installed in other users' PC. In a network environment, user can login the web browser by using his/her password or fingerprint (if the OFIS scanner is installed at the PC).

The login can be done via web browser (Internet Explore or Mozilla FireFox etc.). Other than user, the Head of department can login to check attendance for those under his/her department.

The TCMSv2 viewer is fast and easy to use tool and no extra installation or training is required to normal users. It understands report viewing:

1. Showing IN – Break – Resume – Out – OT – Done
2. Showing work time. OT time and short time
3. View by this month, previous month or this week

TCMS V2 Viewer allows enrolment of user login password through OFIS Scanner. This feature is optional.

TCMS V2 Viewer support multi language, which are:

- English
- Chinese Simplified
- Chinese Traditional
- Spanish
- Arabic

The administrator has access to view every user's attendance sheet by using the TCMSv2 viewer.

With the TCMSv2 viewer the administrator and user are able to query attendance sheet by this week, this month and the previous month.

Other than that, TCMS V2 Viewer allows printing out of attendance sheet report directly from the web browser without requiring installation of any software.

6.2 OFIS TA

6.2.1 Introduction

PC-based Time & Attendance Systems/Fingerprint Enrolment Station

The combination of OFIS scanner and TCMSv2 software has created a PC-based Time and Attendance product known as OFIS TA, made for small sized offices.

TRAINEE NOTES

OFIS TA makes fingerprint reader installation simplified with an easy plug to USB port of any computer system.

For larger corporation that deploy multiple units of FingerTec reader in their corporation, OFIS TA can be used as fingerprint enrolment station, which the enrolled fingerprint template can be transferred to other fingerprint readers from one centralized location.

6.2.2 Features and Benefits

OFIS

- Combination of PIN and biometrics or only biometrics verification to eliminate fraud
- Fast and precise verification with FingerTec OFIS Scanner
- Allow 1:1 and 1:N fingerprint verifications
- Unlimited user capacity for 1:1 fingerprint verifications, 1:N based on PC capacity.
- Hassle – free fingerprint registration and verification.
- Works well with dry, moist or rough fingerprints.

TCMS V2

- Manage time attendance & time clocking activities.
- Provides 6 definable daily clocking activities.
- Supports overnight working time not exceeding 24 hours.
- Supports rotating duty rosters and a maximum of three shifts in a day.
- Provides easy management of multiple FingerTec readers.
- Enables download of data and transactions.
- Allows export of data and transactions.
- Provides irrefutable audit trails reports.
- Produces various kinds of time attendance reports.

6.3 FingerTec Data Processor (FTDP)

6.3.1 Introduction

FTDP is basic software to manage the FingerTec terminals. It is designed to perform basic operations, which include:

- Linking up of all terminals for setting.
- Managing users from terminals for download or upload of users.
- Downloading of transaction logs and saving it into Microsoft Access database.
- Managing of time zones, group time zones and user verification method.

6.3.2 Terminal Management

- The terminal management allows three operations:
- To connect the software to any terminal.
- To connect the software via IP address, COM port or a URL, without having to insert any product key or activation key.
- To support connection up to 999 terminals.

6.3.3 User Management

User management allow five operations:

- To download and upload users from all connected terminal easily
- To delete users from FTDP or terminals directly, if the users are no longer allowed in the system.
- To plug in the OFIS scanner for user enrolment into FTDP.
- To insert user full names and nick names (names for display on terminal during verification) for any users.
- To export user information into Text, Excel, XML and HTML format as input to 3rd party system.

6.3.4 Transaction Management

Transaction Management allows four operations:

- To download all transaction logs from all terminal and save into database.
- To clear those transactions logs after downloading process.
- To view the transaction logs easily by sorting them according to Device ID, User ID, User name or date of transaction logs.
- To export transaction logs into Text, Excel, XML, and HTML format as input to 3rd party system.

6.3.5 Time zone and Group Time zones & Verification Methods

Time zone and group time zone:

- This function is only applies for access control (Ignore this if you are using for time attendance only)
- To configure the valid time zone for group users or particular users to limit their accessibility for any doors.
- For example, user group 1 can access Main Door from 11am to 3pm only. There are a total of 50 sets of time zones ready for configuration.

Different Verification Method

- This function is only applies to FingerTec models with different verification method only.
- To group users that are using the same verification method.
- For example, users in-group 1 use fingerprint method to verify, while group 2 users must verify using ID cards and fingerprints.
- There are a total of 14 different verification methods ready for configuration.

6.3.6 The Microsoft Access Database

- The FTDP stores database in Microsoft Access Database.
- To use ODBC manager to connect to the Microsoft Access Database to retrieve data for 3rd party system.
- For an example, a 3rd party system can connect to ODBC Manager to pull relevant data from FTDP.
- The 3rd party system processes then to analyse i.e. access control software to download transaction logs from database server for preparation of activity reports of each user.

TRAINEE NOTES

6.4 FRIS II

6.4.1 Introduction

FrIS II can be used as online fingerprint enrolment and verification server or can be used as centralized database server.

Online Fingerprint Enrolment & Verification Server

- Used together with FingerTec models with FRIS function.
- Online fingerprint enrolment and verification.
- Supported Models: R2, M2, I-kiosk 100, I-kiosk 100 plus, AC100 plus, TA100.
- Model with same outlook but supports remote identification system.

Centralized Database Server

- Used with all models without FRIS functions.
- Terminals without remote identification system.
- Generally referred to as non-FRIS terminals.

6.4.2 Features and Benefits

- FRIS offers larger storage depends on server capacity for a sizeable user-base and extensive transaction logs.
- FRIS offers better management and monitoring of staff via a stand-alone server.
- Management of unit branches by head quarters through multi-link servers.
- FRIS allows management of multiple readers through one server.
- FRIS provides smoother and safer data sharing between different management levels.
- FRIS offers WAN (wide area network), Internet access or LAN (local area network) to control servers and data management.
- With FRIS, data centralization is efficient and more effective
- FRIS offers secure data storage.
- FRIS is compatible with FingerTec BioBridge SDK for third party software integration.

6.4.3 Online Fingerprint Enrolment & Verification Server

A PC with FRIS II installed and named as FRIS II server

"Giant-size" terminal

- All fingerprints are stored inside the server and there are no limits of fingerprint capacity.
- All transaction logs are stored into database, which is My SQL or MS SQL, and there are no limit of transaction capacity.

FRIS terminals as capturing station

- Sends fingerprint templates to FRIS II server for verification
- Does not store any fingerprints or transaction logs.
- Does not verify fingerprints.

FRIS II server

- Verifies fingerprint.
- Records transaction logs.
- Return message to the terminal as Failed or Passed verification.

TRAINEE NOTES

OFIS scanner as FRIS client

- Installed FRIS client at PC and plugged in OFIS scanner.
- PC is connected to the FRIS II server.
- User now can verify by using the OFIS Scanner.
- Result of verification is displayed on the screen.

The data of FRIS II server stored in My SQL or MS SQL

- TCMSv2 is used to connect to the FRIS II server to download transaction logs.
- TCMSv2 will generate time attendance reports or access control reports.
- TCMSv2 is back-end software to process these transaction logs.
- TCMSv2 can link up many FRIS II server to copy and merge databases.

Benefits of FRIS II server

- As giant-size terminal to enrol and verify users
- No limit of users or transactions, do not need to separate users into different terminals.
- User can verify everywhere at every terminal.
- Database in My SQL or MS SQL could be used by other systems directly.

6.4.4 Centralized Database Server

A PC installed with FRIS II as FRIS II server

FRIS II server works with normal models, which are

- Without FRIS function, terminal cannot capture and send FP to FRIS II server.
- Enrolment and verification are done inside the terminal.
- Transaction logs are stored in terminals.

FRIS II server now will work

- To download/Upload users among all terminals.
- To download transaction logs from the terminals.
- To save all transaction logs into My SQL or MS SQL database.

The data of FRIS II server stored in My SQL or MS SQL

- TCMSv2 is used to connect to the FRIS II server to download transaction logs
- TCMSv2 will generate time attendance report or access control report.
- TCMSv2 is back-end software to process this transaction log.

Good to use in big company with multiple departments

- All transaction logs are stored inside a server – no interruption.
- Each department (or section, team etc) installed a copy of TCMSv2.
- Head of department runs TCMSv2 to connect to FRIS II server to download transaction logs.
- During downloading process, he/she must define the department so that only logs of the users under that department are downloaded.
- Each department can configure TCMSv2 to generate attendance according to their clocking rules.

Chapter 7 Software Development Kit (SDK)

7.1 Introduction

Software Development Kit (SDK) is a programming package that enables a programmer to develop applications for a specific platform. The package includes the APIs, programming tools and documentation.

In this diversified market, system developers can make the most of FingerTec devices to incorporate the "human touch" feature by enhancing their existing solutions to promote their niche

FingerTec SDK has the ability to connect all its devices with one single Active X components.

7.2 OFIS Server Pack

Features and Benefits

- Runs on web-based Browser/Server Environment
- The user's encrypted fingerprint will be transmitted and verified with the templates at the remote back-end server through LAN/WAN
- Allow 1:1 and 1:N fingerprint verifications
- Unlimited user capacity for 1:1 fingerprint verification; 1:N based on server capacity
- Fast and precise verification with FingerTec OFIS scanner
- Program Interface: Active X for easy integration with any third party system solution
- Fingerprint template storage; ODBC compatible database
- Development environment; VB, MS VC++, Delphi, MS ASP, VB.NET, ASP.NET and etc.
- Sample application written in MS VC++, Delphi, MS ASP are provided
- Client module supports multilingual feature
- Works well with dry, moist or rough fingerprints

7.3 OFIS Client Pack

Features and Benefits

- Ready-pack for system developer to add a layer of fingerprint protection to their windows-based software solutions.
- Allow 1:1 and 1:N fingerprint verifications
- Unlimited user capacity for 1:1 fingerprint verification; 1:N based on server capacity
- Fast and precise verification with FingerTec OFIS scanner
- Program Interface: Active X for easy integration with any third party system solution
- Fingerprint template storage; ODBC compatible database
- Sample application written in MS VC++, Delphi, MS ASP are provided
- Client module supports multilingual feature
- Works well with dry, moist or rough fingerprints

7.4 BioBridge

SDK for FingerTec Reader

System developers are full of ideas to make the most of FingerTec readers to suit to more applications for diversified market. Some may want to incorporate the "human touch" feature by enhancing their existing solutions to integrate with FingerTec readers to promote their niche.

TRAINEE NOTES

FingerTec BioBridge SDK come with DLL and Active X formats and currently supports Windows 9x/2000/NT platform. It works well on many development environments including of Visual Basic 6.0, Delphi 7.0, Visual C++, Microsoft.Net and etc.

Features and Benefits

- Ability to connect all FingerTec fingerprint readers with one single Active X component.
- Ability to make full use of FingerTec readers
 - a. Device control management/operation
 - b. General data management
 - c. User information management
 - d. User fingerprint management
 - e. Time zone group management
 - f. Backup data management
 - g. USB flask disk management
- BioBridge SDK currently supports Windows platform; for development purpose sample source code in Delphi 7.0 is provided. The use of DLL and Active X components are demonstrated using BioBridge SDK sample program.
- Well-written complete documentations are provided for reference.
Please take note that the signing of non-disclosure agreement is required to obtain the SDK.