

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

Keytracker Electronic Web based Locking system

Keytracker Ltd – Station Road – Rowley Regis

West Midlands - B65 0JY - England

1 INTRODUCTION

- 1.2 The offer system shall consist the following:
 - 1.2.1 Up to 320 **sets of keys in cabinets with minimum capacity of 40 keys** slot per cabinet with 1 Master control unit
 - 1.2.2 Central Management software for total integration include programming, configuration and monitoring

2 OPERATION REQUIREMENT:

- 2.1 The proposed electronic key management system shall be fully automated and able to operate and integrate with minimum contact-less reading technology using customer supply card system. The system shall be modular, has flexibility and feasibility for future expansion. It shall be equip with built in IP camera and **Global System for Mobile** communications (GSM) modem and all transaction shall be captured by the system; picture file shall be able to integrate with the user id and time of accessing the system; in the event of any violation, the system shall be able to **Short Message Service (SMS)** and E-mail to notify the management.
- 2.2 To gain access to the keys, the user must present an authorized card together with a secured pin number. Upon validation, the system will release the authorized keys to the user. To return the keys, the user shall present the card and secure pin again, and the system shall indicates which key slots to be returned. For any key expiry or validation, the system shall be able to inform the management via SMS and e-mailing. In addition, it shall be able to inform and facilitate management on appropriate actions to be taken, to react to the incident.
- 2.3 The system shall have the ability to generate reports and each report shall be customizable, allowing the operation to select the report parameters including, but not limited to the following:

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

- Keys in.
- Keys out.
- Overdue keys.
- Audit per use.
- Multiple users' activity.
- Alarm activity (definable per alarm type).

The electronic key cabinet offered shall meet the following minimum requirements.

3 GENERAL

3.1 The electronic key shall meet the following minimum general requirements:

- 3.1.1 To be of metal construction cabinet suitable for use within a secure environment. The cabinet should be of steel seam welded construction (minimum 1.5mm); powder coated to specification (standard color – dark grey).
- 3.1.2 Have electronic locking cabinet door with door sensor.
- 3.1.3 Tamper proof glass window on front cabinet door.
- 3.1.4 Capacity to secure up to maximum 320 tamper proof key rings.
- 3.1.5 Each tamper proof key ring can securely hold up to maximum of 8 keys.
- 3.1.6 Wide-angle high quality IP camera with minimum 15,000 Alarm/Active Recorder pictures.
- 3.1.7 Keypad to facilitate programming and input of digital security password.
- 3.1.8 5V light inside the cabinet which shall be trigger to turn on when the system detects an open door by the user.

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

3.2 TAMPER PROOF

The key management cabinet shall include a tamper proof minimum of 6mm polycarbonate window on front cabinet door

The tamper proof key shall meet the follow minimum general requirements:

3.2.1 The key shall be made by solid steel material.

3.2.2 The key shall not be able to duplicate in the general market.

3.2.3 Provide a cylinder change system by a master key in order to allow key replacement.

3.3 ACCESS CONTROL

The electronic key cabinet shall meet the following access control requirements:

3.3.1 Minimum standard PIN (keypad) access control for user input.

Capability to interface with a card reader,.

3.3.2 Ability to track and monitor all keys / users under system

control.

3.3.3 Ability for a manual override system.

3.3.4 Ability to mandate PIN with and / or card.

3.3.5 Ability to interface with the facilities access control system.

3.3.6 The cabinet must also have a Dual and Triple Card Access feature to gain access to the key cabinet.

3.3.7 Ability to present user name on the terminal upon authorized authentication.

3.4 POWER REQUIREMENTS

The electronic key cabinet shall be power by 240V with minimum 24-hour battery backup.

3.5 IT SYSTEM REQUIREMENTS

The electronic key cabinet shall be compatible with existing systems including Windows 98, ME, NT, 2000, XP and have an ability to be networked to such an IT system.

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

SNMP driver must include for third party integration.

The system must be able to support Linux operation system

3.6 REPORTS

The electronic key cabinet control system shall have the ability to generate reports including date, time, event and user of all key movements and access to the key cabinet. Reports shall be exportable to any computers attached to the electronic key cabinet via TCP/IP.

Report generation software shall be capable of generating detailed reports to track and monitor keys and users. Each report shall be customizable, allowing the operator to select the following parameters, but not limited to:

- 3.6.1 A particular date of records.
- 3.6.2 A particular time period of records.
- 3.6.3 Records of a particular key.
- 3.6.4 Records of a particular user.

The report generation shall be displayed in the following format, but not limited to:

Report List							
No	User ID	User Name	Date	Day	Time	Action	Key

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

3.7 KEY REMOVAL AND RETURN

The ability to remove keys shall be programmable to allow the following:

3.7.1 Single key removal and return – single indication. The display will

indicate that one key can be removed and/or returned.

3.7.2 Single key removal and return – multiple indications. The display will indicate more than one key is available for removal, but will only allow one key to be removed.

3.7.3 Multiple key removal and return.

3.7.4 The system shall allow the administrator to remove and return keys for other users of the system.

4 SYSTEM FEATURES

Each cabinet shall also be provided with the following:

4.1 A silent duress alarm to notify the Central Server operator.

Once authorized to access the cabinet, indicator light(s) will provide the user visual indication detailing the key(s) they may access.

4.2 The capacity to store up to 100,000 transactions and operate independently of the Central Server in the event of a network or Server failure.

4.3 Maximum 5000 users.

4.4 Maximum 320 key groups.

4.5 Maximum 32 schedule groups.

4.6 Maximum 5 SMS send to selected users in events of alarms.

4.7 Maximum 24-hour battery backup.

4.8 Maximum 2 min front door expire timer.

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

5 EMBEDDED KEY MANAGEMENT SOFTWARE

The Key Management Software is an embedded application and web based program that does not require any installation of new software. The operation system shall be Linux compatible.

The software shall include but not limited to the following features:

- 5.1 Multiple privilege levels for authorized users.
- 5.2 Remote programming, control and monitoring of all key cabinets.
- 5.3 Real time alarm updates; system shall be able to support both SMS and E-mail alarm notification
- 5.4 The system shall be notified the management of each alarm immediately via SMS, the pre-defined user for notification shall be minimum 5 users.
- 5.5 E-mailing must be part of the system to inform the management of the alarm. Using fetch mail via SMTP protocol, the system must be able to support minimum 5 users email address in every single alarm notification.
However, the system must be able to configure the requirement in the event the user decides to terminate any of the above options.
- 5.6 The system shall log all activities including but not limited to the time and date of the event, user id and key(s) removed/returned.
- 5.7 The system shall produce alarms and send a SMS to the operator within 1 second of their activation. Alarms shall include but are not limited to the following:
 - 5.7.1 Cabinet door forced open.
 - 5.7.2 Cabinet door open too long (DOTL).
 - 5.7.3 Non-returned key. The time frame that the keys must be returned shall be user definable and must allow for multiple shift changes.
 - 5.7.4 Removal and return of critical keys predefined by the administrator.
 - 5.7.5 Duress alarm.

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

6 CENTRAL MONITORING SOFTWARE

- 6.1 The system shall generate Reports using menu-based queries of Centralized ODBC database(s) of Logs including:
 - System Log,
 - Alarm Log and
 - Operator Action Log.
- 6.2 Reports can be generated based on:
 - Date,
 - Time,
 - Name
 - File name.
- 6.3 It shall be possible to Copy and paste these reports to EXCEL and Word. The paste must preserve the column and row alignment without the user having to reformat the data.
 - 6.3.1 All transactions generated by the system shall be logged onto the hard disk of file servers.
 - 6.3.2 Reports generated shall include normal transactions, alarm transactions, system parameters set up, all hardware equipment parameters set up, etc.
 - 6.3.3 It shall be possible to view the reports on computer screen first prior to printing.
 - 6.3.4 The reporting program shall allow transaction report filter selection by
 - event type
 - date range
 - time period
 - operator's name
 - cardholder name

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

- 6.4 The type of alarm reports shall include the following transactions
 - 6.4.1 The specific alarm point occurred, including time and date stamp
 - 6.4.2 The specific alarm point description
 - 6.4.3 Action(s) taken by the operator in response to each specific alarm
 - 6.4.4 Response of the system upon actions taken by operator
- 6.5 The reporting programs shall be able to generate the following database reports:
 - 6.5.1 All alarm points in the system
 - 6.5.2 All technical parameters related to each alarm points
 - 6.5.3 Level of alarm priority for each alarm point
 - 6.5.4 The alarm response action message assigned to each alarm point
- 6.6 Audit Trial Reports; shall be available to provide the following minimum information:
 - 6.6.1 All operators' log-in and log-out time & date stamp
 - 6.6.2 The time & date stamp of each operator whenever the operator made a change in the system database
- 6.7 User Reports
 - 6.7.1 All employees profile and ID cards information
 - 6.7.2 Access Groups and access levels reports

Technical Specification

Main Controller

ATMEL AT91RM9200 processor

Frequency	:	200 MIPS at 180 MHz
Instruction Set	:	ARM® High-performance 32-bit Instruction Set
On-chip cache	:	16-Kbyte Data Cache, 16-Kbyte Instruction Cache
MMU	:	Standard ARMv4 Memory Management Unit (MMU)
Data bus	:	8-, 16-, 32-bit Data Bus for Instructions and Data
Write Buffer	:	16-word Data Buffer, 4-address Address Buffer
Embedded Memories	:	16K Bytes of SRAM and 128K Bytes of ROM

Memories

SDRAM	:	16MB (up to 32MB)
NOR FLASH	:	2MB
NAND FLASH	:	32MB

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

Item	Amount
Ethernet MAC 10/100 Base-T	1
USB 2.0 Full Speed (12 Mbits per second) Host Port	1
Multimedia Card Interface (MCI) for SD card	1
RS232 Port	2
RS485 Port	2
Digital Input Port	8
Digital Output Port	8

Power Supply

Voltage range : 8 - 24V DC
Current: 200mA

LCD Panel

- High resolution LCD
- ASCII font: 16 characters x 4 rows
- User-friendly GUI: dynamic cursor position follow user input; highlight with inverse background and font color; multiple selections with up, down, left, right keys
- Classical white color backlight
- On RS485 comm link

Keypad

- High quality Silicone rubber keys
- 0~9 ten numeric keys
- & # keys represent backspace and enter
- 4 function keys placed below dynamic graphical icons to represent up, down, left, right, select and return
- Beeper integrated
- Each key pressed will beep once
- Beeper will alert user when wrong input detected
- On RS485 comm link

Key Distribution Interface

- Address decoder, each interface has unique ID to main controller
- Key units commander and states collector
- Maximum carry 2(rows) x 4(columns) = 8 keys
- On RS485 comm link

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

Key Unit

- High sensitive IR sensor to update key position
- High security Camlock and guarded by stainless steel solenoid
- Tamper proof key ring
- One LED states indicator Red, Green, Orange

Pictures Recorder

- High quality IP camera
- Wide-angle Lens (36mm)
- 5,000 Alarm/Active Recorders X 3 Picture per activation
- Record , Total 15,000 Pictures expandable

Power Supply & Battery Charger

- Power supply unit: 12Vdc +15%, Current/Power Consumption by Product Model
- Battery: 12V, Lead Acid Fiamm Battery, Capacity by Product Model
- Power Down Detector & Battery Auto Cut-in
- Battery Auto Checking & Battery Low Auto Cut-off
- System Battery Backup: Standby Mode more than 24Hrs; Active mode than 20 Times

Cabinet

- Body: 1.5 mm Steel Plate
- Front Door: Tamper Proof Glass Window
- Electric Strike (Power off to lock)
- Door Contact Sensor
- Back Door Tamper Switch
- Master Key for Emergency Release Keys
- Super Bright LED Night Lighting

GSM Modem

- Dual band GSM900 & GSM1800
- SMS notification to admin when alarm occurs
- SMS reminder to selected user when withdrawal key expired
- Able to send 5 SMS message upon activation for each alarm

Card Reader

- Mifare Proximity Card Reader
- Any reader with Weign Format

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

Embedded Application/Control Software

- Built Web Pages for System Setting, Configuration, Monitoring & Management

Operation Feature

- Keypad - admin
 - ✓ Change pin himself
 - ✓ Create new user
 - ✓ Edit existing user
 - Change user id
 - Change user pin
 - Change key group
 - Change schedule
 - Change maximum key allowed
 - Change maximum hold period
 - Disable user
 - Remove user
 - ✓ Edit key group
 - Add / remove key from group
 - Remove all keys in group
 - ✓ Edit schedule
 - Edit weekday and special day timing
 - Remove all timings
 - ✓ Edit system
 - Edit number of cabinet and key
 - Edit TCP / IP
- Keypad - user
 - ✓ Change pin himself
- Web - admin
 - ✓ Check key status
 - ✓ Check records
 - ✓ Add / edit / remove / disable user
 - ✓ Add / edit / remove key info
 - ✓ Add / edit / remove key group
 - ✓ Add / edit / remove schedule
 - ✓ Edit system
- Web - user
 - ✓ Check key status
 - ✓ Check user records

SPECIFICATION FOR KEY MANAGEMENT SYSTEM

Software Features

- Deploy latest powerful Embedded Linux (kernel 2.6.16) for ARM structure
- Support software controllable MPEG video stream and JPEG picture capture
- Implement embedded web portal to provide remote control and configuration
- Provide mass data storage using SD card, thumb drive or Hard Disk
- Integrate with SQLITE Database to manage data efficiently
- Enable multithread to speed up process execution
- Adapt to 10/100 Base-T Local Network automatically, support DHCP and firewall.
- Employ embedded web server which support dynamic web page such as CGI, PHP, JavaScript, JES and ESP
- Embedded web server support user authorization and Secure Sockets Layer (SSL)

Queries to TechSupport@Keytracker.com